ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA Y TECNOLOGÍA EN COMPUTACIÓN

ESTUDIO E IMPLEMENTACIÓN DE UNA METODOLOGÍA DE PREVENCIÓN DE INTRUSOS PARA REDES LAN. CASO PRÁCTICO: SISTEMA DE PREVENCIÓN DE INTRUSOS EN LA RED CORPORATIVA DEL MUNICIPIO DE RIOBAMBA.

TESIS DE GRADO

Previa obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

Gabriela Catherine Torres Andagana
Diego Fernando Llanga Salcán

RIOBAMBA - ECUADOR
2010

Gracias a mis padres, por inculcarme el afán de superación, por su sacrificio para que lo lograra, por perdonar mis errores, por ayudarme a que este momento llegara.

Gracias mi amor por estar siempre conmigo y por los buenos y malos momentos que supimos sobrellevar.

GABRIELA T.

A mis padres, por darme todo su apoyo y quererme por sobre todas las cosas. A ti preciosa por darme tu amor, apoyo, confianza, y compartir nuevos e inolvidables momentos en mi vida.

Gracias por ayudarme a cumplir mis objetivos como persona y estudiante.

DIEGO LL.

Gracias a nuestros maestros, ellos que se preocuparon porque los conocimientos que nos brindaron sean los correctos y permitieron lograr nuestro objetivo, un agradecimiento especial al Ing. Daniel Haro, director del presente proyecto.

A Dios por el camino recorrido

A mis padres por el amor, comprensión y apoyo incondicional que me han brindado y por creer en mí.

A mis hermanas por su cariño y su comprensión.

GABRIELA T.

A mi padre por brindarme los recursos necesarios y estar a mi lado apoyándome y aconsejándome siempre. A mi madre por hacer de mi una mejor persona a través de sus consejos, enseñanzas y amor, a mis hermanas por brindarme su apoyo y confianza.

DIEGO LL.

Y a todas las personas que de una u otra manera hicieron posible la realización de esta tesis.

NOMBRE	FIRMA	FECHA
Dr. Romeo Rodríguez **DECANO DE LA FACULTAD INFORMATICA Y ELECTRONICA**	----------	----------
Ing. Paúl Romero **DIRECTOR DE ESCUELA DE INGENIERIA ELECTRONICA**	----------	----------
Ing. Daniel Haro **DIRECTOR TESIS**	----------	----------
Ing. Danilo Pastor **MIEMBRO TRIBUNAL**	----------	----------
Lcdo. Carlos Rodríguez **DIRECTOR CENTRO DOCUMENTACION**	----------	----------
NOTA DE LA TESIS	----------	

Nosotros, **GABRIELA CATHERINE TORRES ANDAGANA Y DIEGO FERNANDO LLANGA SALCÁN** somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO.

Gabriela Catherine Torres Andagana

Diego Fernando Llanga Salcán

ÍNDICE DE ABREVIATURAS

Se presentan las abreviaturas de uso frecuente en este documento, tanto en el ámbito de la seguridad de la información, las metodologías de seguridad y los sistemas de prevención de intrusos.

ADOdb: Active Data Objects Data Base.

AGR: Análisis y Gestión de Riesgos.

ALARP: As Low As Reasonably Practicable, tan bajo como sea razonable (referido al nivel de riesgo).

BASE: Base Analysis and Security Engine, Base de análisis y motor de seguridad.

BSI: British Standards Institute, Instituto Británico de Estándares.

CENTOS: Community ENTerprise Operating System, Sistema Operativo para la comunidad empresarial.

CMM: Capability Maturity Model, modelo de madurez de capacidades.

CPD: Centro de Proceso de Datos.

DNS: Sistema de Nombre de Dominio.

DRP: Disaster Recovery Plan, plan de recuperación de desastres.

HTTP: Protocolo de Transferencia de Hipertexto.

ICMP: Protocolo de Mensajes de Control de Internet.

IEC: International Electrotechnical Commission, Comisión Electrotécnica Internacional.

IDS: Sistema de Detección de Intrusos.

IMR: Ilustre Municipio de Riobamba.

IP: Internet Protocol, Protocolo de Internet**.**

IPS: Sistema de Prevención de Intrusos.

ISMS: Information Security Management System, Sistema de gestión de seguridad de la información.

ISO: International Organization for Standardization, Organización Internacional de Estandarización.

MAC: Media Access Control, Control de Acceso al Medio**.**

OCDE: Organización para la Cooperación y el Desarrollo Económico

PDCA: Plan, Do, Check, Act. Planificar, Ejecutar, Comprobar, Actuar. Ciclo de

Deming o de la mejora continua.

PHP: Hypertext Pre-processor. Pre-procesador de Hypertexto

PRD: Plan de recuperación de desastres.

RACI: Responsible, Accountable, Consulted, Informed. Encargado, responsable, consultado, informado.

SGSI: Sistema de Gestión de Seguridad de la Información.

SMTP: Protocolo Simple de Transferencia de Correo.

SSH: Secure Shell, intérprete de órdenes segura.

TCP: Protocolo de Control de Transferencia.

TR: Technical Report, informe técnico.

URL: Uniform Resource Locator, Localizador de Recurso Uniforme

UDP: Protocolo de Datagrama de Usuario.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La existencia de amenazas que afectan la disponibilidad, integridad y confidencialidad de los datos es real. Es difícil para las organizaciones ecuatorianas poder identificar esas amenazas y adoptar recomendaciones que permitan prevenir, detectar y protegerse de ellas.

El Ilustre Municipio de Riobamba, una de las más importantes organizaciones del país, no está ajena a ésta situación, razón por la cual se creyó importante aportar una solución que permita mejorar el nivel de seguridad de la información que la entidad maneja.

Por tal razón, se implementó en la red corporativa del Ilustre Municipio de Riobamba una metodología de prevención de intrusos basada en normas y metodologías de análisis y gestión de riesgos vigentes en la actualidad y reconocidas bajo los estándares internacionales; fue decisiva la selección de los estándares que servirían de guía para el desarrollo de una metodología adaptada a la problemática en inseguridad que la entidad poseía.

Se planteó además como objetivo del proyecto poner en funcionamiento en la empresa un sistema de prevención de intrusos que actúa como gestor de algunas de las amenazas que fueron posibles de determinar según la aplicación de la metodología.

Para lograr el propósito general del proyecto se realizó una investigación experimental, pues se brindó una solución práctica que alteró nuestra variable dependiente y se concluyó que los niveles de seguridad de la red corporativa del municipio de Riobamba se mejoraron en un 25%, siendo éste el resultado final de la aplicación del proyecto.

Con el fin de brindar una guía general para la manipulación del trabajo escrito se detallará brevemente los aspectos tratados en cada uno de los capítulos que componen el documento.

Capítulo I. Marco Referencial. Detalla las generalidades del proyecto de tesis como los antecedentes y justificación para su realización, los objetivos a alcanzar, la hipótesis y los recursos utilizados.

Capítulo II. Marco Teórico. Su objetivo es citar los temas de mayor importancia y que se cree necesarios para el entendimiento del proyecto final; se cita un introductorio a la seguridad informática, las normas ISO 27002 y 27005, las metodologías Une y Magerit y generalidades de los sistemas de prevención de intrusos.

Capítulo III. Marco Metodológico e Hipotético. Pretende justificar el uso de las distintas herramientas software en el desarrollo del proyecto; se citan sitios webs que los recomiendan y validan su funcionamiento.

Capítulo IV. Marco Propositivo. Detalla el estudio de las normas y metodologías que sirvieron de base para el desarrollo de la metodología propuesta en este mismo Capítulo; se detalla cada una de las fases que componen la misma.

Capitulo V. Resultados Obtenidos. Se indica el desarrollo mismo de la metodología propuesta en el capítulo IV, así como la implementación del sistema de prevención de intrusos.

CAPÍTULO I

MARCO REFERENCIAL

1.1. ANTECEDENTES

La seguridad en las redes ha comenzado a ser un problema importante en el mundo moderno. El número de computadoras, la conectividad entre ellas y la importancia que han adquirido en el desarrollo tanto investigativo como empresarial, convirtiéndolas en las principales portadoras de información sensible que requiere no ser alterada y muchas veces no ser consultada por personal no autorizado.

Esto ha hecho que los ordenadores y las redes puedan verse involucrados en un ataque informático siendo las herramientas utilizadas para cometer dicho ataque, siendo las víctimas del ataque o pudiendo ser utilizadas para propósitos incidentales relacionados con la irrupción.

En el M.I Municipio de Riobamba conjuntamente con su departamento de Sistemas manejan bases de datos de mucha importancia como son:

Pago de predios, permisos de locales comerciales, información financiera de los mercados de la ciudad, contribución de patentes, arrendamientos de locales

comerciales, información del Serot, entre otros; estos datos son manejados por medio de un servidor con un Sistema Operativo Windows Server 2003 con la ayuda del manejo de bases de datos en Oracle; para lograr cierto tipo de protección la red maneja el antivirus Mcafee v8.7 conjuntamente con la ayuda de Policy, servicio adicional de Mcafee, que cuenta con su respectiva licencia.

Esta entidad también posee un servidor de Internet de banda ancha proporcionado por CNT con una velocidad de 512 Kbps, el cual cuenta con un administrador de servicio para determinar ancho de banda y restricciones de acceso; el dispositivo que permite este control es el Kypus versión 1.3.0.8 usado para compartir dicho recurso a todos los departamentos que conforman la entidad.

La entidad cuenta además con un servidor secundario con un Sistema Operativo Windows Server 2003 para realizar todos los respaldos de la información que maneja.

Para la distribución de datos por medio de la intranet en sus diferentes departamentos dentro de esta entidad como son: Proyectos, Sistemas, Alcaldía, Consejeros, Concejales, Prefectura, Recursos Humanos, Secretaria, Pagos de impuestos, la red local maneja 5 switchs, 4 switchs de marca 3com y 1 de marca D-Link..

Posee también un enlace de Fibra óptica que permite la comunicación con el departamento de Planificación y Avalúos ubicado a 100 metros de esta institución por lo que dispone de un transceiver de Fibra Óptica a conector RJ45 de marca Nexxt ubicado en el armario donde se sitúan los switchs.

El Municipio de Riobamba se beneficia de enlaces inalámbricos de radio frecuencia con distintos puntos dentro de la ciudad de Riobamba para el almacenamiento de datos de todos los usuarios, estos puntos son los siguientes:

Mercado Oriental, Terminal, Condamine, Santa Rosa, Patronato y Emapar.

Toda esta información y la gran área de la red local no está sujeta a una política de seguridad íntegra para su protección, y si no se implementa alguna técnica para lograrlo, toda esta información puede ser manipulada de forma remota o local por usuarios que no tengan acceso causando pérdidas para dicha entidad.

Para dar solución a la problemática ya mencionada y con el fin de proteger los recursos informáticos de esta empresa se han implementado algunas medidas de seguridad pero no muy eficaces como son McAffee con ayuda de Policy y aunque se sigan todas las recomendaciones de los expertos, esta institución no está libre de posibles ataques a futuro.

Una de las políticas de seguridad que se logró implementar en dicha entidad son los (IPS) Sistemas de Prevención de Intrusos que conforman la nueva tecnología de seguridad informática para protección de servidores y redes que bloquean de forma eficiente ataques externos e internos y todo tipo de amenazas conocidas y desconocidas.

Los IPS aparecieron como una evolución de los IDS, los IPS no se limitan a escuchar y monitorear el tráfico de la red sino que intervienen activamente ya que el tráfico circula a través del sistema y cualquier intento de ataque será bloqueado por el sistema en el mismo momento en que el evento ocurre.

1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS

Debido a la falta de políticas de seguridad en la red de la entidad mencionada, es de vital importancia el estudio de una metodología de prevención de intrusos adecuada a la problemática de la red, y la implementación de un sistema de prevención de intrusos lo cual permitirá al M.I Municipio de Riobamba conjuntamente con su departamento de Sistemas proteger la información crítica de una forma proactiva de todos sus departamentos sin limitarse a emitir alertas en una consola luego de que los ataques han sucedido, esta tecnología supone un beneficio continuo y una inversión verdaderamente inteligente para dicha entidad, así mismo ésta técnica protegerá la información, aplicaciones y mejorará el rendimiento de la red porque a través de ella no circulará código dañino.

El enfoque clásico de la seguridad de un sistema informático siempre define como principal defensa del mismo sus controles de acceso, desde una política implantada en un cortafuegos hasta unas listas de control de acceso en un *router* o en el propio sistema de ficheros de una máquina, esta visión es extremadamente simplista si no tenemos en cuenta que en muchos casos esos controles no pueden protegernos ante un ataque.

Con la ejecución de este proyecto se desea analizar la seguridad en la red de computadores y en las bases de datos que maneja el M.I Municipio de Riobamba, implementando técnicas para conseguir un nivel de seguridad aceptable para esta organización; debido a que, al ser ésta una entidad pública que brinda servicios varios a la ciudadanía maneja información reservada, delicada y de mucha importancia que necesita obligatoriamente tener un grado alto de seguridad en el manejo de la misma.

Es ésta la principal razón que nos motiva al estudio e implementación de una metodología para la prevención de intrusos que pretende ser desarrollada y aplicada en la plataforma LINUX con ayuda de distintas herramientas como es el caso de Snort.

Es preciso destacar también la inclinación actual del gobierno al querer migrar todas las redes de las entidades gubernamentales a software libre, (Linux) consideramos esto como una ventaja al desarrollo del proyecto.

Otra de las razones por las que creemos conveniente el desarrollo de este proyecto es el creciente avance de tecnología y software en nuestro país así como también el avance en formas y manías de ataque a las redes informáticas. Se puede entonces destacar el documento final como una bibliografía para las generaciones futuras.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Estudiar e implementar una metodología de prevención de intrusos en la red corporativa del M.I Municipio de Riobamba con el fin de proteger la información digital privada que allí se maneja.

1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Realizar un estudio de las metodologías de prevención de intrusos existentes.
- ✓ Elegir la metodología más apropiada para ser implementada en el M.I Municipio de Riobamba.
- ✓ Desarrollar un IPS (Sistema de Prevención de Intrusos) para poder tener una política de seguridad aceptable.
- ✓ Implementar el Sistema de Prevención de Intrusos con el Sistema Operativo Linux y la ayuda de diferentes herramientas.

1.4. HIPOTESIS

El estudio e implementación de una metodología de Prevención de Intrusos en la red corporativa del M.I Municipio de Riobamba permitirán mejorar los niveles de seguridad de la información privada que la institución maneja.

1.5. RECURSOS NECESARIOS

1.5.1. RECURSOS HUMANOS

Para el desarrollo del proyecto de tesis fue necesaria la colaboración de las siguientes personas:

Tutor de Tesis: Ing. Daniel Haro, Docente de la FIE

Desarrolladores: Gabriela Torres, Diego Llanga, Estudiantes de la FIE

Administradores de red del Municipio de Riobamba: Ing. Rosa Zabala, Jefe departamento de sistemas; Ing. Merci Mantilla, Analista de sistemas;

Colaboradores: Ing. Danilo Pastor, Vicedecano FIE

1.5.2. RECURSOS MATERIALES

Se detalla a continuación el hardware y software utilizados durante el desarrollo del proyecto de tesis.

Tabla I.1 Recursos en hardware

Hardware		
Cantidad	**Nombre**	**Estado**
1	Computador Pentium 4	Optimo
	Multimedia 52 x Monitor VGA Disco Duro 80 GB. Memoria Ram.512MB.	
1	Portátil Pentium 4	Optimo
	Multimedia 52 x Disco Duro 80 GB. Memoria RAM. 1GB.	
1	NoteBook HACER	Optimo
	Intel Atom 1.6 GHz Disco Duro 120 GB. Memoria RAM 2 GB.	
1	Impresora Epson Stylus C92	Optimo
	Sistema de inyección a Tinta Cartuchos 1 Negro 3 Color	
1	Modem Movistar 3.5G	Optimo
	USB ZTE	
1	Switch NEXXT	Optimo
	8 puertos 10/100Mbps	

Tabla I.2. Recursos en Software

Nombre	Descripción	Estado
Windows XP SP2	Sistema Operativo	No Legal
Linux Cento5	Sistema Operativo	Legal
Microsoft Word	Procesador de Texto	No Legal
Microsoft Excel	Editor de Hojas de Cálculo	No Legal
Microsoft Power Point	Editor de diapositivas	No Legal
Snort	Herramienta de Seguridad	Legal
Nmap 5.0	Escaneo de red	No Legal
Microsoft Visio 2007	Procesador de Diagramas	No Legal

1.6. TIPO DE INVESTIGACIÓN

Al hablar de la implementación de una metodología para la detección de intrusos, se dió solución en lo que a seguridad se refiere a la red corporativa del Municipio de Riobamba, razón por la cual ubicamos nuestro tema dentro del campo de la investigación experimental que además hará uso de los siguientes métodos de investigación:

Método Científico: Es claro que al ser este un trabajo final de investigación científica está obligado a seguir un orden esquemático lógico para descubrir los medios científicos en los cuales se apoyó para llegar a los fines que se propuso inicialmente.

Método Inductivo: Puesto que se hizo un proceso analítico-sintético mediante el cual se partió del estudio de las actuales medidas de seguridad en la red estudiada para llegar a determinar las principales amenazas que la aquejaban.

Método Deductivo: Se realizó también un proceso sintético-analítico ya que a partir de conceptos, normas, y principios generales sobre la seguridad informática se llegó a conclusiones que fueron la base para ser aplicadas en el diseño de una metodología para la seguridad de la red informática del Municipio de Riobamba.

CAPÍTULO II

MARCO TEÓRICO

2.1. INTRODUCCIÓN A LA SEGURIDAD EN REDES LAN

Se entiende a la seguridad como un estado de cualquier tipo de información o lo que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- ✓ **Integridad**: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- ✓ **Confidencialidad**: La información sólo debe ser legible para los autorizados.
- ✓ **Disponibilidad**: Debe estar disponible cuando se necesita.
- ✓ **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Toda organización debe estar a la vanguardia de los procesos de cambio, donde disponer de información continua, confiable y en tiempo preciso, constituye una ventaja fundamental.

Donde tener información es tener poder.

Donde la información se reconoce como:

- ✓ **Crítica**, indispensable para garantizar la continuidad operativa de la organización.
- ✓ **Valiosa**, es un activo corporativo que tiene valor en sí mismo.
- ✓ **Sensitiva**, debe ser conocida por las personas que necesitan los datos.
- ✓ Donde identificar los riesgos de la información es de vital importancia.

2.2. TIPOS DE SEGURIDAD INFORMÁTICA

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres tipos: seguridad física, seguridad ambiental y seguridad lógica.

2.2.1. SEGURIDAD FÍSICA

Es muy importante ser consciente que por más que una empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un ataque físico directo, tomando en cuenta esto aparece el concepto de la seguridad física, que es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

Así, la **Seguridad Física** consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante*

amenazas a los recursos e información confidencial". [1] Se refiere a los controles y mecanismos de seguridad dentro y alrededor del departamento de sistemas y equipos, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.2.2. **SEGURIDAD AMBIENTAL**

No se puede dejar de tomar en cuenta los inesperados riesgos naturales a los que pueden estar expuestas las redes informáticas, razón por la cual aparece el concepto de la **Seguridad Ambiental**, que son los procedimientos existentes para controlar que los efectos ambientales no perjudiquen el procesamiento, los equipamientos y el personal de una red.

Algunas reglas básicas sobre la seguridad ambiental son:

Protectores de pico de tensión eléctrica para el equipamiento central.

Protecciones eléctricas, de agua y gas.

Instalaciones de aire acondicionado, sistemas de refrigeración y ventilación fluida.

Protección ante incendios y métodos eficaces de evacuación guiados.

2.2.3. **SEGURIDAD LÓGICA**

Nos referimos a seguridad lógica como los procedimientos existentes para controlar el acceso lógico no autorizado a la información, ya sea que se realice mientras ésta se encuentra almacenada o durante la transmisión.

---

[1] *HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.* http://www.kriptopolis.org

2.3. SITUACIÓN ACTUAL EN EL MEDIO EMPRESARIAL

En nuestro país estadísticamente, la amenaza más importante para nuestros datos, la encontramos dentro de la empresa. Los accesos indebidos o no autorizados a información corporativa son realizados principalmente por empleados de la misma.

A esto hay que sumarle los ataques de virus informáticos ocasionados intencionalmente o por ignorancia, por los propios empleados.

En sentido contrario transitan, en general las empresas de nuestro país, preocupándose más por los agentes externos que por los internos. No es de olvidar que los ataques realizados por los hackers o crackers son tapa de los diarios, lo que lleva a que la gente se sensibilice más por este tipo de delitos.

Lo importante es que la empresa realice un análisis de riesgos formal, para poder identificarlos y establecer su importancia. El resultado de este análisis establecerá si se está más expuesto a ataques internos o externos, o viceversa, o se debe considerar otro tipo de amenazas, y a partir de allí se podrá desarrollar los procedimientos de seguridad con un foco preciso.

Los mecanismos básicos de seguridad, sin importar que tecnología sea utilizada, son los siguientes:

- ✓ Autenticación
- ✓ Autorización
- ✓ Administración
- ✓ Auditoría y registración
- ✓ Mantenimiento de la integridad de los datos

Cualquiera de los cinco mecanismos son llevados a cabo por medio del uso de técnicas de seguridad, las cuales sí van a depender de la tecnología utilizada. A medida que las nuevas tecnologías permiten el uso de herramientas (para soporte del negocio) más

complejas, es necesario desarrollar nuevas técnicas de seguridad que nos ayuden a controlar nuestros datos.

2.4. MECANISMOS BÁSICOS DE SEGURIDAD

2.4.1. AUTENTICACIÓN

Autenticación es la verificación de la identidad del usuario, generalmente cuando ingresamos al sistema o a la red, o accedemos a una base de datos.

Típicamente para ingresar a un sistema se utiliza una contraseña, sin embargo cada vez más se están utilizando otras técnicas que otorgan mayores beneficios desde el punto de vista de la seguridad. Es posible autenticarse, básicamente, de tres maneras:

Por lo que uno sabe (una contraseña).
Por lo que uno tiene (una tarjeta magnética).
Por lo que uno es (las huellas digitales).
La utilización de más de un método a la vez aumenta la seguridad de que la autenticación sea correcta. Aún cuando la utilización conjunta es cada vez más utilizada por las empresas, la decisión adoptada debe ir de la mano con el valor de la información a proteger.

Diariamente se desarrollan nuevas, más exactas y más baratas técnicas de autenticación, impulsadas por el desarrollo tecnológico en general y por la creciente necesidad de seguridad de la información.

En primera instancia, dado que es la técnica más utilizada y no siempre de manera adecuada, nos referiremos a la autenticación mediante contraseñas.

La fortaleza del método está determinada por las características de la contraseña. Cuanto más grande y difícil de adivinar esta sea, más difícil será de burlar el mecanismo. A su vez la contraseña debe ser confidencial, y esto es muy importante. No puede ser conocida por nadie más que el usuario.

Muchas veces sucede que los usuarios se prestan las contraseñas o se apuntan las mismas en un papelito pegado en el escritorio fácilmente legible por cualquier otro empleado, comprometiendo a la empresa y a nosotros mismos, dado que toda acción que se realice con esa contraseña es responsabilidad nuestra.

Para lograr que la contraseña sea difícil de adivinar, esta debe tender lo más posible a un conjunto de caracteres (con minúsculas, mayúsculas y números) inteligible. Lo que sucede es que los usuarios difícilmente recuerdan contraseñas tan elaboradas y utilizan palabras previsibles (el nombre, el apellido, el nombre de usuario, el mes en curso, el nombre de la esposa, el nombre del cuadro de fútbol), que facilitan la tarea de quién desea ingresar al sistema de forma no autorizada.

Como medida complementaria se debe obligar al cambio de contraseña de manera periódica (30 –45 días), impidiendo el uso de contraseñas utilizadas en el pasado.

2.4.2. **AUTORIZACIÓN**

Autorización es el proceso de determinar qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la empresa. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se esté protegiendo.

Las autorizaciones pueden hacerse efectivas por medio de una firma en un formulario o por medio del ingreso de una contraseña específica en el sistema, es importante que quede registrada para ser controlada posteriormente.

Al nivel de datos, las autorizaciones son instrumentadas de manera de asegurar la confidencialidad e integridad, así sea otorgando o denegando el acceso a la posibilidad de leer, modificar, crear o borrar los mismos.

La autorización debe ser otorgada siempre de acuerdo a la necesidad de saber, o sea el acceso a cierto recurso se le otorgará al usuario si es indispensable para la realización de su trabajo, y si no se le negará. Es posible otorgar autorizaciones transitorias o modificar las anteriormente otorgadas a medida que las necesidades de ese usuario varíen.

2.4.3. **ADMINISTRACIÓN**

La administración incluye los procesos de definir, mantener y eliminar las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema. Esta administración de la seguridad es un esfuerzo constante porque los negocios se encuentran en permanente cambio dentro de la empresa, lo que repercute en sus sistemas y usuarios.

Cada uno de los sistemas operativos de redes conocidos (Windows NT, Novell) cuenta con un módulo de administración de seguridad, pero igualmente existe software específico para realizar esta tarea.

2.4.4. AUDITORÍA Y REGISTRACIÓN

Llamamos auditoría al proceso de recolectar información y analizarla, que permite a los administradores u otros especialistas verificar que las técnicas de autenticación y

autorización empleadas se realizan según lo establecido y se cumplen los objetivos fijados por la empresa.

Registrar es el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda asentado en una base de eventos que permite su posterior análisis.

Monitorear la información registrada o auditar, se puede realizar mediante medios manuales o automáticos, y con una periodicidad acorde a la criticidad de la información protegida y al nivel de riesgo. Es evidente que el hecho de registrar los eventos, por sí solo, no brinda ninguna utilidad.

Los registros pueden ser usados por más de una persona, para realizar chequeos de rutina o para constatar hechos individuales, entre los que podemos citar administradores, auditores internos y externos, consultores y gobierno.

2.4.5. **MANTENIMIENTO DE LA INTEGRIDAD**

Mantener la información íntegra refiere a los procedimientos establecidos para evitar o controlar que los archivos permanezcan sin sufrir cambios no autorizados y que la información enviada desde un punto llegue a destino inalterada. El mantenimiento de la integridad también involucra la prevención de cambios accidentales, lo cual generalmente se maneja por medio de códigos de manejo de errores.

Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos, podemos citar: uso de antivirus, encriptación y funciones “hash”.

2.5. ISO/IEC 27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Fue publicada en Ecuador como NTE INEN-ISO/IEC 27002:2009 desde el 4 de Mayo del 2007. Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002) o Perú (como ISO 17799; descarga gratuita).

Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación en 2012.

Una breve descripción de los ítems que componen esta norma se cita a continuación:

A. Introducción: conceptos generales de seguridad de la información y SGSI.

B. Campo de aplicación: se especifica el objetivo de la norma.

C. Términos y definiciones: breve descripción de los términos más usados en la norma.

D. Estructura del estándar: descripción de la estructura de la norma.

E. Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

F. Política de seguridad: documento de política de seguridad y su gestión.

G. Aspectos organizativos de la seguridad de la información: organización interna; terceros.

H. Gestión de activos: responsabilidad sobre los activos; clasificación de la información.

I. Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

J. Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

K. Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

L. Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

M. Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

N. Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.

O. Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

P. Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

Bibliografía: normas y publicaciones de referencia.

Índice

2.6. ISO/IEC 27005:2008 TECNOLOGÍAS DE LA INFORMACIÓN TÉCNICAS DE SEGURIDAD GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Publicada el 4 de Junio de 2008. La norma ISO/IEC 27005:2008 sirve de complemento a las dos primeras normas de la familia ISO/IEC 27001:2005 e ISO/IEC 27002:2005, que como hemos visto, definen la necesidad de elaborar un análisis de riesgos pero no especifican directrices para ello.

Está basada en los informes técnicos ISO/IEC TR 13335-3:1998 [ISO13335-3.98] e ISO/IEC TR 13335-4:2000 [ISO13335-4.00], que quedaron obsoletos desde su publicación. Se basa también en la norma BS 7799-3:2006 [BS7799-3.06].

Su versión traducida al español está en países como México (NMX-I-041/05-NYCE), Chile (NCh-ISO27005) o Colombia (NTC-ISO-IEC 27005).

El proceso de gestión de riesgos de la norma ISO27005.08 se describe en las siguientes 6 cláusulas:

Cláusula 7 Establecimiento del contexto, en la que se definen los objetivos, el alcance y la organización para todo el proceso.

Cláusula 8 Valoración de riesgos, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:

- ✓ Identificación de riesgos, que consiste en determinar qué puede provocar pérdidas a la Organización.
- ✓ Estimación de riesgos, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las políticas.
- ✓ Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Cláusula 9 Tratamiento de riesgos, en la que se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

Cláusula 10 Aceptación de riesgos, en la que se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado.

Cláusula 11 Comunicación de riesgos, en la que todos los grupos de interés intercambian información sobre los riesgos.

Cláusula 12 Monitorización y revisión de riesgos, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

El proceso de gestión de riesgos definido por la norma ISO/IEC 27005:2008 puede resumirse en al siguiente gráfica:

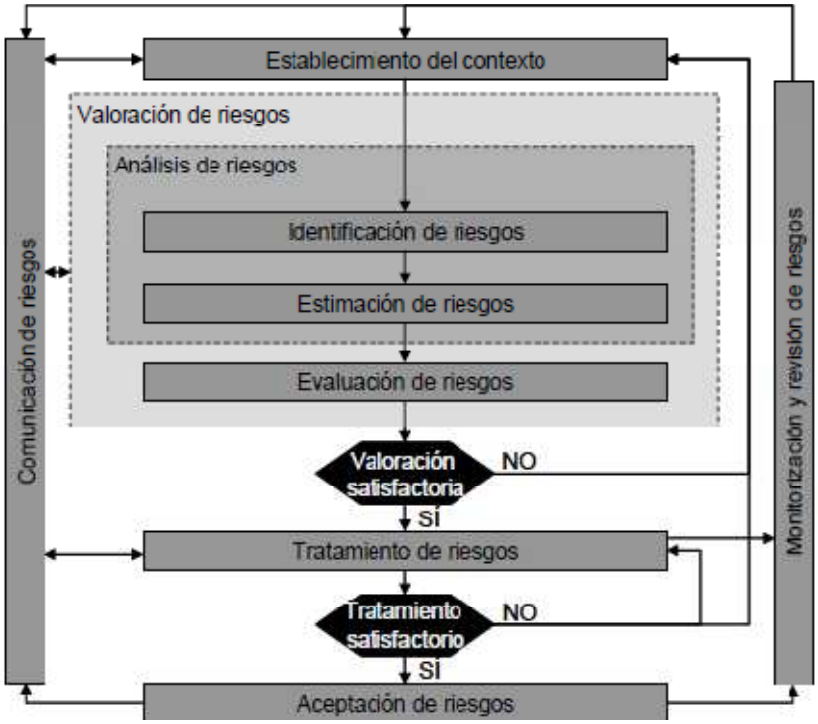


Figura II.1. Proceso de Gestión de Riesgos de Seguridad de la Información de ISO/IEC 27005:2008

En línea con el estándar ISO/IEC 27001:2005, el proceso de gestión de riesgos se considera iterativo, siguiendo el ciclo de Deming:

Tabla II.3. Ciclo Deming

Ciclo de Deming	**Proceso de gestión de riesgos de seguridad de la información**
Planificar	Establecimiento del contexto Valoración de riesgos Desarrollo del plan de tratamiento de riesgos Aceptación de riesgos
Hacer	Implantación del plan de tratamiento de riesgos
Verificar	Monitorización y revisión continua de riesgos
Actuar	Mantenimiento y mejora del proceso de gestión de riesgos de seguridad de la información

2.7. UNE 71504:2008 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Metodología adoptada en España, desarrollada por el comité técnico AEN/CTN 71 Tecnología de la información, de AENOR[2] [UNE71504.08].

El proceso de gestión de riesgos que define consta de las siguientes fases principales:

- ✓ Método de análisis
    - o Tareas preparatorias
    - o Caracterización de procesos
    - o Identificación de los procesos relevantes
    - o Identificación de relaciones entre los procesos
    - o Valoración de los procesos
    - o Caracterización de las amenazas
    - o Identificación de las amenazas relevantes
    - o Valoración de la vulnerabilidad de los activos ante las amenazas
    - o Cálculo del riesgo intrínseco
    - o Caracterización de las políticas
    - o Determinación de las políticas adecuadas
    - o Valoración de las políticas
    - o Cálculo del riesgo efectivo
- ✓ Evaluación de riesgos
- ✓ Tratamiento de riesgos
    - o Definición del plan de seguridad
    - o Aprobación del plan de seguridad
- ✓ Administración de la gestión de riesgos

---

[2] Asociación Española de Normalización y Certificación.

2.8. MAGERIT – Metodología de Análisis y Gestión de Riesgos de IT

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Administraciones Pública [MAGE06].

La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 2.0, publicada en 2006.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública Española.

Dispone de una herramienta de soporte, PILAR II (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

La metodología consta de tres volúmenes:

Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.

Volumen II – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:

- ✓ Dimensiones y criterios de valoración
- ✓ Amenazas
- ✓ Tipos de activos
- ✓ Tipos de recursos de Información
- ✓ Políticas

Volumen III – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:

- ✓ Técnicas específicas para el análisis de riesgos:
  - o Análisis mediante tablas
  - o Análisis algorítmico
  - o Árboles de ataque
- ✓ Técnicas generales
  - o Análisis coste-beneficio
  - o Diagramas de flujo de datos (DFD)
  - o Diagramas de procesos
  - o Técnicas gráficas
  - o Planificación de proyectos
  - o Sesiones de trabajo: entrevistas, reuniones y presentaciones
  - o Valoración Delphi

La metodología MAGERIT se puede resumir gráficamente de la siguiente forma:

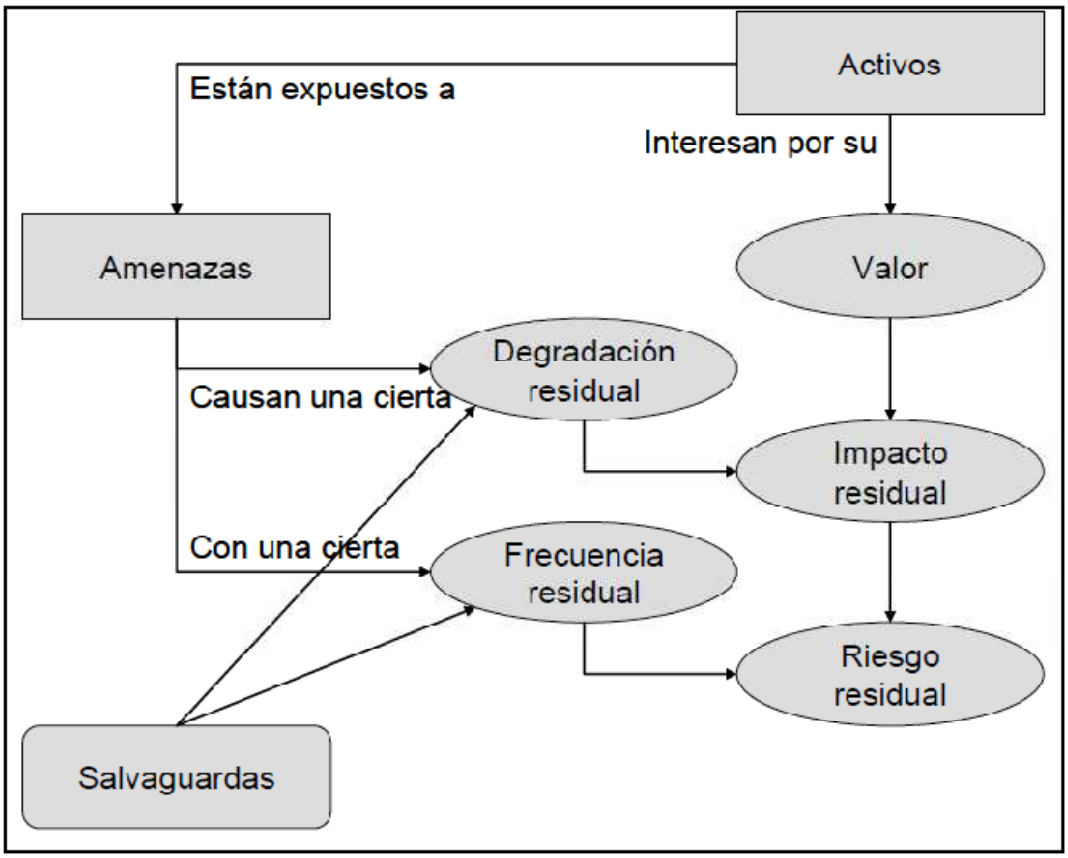


Figura II.2. Modelo MAGERIT

2.9. SISTEMAS DE PREVENCION DE INTRUSOS

2.9.1. ANTECEDENTES

Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Tiempo después, algunos IPS fueron comercializados por la empresa One Secure, la cual fue finalmente adquirida por NetScreen Technologies, que a su vez fue adquirida por Juniper Networks en 2004. Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación.

2.9.2. DEFINICIÓN

Un Sistema de Prevención de Intrusos (IPS) es un mecanismo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión o evolución de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

2.9.3. FUNCIONAMENTO

Un Sistema de Prevención de Intrusos, al igual que un Sistema de Detección de Intrusos, funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso, usuario que activó algún sensor, mientras que un Sistema de Prevención de Intrusos establece políticas de

seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Un IPS puede inspeccionar los flujos de datos con el fin de detectar los ataques que pueden ser explotados mediante vulnerabilidades desde el nivel 2, control de acceso del modelo OSI hasta la capa 7, la de aplicación; por el contrario, los cortafuegos convencionales, como se limitan a realizar inspecciones a nivel 3 o nivel 4, son incapaces de detectar los ataques al nivel de aplicación escondidos dentro de la carga de los paquetes.

Una característica importante es la de la inspección a fondo, en la cual los paquetes pueden ser clasificados y analizados en su totalidad mediante todos los filtros que posee.

Esa clasificación de paquetes se basa en la conocida configuración de cabecera de los paquetes, direcciones origen y destino, etc.

Si hablamos de los filtros que posee podemos decir que están formados por un conjunto de reglas que definen determinadas condiciones que son necesarias cumplirse para informar si un paquete es o no es dañino.

Lo bueno de los IPS es que no solo detectan la vulnerabilidad sino que mediante el Análisis de Protocolo, lo transforma en algo así como un sistema inteligente, el cual permite detectar y tomar acciones sobre una vulnerabilidad que todavía no ha sido anunciada.

Para resumir el funcionamiento de un IPS podemos señalarlo con 4 puntos fundamentales:

El paquete que entra es clasificado por la cabecera y la información de flujo que se asocia.

Según la función de cómo se clasifique el paquete, se aplicaran determinados filtros.

Los filtros relevantes se aplican en paralelo, y si hay un positivo, se etiqueta como sospechoso.

Si es sospechoso, se desecha y se actualiza la base de estado sobre el flujo relacionado para descartar restos de dicho flujo entrante.

2.9.4. **SISTEMA DE PREVENCIÓN DE INTRUSOS SNORT**

Snort es un IDS y desde su versión 2.3.0 también tiene funciones de IPS gracias a la incorporación de la modalidad *Snort inline*. El iniciador del proyecto fue Martin Roesch, quien desarrolló la primera versión completamente en lenguaje C. Snort es gratuito y de código abierto bajo la licencia GPL de GNU. Actualmente el proyecto está respaldado por la empresa SourceFire fundada por el mismo Roesch, la cual fue comprada en el 2005 por la multinacional Checkpoint.

Snort se apoya en un conjunto de reglas donde se tipifican patrones de ataques de los que se tiene clara certeza acerca de su funcionamiento, sobre estas reglas se basa para alertar en el caso de que algún evento que encaje dentro de esos patrones se produzca en la red que está monitoreando. Dichas reglas pueden ser construidas por el usuario lo cual le da un perfil personalizado a la protección de la red.

FUNCIONAMIENTO DE SNORT

Snort tiene cuatro modos de funcionamiento a saber, **Sniffer:** sólo monitorea el tráfico de la red y lo muestra en pantalla. **Packet Logger:** Guarda los paquetes en archivos planos o binarios. **NIDS:** De acuerdo a ciertos parámetros de configuración, alerta y/o

registra los eventos que deben ser verificados posteriormente por el administrador. **Inline:** Puede impedir el paso de paquetes según los parámetros de configuración.

En el modo IPS, cuando Snort recibe un paquete lo hace pasar por diferentes módulos encargados de funciones específicas de decodificación, análisis y generación de reportes.

Las funciones de cada módulo se describen a continuación:

DECODIFICADOR

Encaja los paquetes capturados dentro de estructuras de datos predefinidas e identifica los protocolos de capa de enlace. Luego, sube de nivel, decodifica IP y seguidamente TCP o UDP según sea el caso para obtener información como puertos y direcciones. Snort alertará si encuentra encabezados malformados, opciones TCP de longitudes inusuales o poco usadas.

PREPROCESADORES

Estos son módulos software que dan gran libertad a los programadores para realizar diversos procesamientos con los paquetes capturados. Existen preprocesadores que realizan tareas como re ensamblar paquetes IP, segmentos TCP, realizar seguimiento detallado de conexiones establecidas, detectar ataques a través de la inspección de HTTP y muchas otras funciones útiles.

ARCHIVOS DE REGLAS

Archivos de texto plano donde se encuentra un listado de reglas en una sintaxis definida. Dentro de esta sintaxis se especifica el protocolo, las direcciones y los plug-ins de detección, entre otras cosas. Estos archivos de reglas se actualizan periódicamente de forma similar a como se hace con los archivos de definiciones de un antivirus.

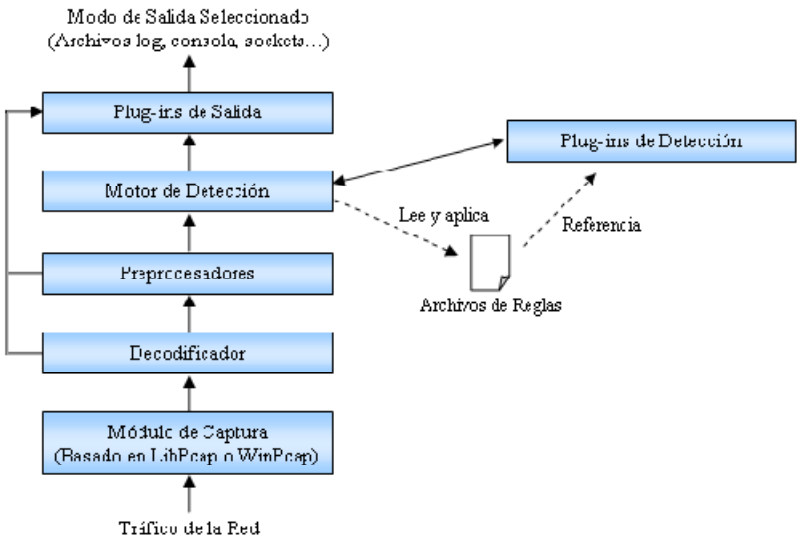


Figura II.3. Componentes de IPS Snort.

PLUG-INS DE DETECCIÓN

Módulos que son referenciados desde su definición en el archivo de reglas y sirven para identificar patrones cuando alguna de ellas es evaluada.

MOTOR DE DETECCIÓN

Haciendo uso de los plug-ins de detección, evalúa los paquetes con las reglas que se han cargado en memoria desde la inicialización del IDS.

PLUG-INS DE SALIDA

Formatean las notificaciones (alertas, logs) para que puedan ser guardadas con diferentes mecanismos (archivos binarios, archivos en texto plano, bases de datos, etc.)

El crecimiento y optimización de Snort se ha facilitado en gran parte gracias a esta arquitectura modular, la cual ha permitido que los miembros de la comunidad de desarrolladores añadan nuevos preprocesadores o plug-ins sin tener que preocuparse por el resto del sistema.

CAPÍTULO III

MARCO METODOLÓGICO E HIPOTÉTICO

3.1. VALIDACIÓN DE INSTRUMENTOS UTILIZADOS

Para la implementación del Sistema de Prevención de Intrusos se vio necesaria la utilización de distintas herramientas de gestión basadas en software, cuya finalidad principal fue lograr el correcto funcionamiento de la aplicación final.

A continuación se detalla la validación del uso de cada una de las herramientas utilizadas.

3.1.1. CENTOS 5.3

Figura III.4. Logo de CentO5

CentOS (**C**ommunity **ENT**erprise **O**perating **S**ystem) es un clon a nivel binario de la distribución Linux Red Hat Enterprise Linux **RHEL**, compilado por voluntarios a partir del código fuente liberado por Red Hat. Esta distribución de Linux es gratuita. Sus creadores aseguran que es compatible 100% con el sistema de Red Hat y su amplia

base de usuarios corporativos la avalan como una de las alternativas libres más profesionales, así consta en las paginas www.linux-magazine.es, www.espaciolinux.com y www.centos.org es por esta razón que se escogió Centos para realizar un Sistema de Prevención de Intrusiones en el IMR ya que se montó un servidor con características corporativas que necesita estabilidad para su funcionamiento durante la ejecución del proyecto.

3.1.2. **SNORT**

Figura III.5. Logo de Snort

Se decidió utilizar este software puesto que luego de una investigación profunda sobre este y otro software aplicable al desarrollo de un IPS, se concluyo que Snort es la herramienta que ofrece mayores funcionalidades. Cabe además indicar otras ventajas que se citan en varios sitios del internet, entre ellos tenemos: www.snort.org, www.sourcefire.com y www.snort-inline.sourceforge.net; de todas las ventajas mencionadas en estos sitios se menciona las que a nuestro parecer son las más importantes: Snort es un Sniffer de paquetes y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus alertas tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Snort es una herramienta de código abierto para administradores de sistemas que permite realizar un análisis en tiempo real del tráfico de nuestra red IP y que tiene como objetivo la prevención de intrusos y el registro de paquetes.

Snort proporciona una selección de reglas de filtrado para el tráfico no deseado. La mayoría de las reglas de Snort son de fácil comprensión y modificación.

3.1.3. **APACHE**

Figura III.6. Logo de Apache

En la implementación del Sistema de Prevención de Intrusos se utilizó este servidor Web ya que es un paquete de fácil instalación y configuración en la distribución Cento5, las características principales de este servidor web según sitios del internet visitados como son: www.ecualug.org y www.apache.org son las que se detallan a continuación:

Es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP y la noción de sitio virtual.

Apache presenta la capacidad de tener código abierto y ser configurable para la aplicación de bases de datos que se utilizó en el proyecto con la ayuda de MySQL.

Apache tiene amplia aceptación en la red: desde 1996, es el servidor HTTP más usado, alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, es esta otra de las razones por las que se utilizó

Apache en el proyecto para la visualización de BASE y las alertas en la página de aplicación.

3.1.4. **BASE**

Según la página oficial de BASE http://base.secureideas.net/ indica que BASE es el reemplazo de la consola de análisis llamada ACID (Consola de Análisis para Bases de Datos de Intrusiones) y está construida sobre esta última.

BASE es una aplicación Web hecha en PHP que permite analizar los logs y las alertas generadas por Snort de una forma más amigable. Surgió debido a la dificultad de analizar los cientos de alertas que se generan en redes con alto tráfico. Entre las facilidades que ofrece BASE, y que se convirtieron en los aspectos considerados para su uso en el proyecto, están: la opción de hacer búsquedas de alertas especificas, observar de una forma grafica los paquetes capturados y la generación de graficas estadísticas.

Al ser esta una evolución de ACID, se opto su utilización para la visualización de resultados en la herramienta utilizada.

3.1.5. **MySQL**

Figura III.7. Logo de MySQL

Se decidió y creyó necesario la utilización de este gestor de Base de Datos por el principal motivo de administrar adecuadamente las amenazas o riesgos que detecta el

IPS; luego de un análisis se tomó en cuenta las siguientes características generales de MySQL citadas en el foro http://forums.mysql.com/read.php?71,101916,101916 y son:

Es un gestor de base de datos sencillo de usar e increíblemente rápido; es uno de los motores de base de datos más usados en Internet, la principal razón de esto es que es gratis para aplicaciones no comerciales.

Posibilidad de crear y configurar usuarios, asignando a cada uno de ellos permisos diferentes.

Facilidad de exportación e importación de datos, incluso de la base de datos completa. Posibilidad de ejecutar conjuntos de instrucciones guardadas en ficheros externos a la base de datos.

La creación y gestión de Bases de Datos en MySQL para la implementación de un IPS es fácil y sencilla según manuales que se descargaron gracias al fácil acceso a distintas páginas tales como www.webestilo.com, www.mysql-hispano.org, etc.

3.1.6. **PHP 5.2**

Figura III.8. Logo de Php

Para la generación de la página Web en la que se visualiza todas las alertas con sus respectivos detalles se descargó y compiló Php para su correcto funcionamiento gracias a la ayuda de sitios Web encontrados como son los siguientes: www.php.net, http://php.net/downloads.php, etc.

Estos Sitios Web certifican a Php como una de las mejores herramientas utilizadas para la visualización y configuración de páginas, las características encontradas en estas direcciones son:

Es un lenguaje de script interpretado en el lado del servidor utilizado para la generación de páginas Web dinámicas, similar al ASP de Microsoft o el JSP de Sun, embebido en páginas HTML y ejecutado en el servidor.

La mayor parte de su sintaxis ha sido tomada de C, Java y Perl con algunas características específicas de sí mismo. La meta del lenguaje es permitir rápidamente a los desarrolladores la generación dinámica de páginas.

3.1.7. **DEPENDENCIAS**

Snort In Line necesita de ciertas librerías adicionales, que toman el nombre de dependencias y que son necesarias para la correcta instalación del software mencionado, se describen a continuación las dependencias usadas:

- ✓ IPTABLES-DEV

Conjunto de reglas de filtrado de paquetes de Linux.

- ✓ LIBDNET

Interfaz con varias rutinas de red de bajo nivel incluyendo:
Manipulación de direcciones de red.
Cortafuegos de red.
Búsqueda y manipulación de interfaces de red.
Transmisión de tramas Ethernet.

- ✓ LIBPCAP

Pcap es una interfaz de una aplicación de programación para captura de paquetes. La implementación de Pcap para sistemas basados en Unix se conoce como LibPcap; para Windows la librería de LibPcap recibe el nombre de WinPcap.

El LibPcap y WinPcap pueden ser utilizados por un programa para capturar los paquetes que viajan por toda la red y, en las versiones más recientes, para transmitir los paquetes en la capa de enlace de una red, así como para conseguir una lista de los interfaces de red que se pueden utilizar con el LibPcap o WinPcap.

El LibPcap y WinPcap son la captura del paquete y los motores de filtración de muchas herramientas de código abierto y comerciales de la red, incluyendo analizadores de protocolo, monitores de la red, sistemas de detección de intrusos en la red, programas de captura de las tramas de red (Packet Sniffer), generadores de tráfico y puesta a punto de la red.

3.2. COMPROBACIÓN DE LA HIPOTESIS

El estudio realizado sobre la implementación de la metodología de prevención de intrusos para la red corporativa del M.I. Municipio de Riobamba y el análisis de los resultados obtenidos antes y luego de su aplicación permitieron comprobar que la implementación de dicha metodología mejoró la seguridad de la información privada que la entidad maneja.

Esta comprobación se la confirma con la aplicación del método ponderado simple, debiendo para esto, asignar valores numéricos según la efectividad que tienen las políticas sobre las amenazas detectadas, para lograrlo se ha realizado un análisis cualitativo que se detalla así:

Se debió indicar los niveles de seguridad en los que se basa la conclusión final, estos valores están determinados por un incremento lineal y dividido en intervalos iguales, para cada intervalo se presenta el aspecto principal y su grado de consideración a nivel de red.

Tabla. III.4. Niveles de Seguridad.

Nivel de Seguridad (%)	Aspectos	Consideración
0-25	No presenta políticas de seguridad	**Inaceptable**
26-50	Presenta pero no son las adecuadas	**Poco Aceptable**
51-75	Presenta algunas políticas aceptables pero necesita de otras	**Medianamente Aceptable**
76-100	La mayoría de las políticas son adecuadas sin decir que se llego a la excelencia.	**Aceptable**

Luego se realizó una valoración de la efectividad de las políticas sobre una escala de 5 valores:

No existe: Ninguna política está implementada para una determinada amenaza.

Sin efecto La política no tiene ningún impacto sobre la amenaza.

Poca efectividad: La política tiene un impacto indirecto o general sobre la amenaza.

Efectivo: La política reduce la frecuencia o el impacto de la amenaza de forma significativa.

Muy efectivo: Política específicamente diseñada para la amenaza.

Se ha asignado un valor numérico a cada nivel de la escala para permitir el uso de los cálculos cuantitativos. Cabe indicar que se usó para este fin una gráfica exponencial adecuada a una calificación del 0 al 100 por ciento para cinco niveles aplicativos (Ver Anexo 2); de lo citado se extrajeron los siguientes valores numéricos.

Tabla III.5. Valoración de la Efectividad de las Políticas

IMPACTO	VALORES DE LA EFECTIVIDAD (%)
No Existe	**0**
Sin Efecto	**15**
Poco Efectiva	**30**
Efectiva	**60**
Muy Efectiva	**100**

Cabe indicar que la tabla anterior será la base para asignar los valores cuantitativos a cada amenaza, las amenazas tomarán un valor porcentual según si posee o no una política de seguridad y según la efectividad de la misma, si la tuviese.

Este análisis se lo hace antes y después de aplicar la metodología propuesta con el fin de determinar el incremento o decremento del nivel de seguridad.

- ✓ **Nivel de Seguridad Antes de Implementar la Metodología**

El valor promedio de la efectividad de las políticas sobre las amenazas detectadas más la efectividad de las políticas ya existentes e implantadas por el propio departamento de sistemas del IMR, permite obtener el valor porcentual del Nivel de Seguridad de la Red antes de la implementación de la política.

Se detallan estos valores a través de la siguiente tabla:

Tabla III.6. Valoración de Políticas Sobre Amenazas Detectadas. Situación Inicial

Amenaza	Efectividad de las políticas de Seguridad						
	Aspecto Considerado en el IMR	No existe	Sin Efecto	Poco Efectiva	Efectiva	Muy Efectiva	Funcionalidad (%)
Fallo de Servicio de Comunicaciones	✓ Fallas del proveedor de internet CNT. ✓ Caída de la red de datos interna por fallas de energía en switchs y desconexión de cables de red.		**X**				15
Incumplimiento legal	Sin Licencia: ✓ Windows 98 ✓ Windows 2000 ✓ Windows XP ✓ Windows Vista ✓ Windows 2003 server			**X**			30
Error de los usuarios	✓ Eliminación de archivos de sistema. ✓ Desconfiguración de Impresoras.			**X**			30
Caída del sistema	✓ Procesadores no actualizados. ✓ Memoria RAM de baja capacidad. ✓ Almacenamiento en discos duros.		**X**				15
Error de los Administradores de Red	✓ Actualización de antivirus. ✓ Falla mantenimiento de computadoras. ✓ Mala configuración de Kypus		**X**				15
Error de Monitorización	✓ La Entidad no posee ningún Sniffer	**X**					0
Difusión de software dañino	✓ Instalación de Sw. sin licencia. ✓ No escaneo de flash memory.			**X**			30
Vulnerabilidades de Programas	✓ Desbordamiento de Buffer de Oracle			**X**			30
Error de mantenimiento (Software)	✓ Falla en el formateo de PCs			**X**			30
Exceso Trafico Multimedia	✓ Acceso a páginas de entretenimiento. ✓ Descarga de archivos de audio. ✓ Acceso a Windows Messenger.			**X**			30
Ataque en la Red	✓ Escaneo de Puertos. ✓ Utilidad Ping.	**X**					0
TOTAL EFECTIVIDAD DE POLÍTICAS SOBRE AMENAZAS DETECTADAS							225

Tabla III.7. Valoración de Políticas Existentes.

Políticas ya implementadas	Efectividad				
	Sin Efecto	Poco Efectiva	Efectivo (%)	Muy Efectivo (%)	Funcionalidad
Protección de Antivirus			**X**		**60**
Distribución de Ancho de Banda				**X**	**100**
Horarios de uso para conexión de Internet				**X**	**100**
Administración de grupos de usuarios				**X**	**100**
Distribución adecuada de los equipos de Interconexión			**X**		**60**
Ubicación ambiental de Servidores, Firewall y Modem CNT				**X**	**100**
Uso adecuado de Proxy			**X**		**60**
TOTAL EFECTIVIDAD DE POLÍTICAS EXISTENTES					**580**

Se diferencian claramente once amenazas detectadas y siete políticas existentes.

La suma total de los niveles de funcionalidad en ambas tablas es de 805 lo que promedia 44.7% que equivale a UN NIVEL DE SEGURIDAD ANTES DE IMPLEMENTAR LA METODOLOGÍA DE 45%. Se detallan los cálculos a continuación.

Tabla.III.8. Efectividad Políticas. Situación Inicial

Efectividad de Políticas sobre Amenazas Detectadas	**225**
Efectividad de Políticas Existentes	**580**
TOTAL EFECTIVIDAD POLITICAS EN LA RED	**805**

Tabla. III.9 Total Amenazas

Número de Amenazas Detectadas	**11**
Número de Amenazas que ya Posee una Política de Seguridad	**7**
TOTAL AMENAZAS	**18**

$$\textbf{NIVEL DE SEGURIDAD} = \frac{\boldsymbol{TOTAL\ EFECTIVIDAD\ DE\ POLITICAS\ EN\ LA\ RED}}{\boldsymbol{TOTAL\ AMENAZAS}}$$

$$\textbf{NIVEL DE SEGURIDAD} = \frac{805}{18} = \textbf{45\%}$$

- ✓ **Nivel de Seguridad Después de Implementar la Metodología**

El valor promedio de la efectividad de las políticas sobre las amenazas detectadas varía considerablemente luego de aplicar la metodología lo que nos hace predecir un incremento en los niveles de seguridad, a continuación se detalla la tabla que muestra dichos valores.

Tabla III.10. Valoración de Políticas Sobre Amenazas Detectadas Situación Actual.

Amenaza	Efectividad de las políticas de Seguridad sobre Amenazas Detectadas					
	Aspecto Considerado en el IMR	**Sin Efecto**	**Poco Efectiva**	**Efectiva**	**Muy Efectiva**	**Funcionalidad (%)**
Fallo de Servicio de Comunicaciones	✓ Fallas del proveedor de internet CNT. ✓ Caída de la red de datos interna por fallas de energía en switchs y desconexión de cables de red.	**X**				15
Incumplimiento legal	Sin Licencia: ✓ Windows 98 ✓ Windows 2000 ✓ Windows XP ✓ Windows Vista ✓ Windows 2003 server			**X**		60
Error de los usuarios	✓ Eliminación de archivos de sistema. ✓ Desconfiguración de Impresoras.			**X**		60
Caída del sistema	✓ Procesadores no actualizados. ✓ Memoria RAM de baja capacidad. ✓ Almacenamiento en discos duros.	**X**				15
Error de los Administradores de Red	✓ Actualización de antivirus. ✓ Falla mantenimiento de computadoras. ✓ Mala configuración de Kypus			**X**		60
Error de Monitorización	✓ La Entidad no posee ningún Sniffer			**X**		60
Difusión de software dañino	✓ Instalación de Sw. sin Licencia. ✓ No escaneo de flash memory.		**X**			30
Vulnerabilidades de Programas	✓ Desbordamiento de Buffer de Oracle				**X**	100
Error de mantenimiento (Software)	✓ Falla en el formateo de PCs		**X**			30
Exceso Trafico Multimedia	✓ Acceso a páginas de entretenimiento. ✓ Descarga de archivos de audio. ✓ Acceso a Windows Messenger.				**X**	100
Ataques en la Red	✓ Escaneo de Puertos. ✓ Utilidad Ping.				**X**	100
TOTAL EFECTIVIDAD DE POLÍTICAS SOBRE AMENAZAS DETECTADAS						690

Para calcular el nuevo nivel de seguridad de la Red se considera nuevamente el valor de efectividad de las políticas existentes, señalado en la Tabla III.7 pues se debe considerar que se hizo un estudio del nivel de seguridad total, no solo de las amenazas detectadas. A este total se le sumó el nuevo valor de Efectividad de Políticas calculado en la tabla III.10 obteniéndose los siguientes resultados.

Tabla.III.11. Efectividad Políticas. Situación Actual

Efectividad de Políticas sobre Amenazas Detectadas	**690**
Efectividad de Políticas Existentes	**580**
TOTAL EFECTIVIDAD POLITICAS EN LA RED	**1270**

La tabla III.7 no sufre ninguna modificación puesto que las amenazas detectadas siguen siendo las mismas; utilizando los valores actuales tenemos el siguiente cálculo:

$$\textbf{NIVEL DE SEGURIDAD} = \frac{TOTAL\ EFECTIVIDAD\ DE\ POLITICAS\ EN\ LA\ RED}{TOTAL\ AMENAZAS}$$

$$\textbf{NIVEL DE SEGURIDAD} = \frac{1270}{18} = \textbf{70\%}$$

Con estos resultados se concluye que se mejoró el nivel de seguridad de la red en un 25%, lo que permitió que se ascendiera de un nivel Poco aceptable en seguridad a un nivel Aceptable. Quedando comprobada la hipótesis y afirmando que se la logró cumplir.

CAPÍTULO IV

MARCO PROPOSITIVO

4.1. ESTUDIO COMPARATIVO DE LAS NORMAS Y METODOLOGÍAS CITADAS.

Luego de mencionar en el capítulo dos las normas y metodologías que sirvieron de guía para el proyecto, se creyó necesario realizar un estudio más detallado de cada una, basado en el análisis FODA, lo que permitió destacar los aspectos más adecuados, que formarían parte de la metodología de prevención de intrusos a diseñar.

Cabe indicar que, en el presente proyecto se contempla al término PREVENCIÓN DE INTRUSOS como un todo, que abarca tanto al análisis como a la gestión de riesgos, pues se afirma El concepto de prevención de intrusos enmarca dos grandes aspectos: el de Análisis de Riesgos y el de La Gestión de Riesgos, pues es claro que si no se determina de lo que se debe proteger, difícilmente se logrará un nivel de prevención certero, pues no se podrá determinar las acciones a tomar al enfrentar una amenaza de cualquier índole.

Bajo este concepto, se decidió orientar hacia el análisis y la gestión de riesgos el estudio de las metodologías citadas.

Se presenta por cada metodología una tabla con su análisis FODA correspondiente, luego se detallan tablas comparativas sobre aspectos relevantes, para finalmente realizar una conclusión de la metodología resultante y la justificación de la elección de cada fase de la misma.

4.1.1. **ANÁLISIS DE LA NORMA ISO 27002**

Tabla. IV.12 Análisis Foda Norma ISO 27002

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Es un estándar adoptado en nuestro país por el INEN como NTE ISO/IEC 27002:2009	Es un estándar internacional, lo que la faculta mayor aceptación.	Tiene un alcance pobre en el ámbito del análisis de riesgo	No es certificable.
Presenta un alcance amplio en la gestión de riesgos.	Modificación completa con herramientas de edición estándar HTML, fácil conversión a otros estilos	No tiene como objetivos de seguridad la trazabilidad.	
Señala la posibilidad de determinar un objetivo específico de la norma, para una mejor comprensión.			
Proporciona una guía de consideraciones(controles) a tener en cuenta para y un conjunto de "sugerencias" para cada uno de esos controles			
Fácil de adaptar a un plan de políticas específico de una organización			
Aprovecha al máximo la funcionalidad y ventajas de ISO 27001			
Es una guía para, en distintos ámbitos, conocer qué se puede hacer para mejorar la seguridad de la información.			

4.1.2. **ANÁLISIS DE LA NORMA ISO 27005**

Tabla. IV.13. Análisis Foda Norma ISO 27005

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Es un complemento de la ISO 27001 y la ISO27002	Es un estándar internacional, lo que la faculta mayor aceptación.	No permite un análisis óptimo cuantitativo.	No posee herramientas, técnicas, ni comparativas de ayuda para su implementación
Se la considera con un alcance completo tanto en el análisis como en la gestión de riesgos	Publicación reciente de su última versión (2008)	No involucra a los procesos como elementos del modelo a seguir.	
Posee la fase de aceptación de riesgos, previa su justificación.	Posee una cláusula completa orientada a la monitorización y revisión de riesgos.		
Permite un análisis completo cualitativo.			

4.1.3. **ANÁLISIS DE LA METODOLOGÍA MAGERIT**

Tabla. IV.14. Análisis Foda Metodología Magerit.

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Se la considera con un alcance completo tanto en el análisis como en la gestión de riesgos	Dispone de una herramienta de soporte PILAR II	No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir.	No es una metodología reconocida en el Ecuador.
Posee un extenso archivo de inventarios en lo referente a Recursos de información, Amenazas y Tipos de Activos	Es una metodología líder en España, con buenos referentes de aplicación.	No posee un inventario completo en lo referente a Políticas.	
Permite un análisis completo cualitativo y cuantitativo.			

4.1.4. **ANÁLISIS DE LA METODOLOGÍA UNE 71504:2008**

Tabla. IV.15 Análisis Foda Metodología UNE 71504:2008

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS
Se la considera con un alcance completo tanto en el análisis como en la gestión de riesgos	Es una metodología líder en España, con buenos referentes de aplicación.	No permite un análisis completo cualitativo ni cuantitativo.	No es una metodología reconocida en el Ecuador.
Involucra a los procesos relevantes y su relación entre ellos como elementos del modelo a seguir.		No tiene objetivos óptimos para la seguridad en la trazabilidad y la autenticidad.	No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.
		No posee un archivo de inventarios en lo referente a Recursos de información, Vulnerabilidades, Amenazas y Políticas.	

Como un resumen de los análisis FODA se presentan las siguientes tablas que pretenden orientar las diferencias existentes entre las metodologías estudiadas.

Tabla IV.16. Análisis de Origen de Creación.

Nombre	Origen			
	Descripción	Organización	País	Año[3]
ISO/IEC 27002:2005	Tecnología de Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información	ISO International Organization for Standardization	Internacional (Suiza)	2005
ISO/IEC 27005:2008	Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información	ISO International Organization for Standardization	Internacional (Suiza)	2008
MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT	Ministerio de Administraciones Públicas	España	2006
UNE 71504:2008	Metodología de análisis y gestión de riesgos para los sistemas de información	AENOR Asociación Española de Normalización y Certificación	España	2008

[3] Se considera la fecha de publicación de la versión más reciente.

Tabla IV.17. Análisis y Gestión de Riesgos.

Nombre	Alcance Considerado	
	Análisis de Riesgos	**Gestión de Riesgos**
ISO/IEC 27002:2005	●	◑
ISO/IEC 27005:2008	●	●
MAGERIT	●	●
UNE 71504:2008	●	●

Leyenda: ● Completo ◕ Amplio ◑ Satisfactorio ◔ Pobre ○ No tiene

Tabla IV.18. Análisis Cuantitativo y Cualitativo.

Nombre	Análisis	
	Cuantitativo	**Cualitativo**
ISO/IEC 27002:2005	◑	●
ISO/IEC 27005:2008	◑	●
MAGERIT	●	●
UNE 71504:2008	◔	◔

Leyenda: ● Completo ◕ Amplio ◑ Satisfactorio ◔ Pobre ○ No tiene

Tabla IV.19. Elementos del Modelo.

Nombre	Elementos del Modelo						
	Procesos	Activos	Recursos	Dependencias	Vulnerab.	Amenazas	Políticas
ISO/IEC 27002:2005	◔	◔	◑	◑	◑	○	●
ISO/IEC 27005:2008	○	●	●	●	○	●	●
MAGERIT	○	●	○	●	○	●	●
UNE 71504:2008	○	●	○	●	○	●	●

Leyenda: ● Completo ◕ Amplio ◑ Satisfactorio ◔ Pobre ○ No tiene

Tabla IV.20. Objetivos de Seguridad.

Nombre	Objetivos de Seguridad					
	Confidencial.	Integridad	Disponibilidad	Autenticidad	Trazabilidad	Otros
ISO/IEC 27002:2005	●	●	●	◑	○	○
ISO/IEC 27005:2008	●	●	●	●	●	Fiabilidad
MAGERIT	●	●	●	●	●	○
UNE 71504:2008	●	●	●	◑	◑	◑

Leyenda: ● Completo ◕ Amplio ◑ Satisfactorio ◔ Pobre ○ No tiene

CONCLUSIÓN:

Terminado el análisis de las cuatro metodologías y respetando el concepto de Prevención de Intrusos planteado al inicio del capítulo, se decidió, adoptar la lógica

utilizada por todas las normas y metodologías, de seguir un orden secuencial informativo e instructivo.

Bajo este análisis se decidió diferenciar en la metodología dos grandes fases que a su vez se desglosan en varios ítems, los necesarios a nuestro criterio, para lograr un modelo de metodología apropiado y enmarcado a las necesidades de la red del M.I. Municipio de Riobamba.

A continuación se muestra una gráfica que resume el desarrollo de la metodología propuesta y su derivación de las otras estudiadas; posteriormente se explican las fases que componen la nueva metodología y sus relaciones con las normas y metodologías analizadas:

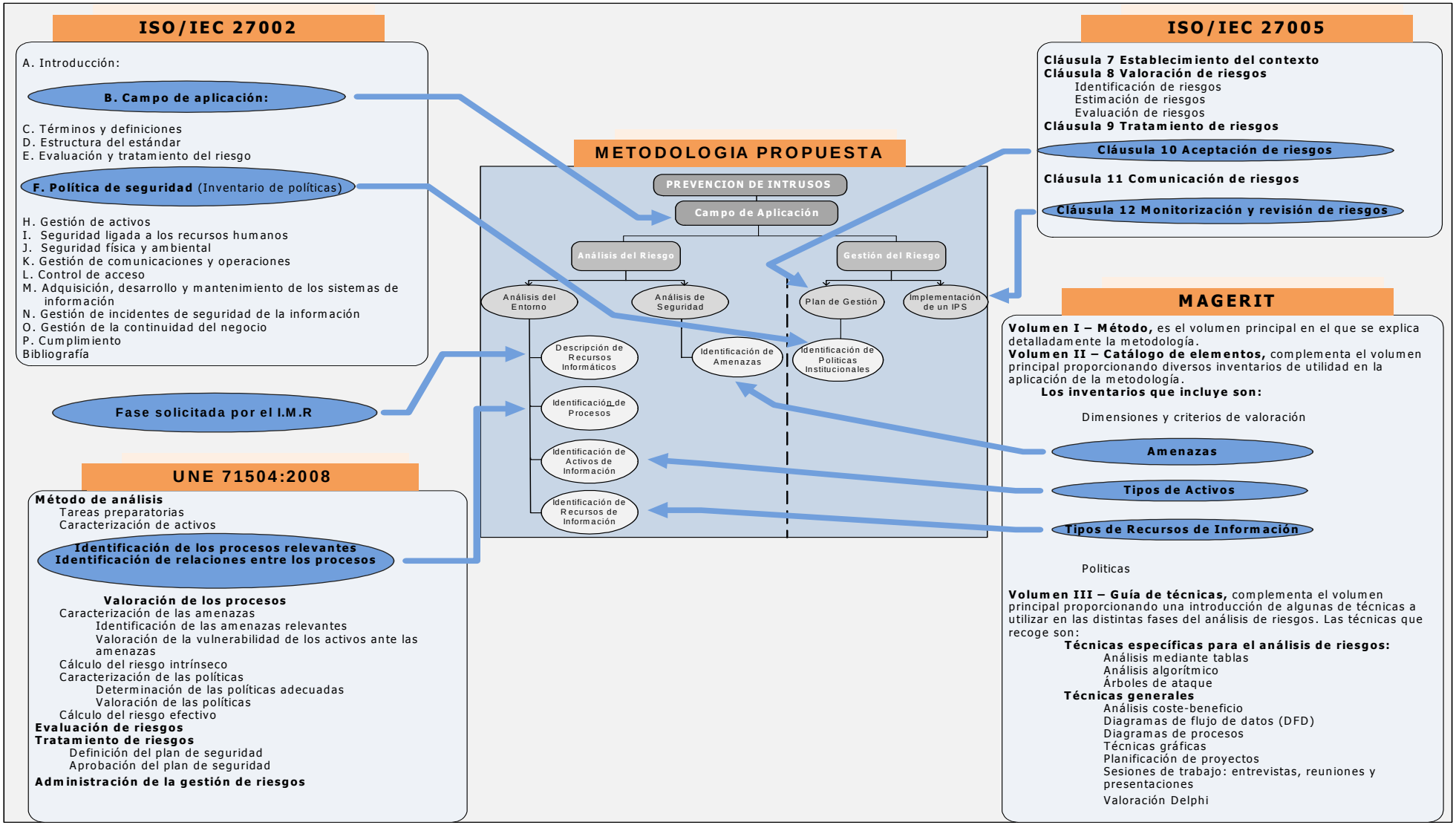


Figura IV.9. Detalle del Diseño de la Metodología Propuesta

- ✓ **Campo de Aplicación**

Se desea que la metodología indique antes de nada, su propósito u objetivo a lograr luego de ser aplicada.

- ✓ **Análisis de riesgos:**

Comprende el análisis del entorno de red, es decir recabar toda la información referente a la institución, entre lo que se identifica topología de la red, objetivos productivos y recursos de red, que pueden ser físicos y/o de información.

Forma parte de esta fase el análisis de seguridad que permitirá definir las amenazas que están afectando la red del IMR

- ✓ **Gestión de riesgos**

Permite determinar la aceptación o no de las amenazas para que sean tratadas en la metodología, aplicando políticas de seguridad y ayudándose con la implementación de un IPS.

Gráficamente el modelo metodológico se resume:

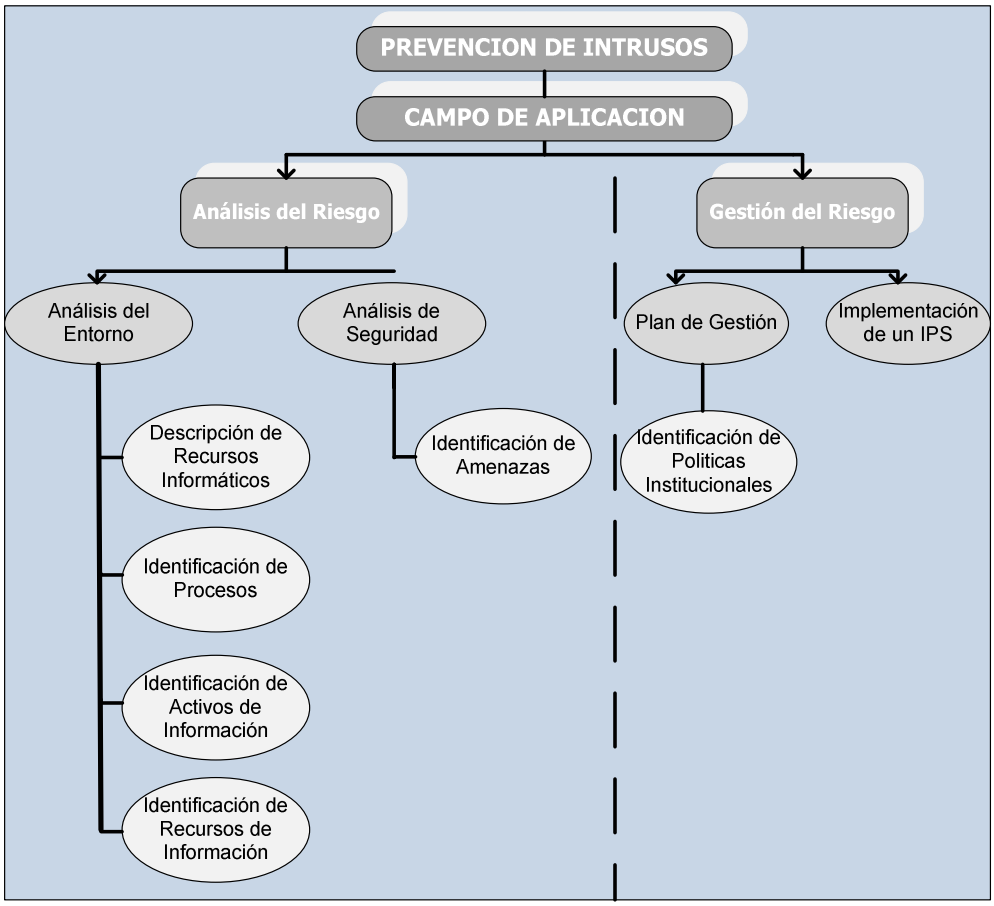


Figura IV.10. Fases de la Metodología Propuesta

4.2. DESARROLLO DE LA METODOLOGIA DE PREVENCION DE INTRUSOS

4.2.1. CAMPO DE APLICACIÓN

Fase basada en la norma ISO/IEC27002; pretende dar una idea general de la finalidad de la implementación de la metodología. Se deberá indicar su objetivo general.

4.2.2. ANÁLISIS DE RIESGOS

ANALISIS DEL ENTORNO

DESCRIPCION DE RECURSOS INFORMATICOS

Es necesario antes de empezar a realizar cualquier propuesta de mejora en la seguridad de una red, determinar los equipos y más recursos informáticos que posee la

organización para poder tener una idea superficial del alcance que tendrá el proyecto y además para determinar si la metodología a diseñar cubrirá o no todo el entorno de la red. Esta fue la principal razón por la que los administradores de red del IMR solicitaron se realice esta fase.

IDENTIFICACIÓN DE PROCESOS

Fase adoptada de la norma UNE 71504 identificación de los procesos relevantes y la relación que existe entre ellos.

Los procesos del IMR son el elemento de mayor valor, puesto que son los que permiten a la entidad cumplir sus objetivos de negocio.

Según la norma citada los procesos pueden dividirse en:

- ✓ **Procesos productivos**, que son los definidos para cumplir el cometido y los objetivos finales de la organización.
- ✓ **Procesos de soporte o de apoyo**, que son los procesos cuyo objetivo consiste en asegurar el funcionamiento de los procesos productivos.

La metodología requiere la identificación de los diferentes procesos de negocio y de soporte, por diferentes motivos:

- o Definir la importancia relativa de los distintos elementos del sistema.
- o Descartar de forma precoz los procesos que no disponen ni requieren de información relevante, y que, por tanto, pueden obviarse durante el análisis de riesgo, reduciéndose en consonancia el esfuerzo necesario para la realización del análisis sin afectar a la calidad del resultado final.

Las tareas a realizar en relación con los procesos productivos son:

- Inventariar los procesos dentro del alcance del análisis de riesgo.
- Documentar brevemente los objetivos de cada uno de los procesos productivos, para facilitar la interpretación posterior del análisis realizado.
- Identificar las relaciones existentes entre los distintos procesos: dependencia, secuencia, etc.
- Realizar un análisis informal de riesgos de seguridad de la información a alto nivel, que permita descartar aquellos procesos que no resulten de interés para las fases posteriores.

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Fase basada en la metodología Magerit que determina detallar los diferentes activos de información según los procesos que se hayan determinado en la organización.

Una vez identificados los procesos necesarios para cumplir con los objetivos de cada uno de los servicios que brinda el IMR, se debe identificar los activos de información relevantes involucrados en cada uno de ellos.

Se considera **activo de información** a toda aquella información que tiene valor para el IMR en la medida en que le permite el cumplimiento de sus objetivos.

Los activos de información son intangibles, esto es, la tarea no consiste en identificar aplicaciones ficheros o bases de datos sino la información que se utiliza en el proceso desde un punto de vista conceptual.

IDENTIFICACION DE RECURSOS DE INFORMACIÓN

Fase necesaria de continuar, según la metodología de Magerit, luego de haber identificado los activos de información.

Razón principal: Se considera **recurso de información** a cualquier elemento que se emplea en el manejo de activos de información.

Para facilitar la identificación de los recursos de información se considera necesario disponer de un inventario de tipos de recursos de información, que se ha elaborado en base al inventario de la metodología MAGERIT [MAG06], y se puede encontrar en el Anexo III. Este inventario puede modificarse para adaptarlo a las necesidades específicas de cada análisis de riesgos.

Todos los recursos de información que se identifiquen deben asignarse a una de las categorías definidas para facilitar el análisis posterior.

ANALISIS DE SEGURIDAD

ANALISIS DE AMENAZAS

La metodología proporciona un inventario clasificado de amenazas basado en el proporcionado por la Metodología MAGERIT [MAGE06] que puede consultarse en el Anexo IV. Este inventario incluye unos valores de referencia de la frecuencia y el impacto de cada amenaza sobre cada uno de los tipos de recurso de información definido que no se han incluido en el documento debido a su elevado volumen.

En función de los objetivos definidos para el análisis de riesgos el inventario de amenazas puede ajustarse a los requerimientos específicos o sustituirse por otro que se adapte mejor a ellos.

En el caso del IMR se deberá, por pedido del departamento de sistemas, modificar el inventario en la sección Errores y Fallos Intencionados.

Se debe tener claro que una amenaza es cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información, y, por extensión, a los activos de información que dicho recurso soporta.

En el caso de amenazas fortuitas, algunos de los principales factores que pueden considerarse incluyen:

- ✓ Cambios en la estructura organizativa o tecnológica de la Organización.
- ✓ Cualquier cambio en una organización supone un periodo de estabilización y de formación del personal
- ✓ Externalización de procesos. La existencia de procesos externalizados puede incrementar los incidentes fortuitos de seguridad, debidos a la compartición de recursos con otras organizaciones que puedan ser atacadas.

En el caso de las amenazas intencionadas, algunos de los principales factores que pueden considerarse incluyen:

- ✓ Beneficio que un potencial atacante puede esperar de la realización del Ataque, pues los potenciales atacantes pueden esperar un beneficio elevado de sus ataques, estos se producirán con mayor frecuencia.
- ✓ Dificultad que un potencial atacante percibe de la realización del ataque, conocimientos y material necesarios para su ejecución, pues si la entidad proyecta una imagen de debilidad en la protección de su información, por ejemplo, a través de noticias en prensa, o a través de la percepción de empleados y terceros, la frecuencia con la que es atacada puede incrementarse.
- ✓ Existencia de motivaciones no económicas para la realización de sabotajes: conflictividad laboral, relaciones agresivas con competidores, proveedores o

clientes, etc pues el sabotaje se producirá con mayor frecuencia cuanto mayor sea el número de motivaciones para realizarlo.

- ✓ Relevancia de la organización. Si el IMR tiene una especial exposición al público, por su elevado número de empleados, de clientes, o por su actividad comercial y de marketing, el número de potenciales atacantes que pueden planear un ataque se incrementa, y con ello la frecuencia de los ataques.
- ✓ Volumen de tratamiento de información relacionada con terceros.
- ✓ La existencia de un elevado número de puntos de entrada y salida de información con terceros supone la existencia de múltiples puntos de ataque que pueden ser utilizados por potenciales atacantes que tienen noticia de ellos, incrementándose con ello la frecuencia de los ataques.
- ✓ Conocimiento de la estructura organizativa y tecnológica del IMR.

La información disponible por parte de terceros o de la opinión pública sobre la Organización puede utilizarse para realizar ataques. Por ello, cuanto mayor sea el volumen de información en manos de terceros: empleados, proveedores, clientes, etc. mayor será la frecuencia en la que esta información será utilizada contra la entidad para la realización de ataques.

4.2.3. **GESTION DE RIESGOS**

PLAN DE GESTION

Se toma como base la Cláusula 10 de la norma ISO/IEC 27005 que permite realizar una clasificación de las amenazas detectadas decidiendo, según sea el fin de la metodología, la aceptación o no del tratamiento de ciertas amenazas detectadas con anterioridad. Al definir a esta metodología dentro del ámbito de la prevención de intrusos, estamos orientándola a la seguridad lógica; éste será un ítem importante para la decisión a tomar en este punto.

ANALISIS DE POLITICAS INSTITUCIONALES

Las políticas son las medidas establecidas por el IMR para mitigar sus riesgos. Las políticas pueden reducir la probabilidad de éxito de una amenaza reduciendo, por tanto, su frecuencia y/o reducir el impacto en caso de producirse. [MAGE06].

La metodología incluye un inventario de políticas obtenido del código de buenas prácticas ISO/IEC 27002:2007 [ISO27002.05], según se recoge en el Anexo V de este documento. Se ha elegido este inventario de salvaguardas por diversos motivos:

- ✓ Alineación con el objetivo de implantar una metodología bajo la norma ISO/IEC 27002:2005 [ISO27002.05].
- ✓ Uso extendido y conocimiento del código de buenas prácticas, que además es una norma reconocida y adoptada por el Instituto Ecuatoriano de Normalización como NTE ISO-IEC 27002:2007.(Ver Ley Regulatoria Anexo XI)

En función de los objetivos definidos para el análisis de riesgos, el inventario de políticas puede ajustarse a los requerimientos específicos o sustituirse por otro que se considere más adecuado.

Cabe indicar que el IMR actualmente cuenta con ciertas políticas implantadas pero que no aseguran la información en un 100%.

IMPLEMENTACION DEL SISTEMA DE PREVENCION DE INTRUSOS IPS.

Cumpliendo las etapas previas, correspondientes al análisis de riesgos se planteó la posibilidad de realizar la gestión de los mismos a través de una herramienta combinada de software y hardware como es un Sistema de Prevención de Intrusos, el mismo que estará en condiciones de tomar las decisiones adecuadas para mejorar la seguridad de la Red Corporativa de M.I. Municipio de Riobamba, y que se sustenta en la Clausula 12 de la norma ISO/IEC 27005, que recomienda la monitorización y revisión de riesgos.

CAPÍTULO V

RESULTADOS OBTENIDOS

5.1. IMPLEMENTACIÓN DE LA METODOLOGÍA

5.1.1. CAMPO DE APLICACIÓN

El objetivo general de la metodología es lograr mejorar la seguridad de la información digital que maneja la red corporativa del IMR.

Dotando de un método sistemático y claro a seguir, brindando además la ayuda de una herramienta software como es el caso del Sistema de Prevención de Intrusos.

5.1.2. ANÁLISIS DE RIESGOS

ANÁLISIS DEL ENTORNO

DESCRIPCIÓN DE RECURSOS INFORMÁTICOS

Como se mencionó en el capítulo anterior el segundo paso a realizar en el desarrollo de la metodología propuesta es una breve descripción de todos los recursos informáticos que conforman la red del Municipio de Riobamba, por tal razón se detalla brevemente, a modo de informativo, los detalles requeridos.

La red del IMR pose una topología de estrella extendida para la distribución de datos por medio de la intranet a sus diferentes departamentos como son: Proyectos, Sistemas, Alcaldía, Sindicatura, Concejales, Prefectura, Recursos Humanos, Secretaria, Pagos de impuestos, Proveeduría, y Sistemas.

La red local maneja 5 switchs, 4 switchs de marca 3com y 1 de marca D-Link que son los encargados de interconectar todos los departamentos; para el almacenamiento de datos cuenta con tres servidores de produccion uno principal y dos redundantes, todos estos dispositivos están a cargo del departamento de sistemas.

La red posee además un enlace de fibra óptica que permite su comunicación al departamento de Planificación y Avalúos ubicado a 100 metros del edificio principal de esta institución por lo que dispone de un transceiver de fibra óptica a conector RJ-45 de marca Nexxt ubicado en el armario de distribución donde también se sitúan los switchs.

Figura V.11. Area de Servidores IMR

La entidad posee un servidor de Internet de banda ancha proporcionado por CNT con una velocidad de 512 Kbps, el cual cuenta con un administrador de servicio basado en

Kypus versión 1.3.0.8 usado para compartir dicho recurso a todos los departamentos que conforman la entidad.

Para finalizar se muestra dos figuras detalladas de la red del IMR, la Figura V.2. indica los equipos correspondientes al Area de servidores, pudiendose observar sus direcciones IP y conexiones.

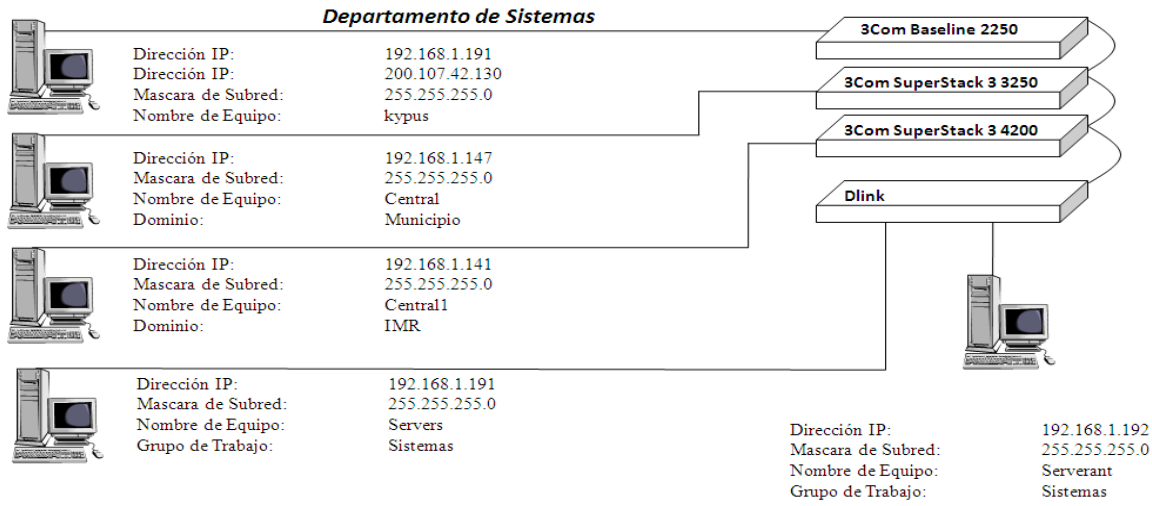


Figura V.12. Conexión Area de Servidores

La Figura V.3. indica el numero de puntos de red q poseen en total cada uno de los switchs, los q tienen usos especiales y los que quedan libres.

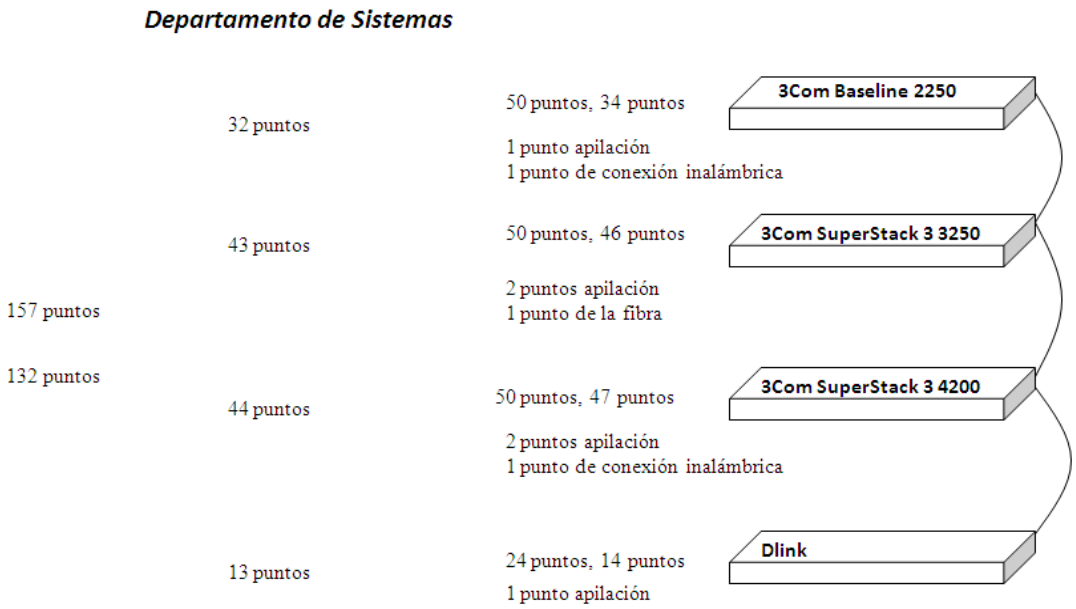


Figura V.13. Distribucion de Puntos de Red Area de Servidores

Luego de obtener una idea general de la red que se desea proteger pudimos indicar que nuestra metodología y su IPS está en condiciones de proteger el tráfico que ingresa y sale desde y hacia la red pública.

IDENTIFICACIÓN DE PROCESOS

Una de las fases más importantes de la metodología fue la identificación de procesos tanto productivos, como de soporte o apoyo, pues esto nos permite determinar la finalidad comercial que tiene el IMR, y de esta manera determinar posteriormente la importancia que tiene la información que se maneja.

Se cita a continuación el inventario obtenido:

Tabla V.21 Procesos Productivos y de Soporte.

PROCESOS	OBJETIVOS	RELACIÓN ENTRE PROCESOS	PRESENTA RIESGOS		JUSTIFICACIÓN
			SI	NO	
Permisos de locales comerciales	Facilitar a los propietarios de locales comerciales permisos para su respectivo funcionamiento.		X		Los procesos seleccionados trabajan todos mediante una base de datos donde se almacena la información de cada usuario, que sirve de base para el normal funcionamiento de las actividades a desarrollar; si existe una intrusión, se podrían alterar datos, lo que sería perjudicial para la entidad.
Cobro de Predios	Cobro anual de predios a los propietarios de bienes inmuebles.	Proceso #6	X		
Cobro de Serot	Registro diario de información de los pagos del Serot		X		
Cobro de impuestos de Rodamiento	Registro del cobro de rodamiento a todos los vehículos existentes dentro de la ciudad de Riobamba		X		
Actualización de datos del predio	Actualización de datos en los catastros urbano / rural	Proceso#5 Proceso #2	X		
Administración de los locales comerciales de los Mercados de la ciudad	Registro de información correspondiente a los mercados existentes dentro de la ciudad.	Proceso #1	X		
Registro de Escrituras	Almacenamiento digital de las escrituras y registros de propiedad.	Proceso #5	X		
Clasificación de predios	Determinar valores a cobrar según la extensión y ubicación de las propiedades	Proceso #8		X	Se trata de una clasificación y no de un registro en la base de datos, por ende el riesgo lógico no existe.

IDENTIFICACION DE ACTIVOS DE INFORMACION

Para lograr una clasificación de los activos de información se tomó en cuenta lo anotado en el capitulo anterior acerca de las relaciones activos-recurso, razón por la cual creímos conveniente citar los procesos estudiados anteriormente para mediante estos identificar los activos útiles en cada uno de ellos.

Tabla V.22. Activos de Información

Número de proceso	Procesos	Descripción	Activos de Información
1	Permisos de locales comerciales	Facilitar a los propietarios de locales comerciales permisos para su respectivo funcionamiento.	*Identificación de propietario *Ubicación del local comercial. *Productos que ofrece. *Fecha de inicio de funcionamiento.
2	Cobro de Predios	Cobro anual de predios a los propietarios de bienes inmuebles.	*Identificación de propietario *Ubicación de la propiedad. *Avalúo de la propiedad. *Extensión de la propiedad.
3	Cobro de Serot	Registro diario de información de los pagos del Serot	*Identificación de empleado. *Monto a ingresar. *Nombre de calles registradas. *Horario de ingreso y salida de empleado.
4	Cobro de impuestos de Rodamiento	Registro del cobro de rodamiento a todos los vehículos existentes dentro de la ciudad de Riobamba	*Identificación de propietario de vehículo. *Modelo de vehículo. *Placa de vehículo.
5	Clasificación de predios	Determinar valores a cobrar según la extensión y ubicación de las propiedades	*Identificación de propietario. *Extensión de la propiedad. *Ubicación de la propiedad.
6	Actualización de datos del predio	Actualización de datos en los catastros urbano / rural	*Identificación de propietario *Ubicación de la propiedad. *Avalúo de la propiedad. *Extensión de la propiedad.
7	Administración de los locales comerciales de los Mercados de la ciudad	Registro de información correspondiente a los mercados existentes dentro de la ciudad.	*Identificación de propietario *Ubicación del local comercial. *Productos que ofrece. *Fecha de inicio de funcionamiento.
8	Registro de Escrituras	Almacenamiento digital de las escrituras y registros de propiedad.	*Identificación del propietario. *Ubicación de la propiedad. *Plano de ubicación *Información de línea de fabrica

IDENTIFICACION DE RECURSOS DE INFORMACION

Se decidió hacer uso de los tipos de recursos de información incluidos en el inventario base de la metodología de análisis de riesgos MAGERIT 06, que se los puede consultar en el anexo VI, modificándolo para adaptarlo a las necesidades especificas de la entidad. Se listara a continuación los recursos de información principales:

- Procesos y Servicios
  - **Procesos**
    - ✓ Permisos de locales comerciales.
    - ✓ Cobro de Predios
    - ✓ Cobro de Serot
    - ✓ Cobro de impuestos de Rodamiento
    - ✓ Clasificación de predios
    - ✓ Actualización de datos del predio
    - ✓ Administración de los locales comerciales de los Mercados de la ciudad
    - ✓ Registro de Escrituras
- Personas
  - Directivos
    - ✓ **Dirección financiera**

      Ing. Lazo Ramírez Victoria Fanny
    - ✓ **Avalúos y Catastros**

      Sr. Velasteguí Álvarez Ángel Vicente
    - ✓ **Concejo Cantonal**

      Concejales de la Ciudad de Riobamba
    - ✓ **Administración de mercados**

      Ing. Vallejo Costales Ángel Vinicio
    - ✓ **Comisaria Municipal**

      Ramírez Herrera Milton Patricio

- ✓ **Alcaldía**

  Lic. Salazar López Juan Alberto

- o Usuarios Internos
  - ✓ **Ventanilla de atención ciudadana**

    Arrieta Aguagallo Raúl Gustavo
  - ✓ **Auditoría interna**

    Murillo Cobo Elsa Beatriz
- o Administradores de Sistemas
  - ✓ **Jefe de departamento de sistemas**

    Ing. Zabala Cuadrado Rosa Mercedes
- o Clientes
  - ✓ Ciudadanía

- **Aplicaciones Informáticas**

  El I.M.R para trabajar de mejor manera con sus usuarios posee aplicaciones informáticas, las cuales apoyan a la gestión Municipal en los siguientes ámbitos:

  - ✓ Contable y presupuestaria.
  - ✓ Gestión del talento humano.
  - ✓ Sistema de control y seguimiento de trámites.
  - ✓ Catastros municipales (predios urbanos, predios rurales, actividades económicas, arrendamiento, mercados, cementerios, rodaje y Serot). Emisión de tributos (impuestos, tasas, contribución especial de mejoras y multas). Gestión y recaudación de tributos.

- **Software de Sistemas**
  - o **Sistemas Operativos**
    - ✓ Windows 98 utilizado en 10 maquinas.
    - ✓ Windows 2000 utilizado en 18 maquinas.
    - ✓ Windows XP utilizado en 137 maquinas.

- ✓ Windows Vista utilizado en 36 maquinas.
- ✓ Windows 2003 server utilizado en 4 maquinas.

o **Bases de datos.**

- ✓ Oracle

- **Dispositivos de Hardware**

o Servidores

- ✓ 3 Servidores de bases de datos Windows Server 2003.
- ✓ 1 Servidor de Internet McAffee.
- ✓ Modem de conexión de Internet CNT.
- ✓ Dispositivo Kypus que actúa como firewall y para la distribución del ancho de banda de internet, además de manejar el correo electrónico del personal.

o Impresoras

- ✓ Multifuncionales Laser
- ✓ Mono funcionales Laser

o Ordenadores de trabajo

Tabla. V.23. Detalle computadoras IMR

MODELO	VELOCIDAD	CANTIDAD
PENTIUM III	600 MHZ	3
PENTIUM III	650 MHZ	5
PENTIUM III	750 MHZ	2
PENTIUM III	800 MHZ	5
PENTIUM III	866 MHZ	6
PENTIUM III	900 MHZ	1
PENTIUM III	1000 MHZ	6
PENTIUM III	1200 MHZ	2
PENTIUM IV	1500 MHZ	24
PENTIUM IV	1600 MHZ	9
PENTIUM IV	1700 MHZ	10
PENTIUM IV	2000 MHZ	1
PENTIUM IV	2200 MHZ	1
PENTIUM IV	2400 MHZ	27
PENTIUM IV	2800 MHZ	13
CORE DUO	1.6 GHZ	25
CORE DUO	1.8 GHZ	25
CORE DUO	2.0 GHZ	20
CORE DUO	2.4 GHZ	16
TOTAL		**201**

- **Switchs Edificio Central**
  - ✓ 3COM Baseline Switch 2250 PLUS, 50 puertos, 10/100 Mbps.
  - ✓ 3COM Super Stack3 Switch 3250, 50 puertos, 10/100/1000 Mbps.
  - ✓ 3COM Super Stack3 Switch 4200, 50 puertos, 10/100/1000 Mbps.
  - ✓ D-LINK DES-1024R, 24 puertos, 10/100 Mbps
  - ✓ 3COM Office connect Switch, 8 puertos, 10/100 Mbps
  - ✓ Cisco Aironet 1131 AG- Wireless access point 802.11b, 802.11a, 802.11g.
- **Switchs Planificación**
  - ✓ ALLIED TELESYN AT-FS724i, 24 puertos, 10/100 Mbps.
  - ✓ ALLIED TELESYN AT-FS724i, 24 puertos, 10/100 Mbps.
  - ✓ D-LINK DES- 101GD, 16 puertos, 10/100 Mbps.

- Redes de comunicaciones
  - **Red local**
    - ✓ 71 NICs Fast Ethernet 10/100 Mbps.
    - ✓ NIC 3COM EtherLink Server PCI 10/100 (Servidores)
    - ✓ 1 Modem ADSL Alcatel Speed Touch
    - ✓ Converter 10/100 Base-Fx Nexxt
    - ✓ 1 Firewall Kypus.
  - **Equipamiento Wireless**
    - ✓ 1 Proxim Tsunami MP 115054-R Base Station.
    - ✓ 2 Proxim Tsunami MP 115054-R Subscriber.
    - ✓ 2 Proxim Tsunami MP 5012 Sur Outdoor.
  - **Equipos Pasivos Edificio Central**
    - ✓ 1 Armario Metálico incluido el Rack
    - ✓ 2 Patch Panel: Panduit Data Patch cat. 5 T 568 B 48 puertos.µ
    - ✓ 1 Patch Panel 24 puertos.
    - ✓ 3 Organizadores de cables Panduit.
    - ✓ 142 Patch Cord.

- ✓ 284 Conectores RJ45.
- ✓ 71 Jack Conector.
- ✓ 71 Cajetines.
- ✓ 71 Face Place.
- ✓ 1200 Canaletas.
- ✓ 2700 m de Cable UTP cat. 5e
- ✓ 1 UPS Tripplite.

o **Equipos pasivos Planificación.**

- ✓ 1 Armario Metálico incluido el Rack.
- ✓ 2 Patch Panel: Panduit Data Patch cat. 5 T 568 B 48 puertos.
- ✓ 2 Organizadores de cables Panduit.
- ✓ 80 Patch Cord.
- ✓ 50 Conectores RJ45.
- ✓ 50 Jack Conector.
- ✓ 50 Cajetines.
- ✓ 50 Face Place.
- ✓ 300 Canaletas.
- ✓ 1000 m de Cable UTP cat. 5e
- ✓ 1 UPS Tripplite.

o **Direccionamiento**

- ✓ La red interna del municipio de Riobamba posee el siguiente direccionamiento.

Tabla. V.24. Direccionamiento IMR

Dirección de Red	192.168.1.0
Mascara de Red	255.255.255.0
Broadcast	192.168.1.255
Puerta de Enlace	192.168.1.1

- **Soportes de información**
  - Papel
  - Cintas
  - Memorias flash
- **Equipamiento auxiliar**
  - Sistemas de Alimentación Eléctrica.
    - ✓ 2 UPS Tripplite.
    - ✓ Generador de Energía Eléctrica.
  - Sistemas de control de acceso
- **Dispositivos de seguridad**
  - IDS/IPS
    - ✓ IPS desarrollado en el presente proyecto.
  - Firewall
    - ✓ Dispositivo Kypus versión 1.3.0.8.
  - Antivirus
    - ✓ Servidor de antivirus McAffee versión 8.7.

ANALISIS DE SEGURIDAD

IDENTIFICACIÓN DE AMENAZAS

En la metodología propuesta se indicó que nos basaremos en el inventario de amenazas registrado en la metodología MAGERIT; se debe indicar que se realizaron algunos ajustes a dicho inventario con el fin de adecuarlo a la situación real del IMR.

Es necesario aclarar que se hizo un análisis completo de las amenazas que aquejan a la situación de seguridad de la red del IMR; sin embargo en las fases posteriores de la metodología se determinará aquellas que deberán incluirse en la metodología propuesta como parte de estudio; para esto se tomó en cuenta que la prevención de

intrusos abarca lo referente a la seguridad lógica, y deja de lado lo referente a la seguridad física y ambiental.

A continuación se detalla las principales amenazas encontradas en dicha entidad.

- **De origen industrial**
  - Fallo de servicios de comunicaciones
    - ✓ Fallas del proveedor de internet por la caída de enlaces de comunicación de CNT.
    - ✓ Caída de la red de datos interna por fallas de energía en switchs y desconexión de cables de red.
- **De origen regulatorio**
  - Incumplimiento legal

    El IMR no posee licencias para los sistemas operativos que utilizan; obteniendo los siguientes resultados:
    - ✓ Windows 98 utilizado en 10 maquinas.
    - ✓ Windows 2000 utilizado en 18 maquinas.
    - ✓ Windows XP utilizado en 137 maquinas.
    - ✓ Windows Vista utilizado en 36 maquinas.
    - ✓ Windows 2003 server utilizado en 4 maquinas.
- . **Errores y fallos no intencionados**
  - Errores de los usuarios

    El IMR posee un alto porcentaje de usuarios que tienen conocimientos muy básicos en el campo computacional, y aun no ha implantado una política para fomentar a los usuarios sus conocimientos en este campo y así lograr reducir problemas frecuentes como:

- ✓ Eliminación de archivos del sistema.
- ✓ Desconfiguración de las impresoras en la red.

- o Errores de los administradores de Red

  La entidad no posee un informe técnico descriptivo que sea manejado por los administradores, donde se detalle normas técnicas sobre el mantenimiento de Pcs, una normativa a seguir para los formateos de las maquinas, además de determinar la adecuada administración del equipo Kypus que posee. Debido a estas razones sucitan problemas como:

  - ✓ No instalación o actualización inmediata de antivirus luego del formateo.
  - ✓ Falla en el mantenimiento de Computadoras, recurrencia de los daños reportados.
  - ✓ Mala administración del equipo Kypus.
- o Errores de monitorización (log)

  La entidad no hace utilización de ningún Sniffer para realizar un monitoreo de los logs en la Red.

- o Difusión de software dañino

  Como ya se ha mencionado no se dispone de un normativo dirigido a los usuarios donde se detalle las acciones preventivas que deben seguir para evitar que software dañino ponga en riesgo sus Pcs; consecuencia de esto tenemos:

  - ✓ Instalación de software sin licencia por parte de los usuarios de la Red.
  - ✓ No escaneo de flash memory antes de su uso.
- o Vulnerabilidades de los programas (software)

Aunque se cuente con la licencia de Oracle, nunca está libre de que pueda darse un desbordamiento de búfer de Oracle, lo que podría permitir la ejecución de código arbitrario y la consiguiente capacidad por parte de un atacante de leer, modificar y borrar información sensible.

- Errores de mantenimiento / actualización de programas (software)

  Existen fallas que se da por parte de los técnicos, al momento de formatear una PC, se instala siempre los drivers por defecto que contiene el CD del Mainboard, sin buscar actualizaciones de los mismos, ni tampoco se hace una actualización de la BIOS de los Mainboards.

- Caída del sistema por agotamiento de recursos

  El IMR se encuentra actualmente realizando un inventario correspondiente a las características técnicas de cada una de las Pcs que componen la Red, con el propósito de determinar:

  - ✓ Procesadores no actualizados.
  - ✓ Memorias RAM de baja capacidad de operación.
  - ✓ Falta de capacidad de almacenamiento en discos duros.

- **Errores y fallos intencionados**

  Como se señaló en la propuesta de la metodología, esta sección del inventario de amenazas de MAGERIT se la adaptó a las sugerencias y pedidos por parte de los miembros del departamento de Sistemas del IMR; obteniéndose como conclusión lo citado a continuación:

  - Uno de los principales problemas que afecta a la red es el exceso de trafico multimedia; debido al mal uso por parte de los usuarios del servicio de Internet, pues se ha determinado que muchos de ellos gastan su tiempo de trabajo visitando paginas de entretenimiento, con el fin de mirar videos,

fotografías, descargar archivos de música, visitar paginas de adultos, paginas de chat y el uso excesivo del Windows Live Messenger; provocando de esta manera disminución en el ancho de banda y mal uso de su tiempo de trabajo.

- Otro problema que se considero es el escaneo de puertos que puede hacerse desde un atacante externo con la finalidad de analizar y determinar puntos débiles para el ataque en la Red.
- El ping es considerado un ataque porque así se conocen las PCs activas en una red y el atacante ya puede dirigir procesos más específicos sobre este.

  El ping utiliza el protocolo ICMP, así tenemos que se considera un ataque debido a la forma de operación del ping, ya que por el formato de la trama, el usuario malicioso pide con la trama una solicitud de respuesta, y el equipo que recibe esta trama acepta la petición, así que el otro espera, hasta que el equipo vulnerable mande la respuesta a la petición.

5.1.3. **GESTION DE RIESGOS**

Luego de haber terminado la fase correspondiente al análisis de los riesgos, se empieza la siguiente fase correspondiente a la gestión del riesgo, en donde se determinara la aceptación o no de los riesgos, se crean las políticas y se implementa la herramienta en software.

PLAN DE GESTION

Al tener identificadas las amenazas a las que está expuesta la Red del IMR, lo que resta es hacer un análisis de valoración para clasificar los riesgos que están al alcance de ser mitigados en esta metodología.

Para ello nos basamos en la clausula número 10 de la norma ISO/IEC 27005, que nos da la libertad suficiente de decidir que riesgos aceptar, tomando en cuenta que la metodología está orientada a la prevención de intrusos, por ende las amenazas que aceptamos son aquellas que permiten mantener la seguridad de información a un nivel lógico, siendo ésta la justificación principal para su aceptación.

Se muestra a continuación una tabla donde se identifican las amenazas identificadas en el inventario de amenazas de Magerit, los aspectos considerados en el IMR que corresponden a dichas amenazas, los niveles de ataque de las amenazas, es decir nivel lógico o nivel físico y la aceptación o no de la amenaza para ser considerada dentro de la metodología con su respectiva justificación.

Se logra de esta manera archivar un inventario de amenazas que aquejan a la red del IMR.

Tabla V.25. Lista de Amenazas que se Aceptaron Corregir en la Metodología

AMENAZA SEGUN MAGERIT		ASPECTO CONSIDERADO EN EL IMR	NIVEL		ACEPTACIÓN DE CORREGIR LA AMENAZA		JUSTIFICACIÓN
			LOGICO	FISICO	POSITIVA	NEGATIVA	
Origen Industrial	**Fallo de Servicio de Comunicaciones**	✓ Fallas del proveedor de internet CNT. ✓ Caída de la red de datos interna por fallas de energía en switchs y desconexión de cables de red.		**X**		**X**	La metodología propuesta está orientada a la seguridad lógica, y los ítems mencionados se relacionan a la seguridad física, lo que no está contemplado dentro de la metodología; por lo tanto queda fuera del análisis.
Origen Regulatorio	**Incumplimiento Legal**	Sin Licencia: ✓ Windows 98 ✓ Windows 2000 ✓ Windows XP ✓ Windows Vista ✓ Windows 2003 server	**X**		**X**		El IMR no posee cumplimientos legales para Sistemas Operativos que la entidad maneja.
Errores y fallos No Intencionados	**Error de los usuarios.**	✓ Eliminación de archivos de sistema. ✓ Desconfiguración de Impresoras.	**X**		**X**		El IMR posee un alto porcentaje de usuarios que tienen conocimientos muy básicos en el campo computacional.
	Caída del Sistema.	✓ Procesadores no actualizados. ✓ Memoria RAM de baja capacidad. ✓ Almacenamiento en discos duros.		**X**		**X**	Amenaza no aceptada en la metodología, por corresponder al ámbito de la seguridad física.
	Error de los Administradores de Red.	✓ Actualización de antivirus. ✓ Falla mantenimiento de computadoras. ✓ Mala configuración de Kypus	**X**		**X**		El IMR no posee un informe técnico descriptivo que sea manejado por los administradores para el correcto mantenimiento de PCs.
	Error de Monitorización.	✓ La Entidad no posee ningún Sniffer	**X**		**X**		El IMR no utiliza ningún Sniffer para la monitorización de la Red.
	Difusión de Software Dañino.	✓ Instalación de Sw. sin Licencia. ✓ No escaneo de flash memory.	**X**		**X**		No se dispone de un normativo dirigido a los usuarios donde se detalle acciones preventivas para evitar software dañino.
	Vulnerabilidades de Programas.	✓ Desbordamiento de Buffer de Oracle	**X**		**X**		Oracle posee vulnerabilidades que dan la facilidad al atacante de leer, modificar y borrar información sensible.
	Error de Mantenimiento (Software).	✓ Falla en el formateo de PCs	**X**		**X**		En el IMR se dan fallas por parte de los técnicos ya que al momento de formatear se instalan drivers no actualizados.
Errores y fallos Intencionados	**Exceso Tráfico Multimedia.**	✓ Acceso a páginas de entretenimiento. ✓ Descarga de archivos de audio. ✓ Acceso a Windows Messenger.	**X**		**X**		Aspectos solicitados por parte de los administradores de Red para disminuir posibles ataques y mal utilización del recurso Internet.
	Ataque en la Red.	✓ Escaneo de Puertos. ✓ Utilidad Ping.	**X**		**X**		

IDENTIFICACIÓN DE POLITICAS INSTITUCIONALES

La metodología desarrollada permite guiarnos en el inventario de políticas publicado en la norma ISO/IEC 27002, que se puede apreciar en el anexo IX, sin embargo conjuntamente con el departamento de sistemas del IMR se decidió implantar políticas de seguridad específicas para las amenazas detectadas, sin dejar de lado las sugerencias que se indican en el Anexo IX.

Se presenta una tabla donde se identifican las amenazas seleccionadas en el punto anterior, que van a ser mitigadas mediante la implantación de una política que se detalla en la misma tabla, así como la relación con la norma ISO/IEC 27002.

Tabla V.26. Políticas Adoptadas Para las Amenazas del IMR

AMENAZA SEGUN MAGERIT		ASPECTO CONSIDERADO EN EL IMR	POLÍTICA ADOPTADA	RELACIÓN CON INVENTARIO DE POLITICAS ISO/IEC 27002:2005
Origen Regulatorio	**Incumplimiento Legal**	Sin Licencia: ✓ Windows 98 ✓ Windows 2000 ✓ Windows XP ✓ Windows Vista ✓ Windows 2003 server	Estandarización de Sistemas Operativos dentro del IMR al uso exclusivo de Windows XP, Windows Vista y Windows 2003 Server bajo su compra oficial de Licencia. Política a largo plazo.	15. Cumplimiento Regulatorio 15.1.1 Identificación de la legislación aplicable. 15.1.2 Derechos de propiedad intelectual 15.2.2 Comprobación del cumplimiento técnico
Errores y fallos No Intencionados	**Error de los usuarios.**	✓ Eliminación de archivos de sistema. ✓ Desconfiguración de Impresoras.	Programar seminarios de capacitación dirigido a usuarios que no tengan conocimientos básicos de computación. Establecimiento de niveles de usuarios. Creación de cuentas de usuario en las Pcs.	8. Control de Empleados 8.1.1 Roles y responsabilidades 8.1.2 Investigación 8.1.3 Términos y condiciones de la ocupación 8.2.2 Conocimiento educación y entrenamiento en la seguridad de la información. 8.2.3 Proceso disciplinario
	Error de los Administradores de Red.	✓ Actualización de antivirus. ✓ Falla mantenimiento de computadoras. ✓ Mala configuración de Kypus	Dictar Charlas y cursos acerca del funcionamiento de Antivirus y administración de la Red a todo el personal del Departamento de Sistemas y crear un informe técnico descriptivo que oriente al personal a realizar una correcta configuración de los equipos	10. Control de las operaciones de los sistemas de información 10.1.1 Procedimientos operacionales documentados 10.2.2 Supervisión y revisión de los servicios de terceros. 12 Control de adquisición y desarrollo y mantenimiento de aplicaciones 12.1.1 Análisis y especificación de requerimientos de seguridad 13. Gestión de los incidentes de seguridad 13.1.1 Comunicación de eventos de seguridad de la información
	Error de Monitorización.	✓ La Entidad no posee ningún Sniffer	Instalación y Ejecución de Ethereal para el monitoreo de la Red	12 Control de la adquisición, desarrollo y mantenimiento de aplicaciones 12.1.1 Análisis y especificación de requerimientos de seguridad 12.2.2 Control de proceso interno 12.3.1 Política de uso de software analizador
	Difusión de Software Dañino.	✓ Instalación de Sw. sin Licencia. ✓ No escaneo de flash memory.	Difundir normativos y dictar cursos a todos los usuarios sobre posibles Virus e instalación de Software con Licencia, y normas para difundir el respaldo de información cada 15 días.	10. Control de las operaciones de los sistemas de información 10.4.1 Controles contra código malicioso 10.4.2 Controles contra código móvil 10.5.1 Copia de seguridad de la información 10.7.1 Gestión de soportes extraíbles
	Vulnerabilidades de Programas.	✓ Desbordamiento de Buffer de Oracle	Se recomienda, a los administradores de la Red que utilicen los programas afectados, la instalación de los parches correspondientes, mientras tanto se sugiere: Deshabilitar los servicios Oracle innecesarios. Ejecutar los servicios Oracle con los menores privilegios posibles. Restringir el acceso desde la red a los servicios Oracle.	10. Control de las operaciones de los sistemas de información 10.2.2 Supervisión y revisión de los servicios de terceros. 10.2.3 Gestión de cambios en servicios de terceros 12 Control de la adquisición, desarrollo y mantenimiento de aplicaciones 12.4.1 Control de software en producción
	Error de Mantenimiento (Software).	✓ Falla en el formateo de PCs	Descarga constante desde el internet de todos los drivers actualizados y actualización de BIOS para las PCs del IMR	8. Control de empleados 8.2.3 Proceso disciplinario 12 Control de la adquisición, desarrollo y mantenimiento de aplicaciones 12.5.2 Revisión técnica de las aplicaciones tras cambio del sistema operativo 12.5.5 Desarrollo externalizado del software
Errores y fallos Intencionados	**Exceso Tráfico Multimedia.**	✓ Acceso a páginas de entretenimiento. ✓ Descarga de archivos de audio. ✓ Acceso a Windows Messenger.	Desarrollo de una aplicación Software (IPS) para la prevención de ataques y bloqueo de acceso a distintas paginas con el motivo de disminuir el consumo del ancho de banda	En este apartado no se posee una relación con el inventario de políticas ISO/IEC 27002, puesto que se ha decidido implementar políticas específicas en el IPS, que logren mejorar las amenazas citadas.
	Ataque en la Red.	✓ Escaneo de Puertos. ✓ Utilidad Ping.		

Se creyó conveniente detallar las políticas aplicadas dentro de lo que corresponde al desarrollo del IPS. Se cita a continuación el detalle de cada política adoptada.

- ✓ **Bloquear el acceso a sitios específicos en el internet.**

Se decidió bloquear las siguientes páginas de entretenimiento:

www.hi5.com
www.facebook.com
www.sexofree.org
www.cdadulto.com
www.pomstarstart.com
www.actrizpornoxxx.com.

- ✓ **Bloqueo de mensajería instantánea.**

Para controlar el uso indebido del paquete de mensajería instantánea propio de Microsoft, Messenger, conjuntamente con los técnicos del departamento se tomo la decisión de bloquear el envió y recepción de mensajes mediante este software en la red.

- ✓ **Descarga de archivos con extensión .mp3**

Con el motivo de evitar el consumo excesivo de ancho de banda se tomó la decisión de bloquear la descarga de archivos con extensión .mp3.

- ✓ **Bloqueo de escaneo de puertos por parte del Software Nmap.**

Para prevenir posibles ataques externos llevados a cabo mediante el escaneo de puertos con Nmap, se protegió a la Red para que no permita enviar información relevante de cada una de sus PCs.

- ✓ **Bloqueo de la utilidad Ping hacia los Servidores.**

Con el fin de evitar cualquier tipo de comunicación mal intencionada hacia los equipos de la Red interna, se bloqueó el comando ping hacia los servidores de producción y hacia cualquier maquina de la Red.

IMPLEMENTACION DE UN SISTEMA DE PREVENCION DE INTRUSOS

GENERALIDADES

Siguiendo la propuesta metodológica, y con el objetivo de gestionar los riesgos analizados, se implementó en el IMR un Sistema de Prevención de Intrusos que cumple con los requerimientos de mejora para la seguridad informática de la organización.

El IPS ha implementar se lo va a ubicar de acuerdo a los dispositivos existentes en la Red del IMR, en este caso se lo va a ubicar después del Firewall Kypus y antes de toda la Red a proteger.

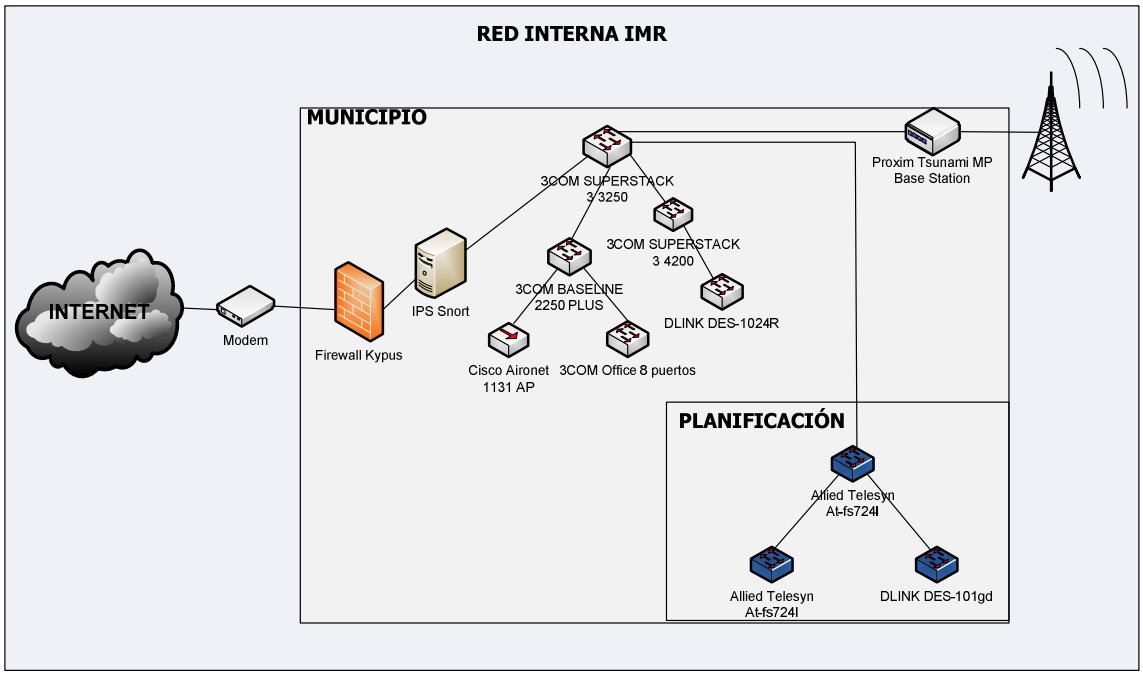


Figura V.14 Ubicación del IPS dentro de la Red del IMR.

A continuación se detalla la implementación en su totalidad del IPS, considerando en cada punto las necesidades específicas del IMR.

Para levantar el servicio se implementó un puente de red o bridge a través de dos interfaces de red, que permitirá el tráfico de los paquetes que serán analizados por el Snort; con el fin de que se realice adecuadamente la generación de alertas para su posible toma de decisión, de acceso o deniego de éstos a través del IP Tables y según las normas que se han creado.

Las alertas generadas se almacenan en una base de datos diseñada en MySQL y éstas a su vez se visualizan a través de una interfaz gráfica denominada BASE (de su acrónimo en inglés Base Analysis and Security Engine)

Gracias al IPS fue posible ver los detalles de un ataque como son las direcciones IP origen y destino, los protocolos y puertos que se han utilizado para el tráfico de las tramas; además fue posible realizar una administración en lo referente a creación de usuarios, así como también realizar búsquedas detalladas de las alertas generadas por el Snort, permitiendo su visualización por fechas específicas, direcciones que generan la alerta y sensores por los cuales accedió el tráfico de los paquetes.

Para el caso particular y según las necesidades del municipio de Riobamba las reglas que se usaron son las siguientes:

- ✓ Bloqueo del protocolo ICMP para evitar el ping desde una red externa hacia la red externa y viceversa.
- ✓ Bloqueo para la descarga de archivos con extensión .mp3 para evitar consumo de ancho de banda innecesario.
- ✓ Bloqueo de acceso o inicio de sesión en Windows Live Messenger.

- ✓ Bloqueo de acceso a páginas web específicas como por ejemplo www.hi5.com, www.facebook.com, www.sexofree.org, www.cdadulto.com, pomstarstart.com, www.actrizpornoxxx.com.
- ✓ Bloqueo de escaneos de puertos con nmap.

Luego de esta breve descripción se procede a realizar un sumario explicativo de todo los pasos concernientes para la implementación del IPS así como también de su manejo luego de concluido.

CARACTERISTICAS DEL EQUIPO UTILIZADO

Para instalar un servidor de Snort es importante tener en cuenta qué tráfico se espera manejar. Snort puede ejecutarse en casi cualquier tipo de hardware.

Pero de todos modos, si se desea tener un IPS rápido y fiable sin un alto porcentaje de paquetes perdidos, Snort necesitará un procesador relativamente potente. Sobra decir que se necesita además espacio de almacenamiento para los registros y alertas.

El elemento más crítico, sin embargo, es una buena interfaz de red. Siempre que sea posible, se revisará que la interfaz de red es dedicada, y nunca integrada en la placa base.

La mayoría de los fabricantes actuales ofrecen una tarjeta de red especial para servidores, con un procesador integrado específicamente diseñado para el procesamiento del tráfico de red.

Como requerimientos mínimos del sistema del equipo que sirvió como servidor IPS tenemos:

Tabla V.27. Requerimientos de Hardware para Servidor IPS.

Procesador	**Intel Inside Pentium IV 3.0 GHZ**
Disco Duro	ATA Samsung 80 Gb
Tarjetas de Red	Realtek Semiconductor
	Sundance Technology PCI
Memoria RAM	512 Mb

DESCARGA Y ALMACENAMIENTO DE PROGRAMAS Y DEPENDENCIAS

Creación de la Carpeta **Snortinstall** para el almacenamiento de los diferentes programas y dependencias descargados.

Todo el procedimiento de creación de carpetas y configuración se lo realiza bajo el usuario root.

En la consola Terminal se creó el directorio bajo /root llamado snortinstall, el comando para la creación es el siguiente:

```
[root@localhost ~]# mkdir
```

En la carpeta snortinstall se ubicó los siguientes archivos de instalación descargados:

Snort_Inline-2.6.1.5

BASE

ADODB

PROGRAMAS NECESARIOS PARA EJECUTAR SNORT_INLINE Y BASE:

La instalación de los programas se lo realizó a través de paquetes YUM.

- ✓ **MySQL 5.0.9**

MySQL Servidor de base de datos.

Comando para instalación:

```
[root@localhost ~]#yum  -y install mysql mysql-server
```

- ✓ **PHP 5.2**

Lenguaje de secuencia de comandos

Comando para instalación:

```
[root@localhost ~]#yum install php5
```

COMPILADORES

Compiladores para poder instalar todos los paquetes utilizados en Snort_Inline

Comando para instalación:

```
[root@localhost ~]#yum install *gcc* *pcre* libdnet php-adodb php-mysql php-gd
+mysql-devel
```

- ✓ **IPTABLES-DEV**

Conjunto de reglas de filtrado de paquetes de Linux.

Comando para instalación:

```
[root@localhost ~]#yum install iptables-dev
```

- ✓ **LIBDNET**

Interfaz con varias rutinas de red de bajo nivel incluyendo:

- ✓ Manipulación de direcciones de red.
- ✓ Cortafuegos de red.
- ✓ Búsqueda y manipulación de interfaces de red.
- ✓ Transmisión de tramas Ethernet.

INSTALACIÓN:

Como no hay paquetes disponibles para libdnet se instaló de forma manual: Descargar libdnet y descomprimirlo:

```
[root@localhost ~]#tar -xvf libdnet-1.11.tar.gz
```

Ubicarse en el directorio de acceso lidbnet e instalar la biblioteca:

```
[root@localhost~]#cd/libdnet-1.11
[root@localhost libdnet-1.11~]#./configure
[root@localhost libdnet-1.11~]#make
[root@localhost libdnet-1.11~]#make install
```

INSTALACIÓN DE SNORT_INLINE

Para que Snort_inline analice el tráfico de un segmento de red, debió ser añadido, de forma transparente y, como ya se mencionó, por medio de dos tarjetas en modo bridge, con funcionalidad inline.

Dicha funcionalidad se consiguió conduciendo el tráfico a través de iptables (ip_queue). Sin embargo, esto no fue suficiente puesto que necesitamos saber, a través de las iptables, que tráfico se debe añadir.

Snort_inline, puede como cualquier otro sistema de prevención de intrusiones bloquear las conexiones que reciba. Para actuar en modo inline, Snort fue compilado con el fin de conseguir respuestas flexibles que permitan restaurar el tráfico que deberá ser bloqueado.

Para concluir, podemos decir que Snort_inline es definitivamente el modo más efectivo y preciso disponible; ya que controla el tráfico basándose en reglas cargadas previamente.

Una vez descargados e instalados las herramientas adicionales a necesitar para que Snort_Inline se configure con éxito, se procedió a la instalación del IPS.

DESCARGA Y CONFIGURACIÓN

La versión de snort que se utilizó en el proyecto fue **snort_inline-2.6.1.5.**

Descargar Snort_Inline y descomprimirlo:

```
[root@localhost snortinstall ~]#tar -xvf snort_inline-2.6.1.5.tar.gz
```

Crear dos directorios, uno para almacenar los archivos de configuración, y el otro para almacenar las reglas de Snort.

```
[root@localhost ~]#mkdir /etc/snort_inline
[root@localhost ~]#mkdir /etc/snort_inline/reglas
```

Directorio para el almacenamiento de alertas.

Todas las alertas generadas por snort se almacenaran en esta carpeta.

```
[root@localhost ~]#mkdir /var/log/snort_inline
```

Copiar los archivos de configuración de Snort_Inline-2.6.1.5 dentro del directorio creado:

```
[root@localhost ~]#cp snort_inline-2.6.1.5/etc/* /etc/snort_inline/
```

ARCHIVO DE CONFIGURACION DE SNORT_INLINE

La configuración del IPS se cambió de acuerdo a la red del IMR a proteger, el archivo maestro que se editó fue snort_inline.conf con los siguientes parámetros:

VARIABLES DE RED

var HOME_NET 192.168.1.0/24

Red Interna a proteger, en este caso se definió la dirección de red que está en uso dentro del IMR.

var EXTERNAL_NET any

Red externa (Internet por ejemplo):

var SMTP_SERVERS any

Protección de servidores SMTP que se encuentran dentro de nuestra red, en este caso definimos any.

var TELNET_SERVERS any

Protección de servicios TELNET en la red interna.

var HTTP_SERVERS any

Protección de servicios Web dentro de nuestra red.

var SQL_SERVERS any

Protección de servidores de Base de Datos existentes en la red.

var DNS_SERVERS any

Protección de servicios DNS.

var HTTP_PORTS 8080

Variable del puerto 8080

var SHELLCODE_PORTS !80

Variable activa para puertos de código Shell

var ORACLE_PORTS 1521

Variable activa para puertos Oracle

var SSH_PORTS 22

Variable para puertos de conexiones no seguras SSH

PRE-PROCESADORES

Se trata de pequeños plugins programados normalmente en C que sirven para tratar los paquetes provenientes del Decodificador. El tratamiento que realiza sobre los paquetes es para darle forma de manera que se pueda interpretar la información de los paquetes de forma más sencilla y lógica. Una vez reordenados los paquetes, al pasar por el motor de Detección se le aplican las Reglas en busca de patrones de ataques, virus, información, etc.

Los preprocesadores pueden desfragmentar paquetes, ordenarlos, decodificar URLs, re ensamblar, etc.

Estos preprocesadores se configuran en el archivo maestro de configuración etc/snort_inline.conf

PREPROCESADORES UTILIZADOS

Flow

Este preprocesador es requerido para que otros preprocesadores puedan funcionar, tales como flowbits detection plug-in y flow-portscan, los preprocesadores Flow permiten a Snort mantener sus mecanismos de adquisición de datos.

Sus funciones son:

- ✓ **stats_interval:** este parámetro especifica el intervalo de tiempo expresado en segundos tras el que queremos que Snort vuelque las estadísticas en stdout.
- ✓ **Hash:** este parámetro especifica el método hash, usando el valor 1 definimos un hash por byte.

```
preprocessor flow: stats_interval 0 hash 2
```

Stream4

Este preprocesador da a Snort la habilidad de ver la base del paquete y donde fue generado (cliente o servidor), este preprocesador tiene la capacidad de re-ensamblaje de streams y almacenar los más recientes ataques no declarados. Sus funciones son:

- ✓ **disable_evasion_alerts:** esta opción se usa para desactivar las alertas escritas en stream4.
- ✓ **midstream_drop_alerts:** le dice al preprocesador que bloquee las conexiones generadas sin establecer un flow determinado.
- ✓ **Rpc decode:** este preprocesador re-ensambla un flujo rpc en un sólo paquete para que sea más fácil de analizar, si el preprocesador stream4 está presente, sólo analizará el tráfico proveniente del cliente.
- ✓ **Telnet decode:** este preprocesador normaliza el flow de caracteres de un protocolo telnet en una sesión. Debemos especificar los puertos a analizar.
- ✓ **log:** hace un log en un archivo o base de datos.
- ✓ **Pass:** ignora el tráfico que ha encontrado.
- ✓ **Drop:** pasa el paquete a través de las iptables y lo guarda en un archivo o base de datos.
- ✓ **Reject:** si es un TCP resetea la conexión a través de las iptables, si es UDP manda un mensaje icmp host unreachable y hace un log en un archivo o base de datos.
- ✓ **Sdrop:** pasa el paquete a través de iptables y no lo archiva.

```
preprocessor stream4:          disable_evasion_alerts, \
                                stream4inline, \
                               enforce_state drop, \
                                memcap 134217728, \
                                timeout 3600, \
                                truncate, \
                                window_size 3000,\
                                disable_ooo_alerts
```

HTTP Inspect

Es un decodificador HTTP genérico para aplicaciones de usuario. Dado un búfer de datos, HTTP Inspect decodificará el buffer, encontrara campos de HTTP, y los normalizara. HTTP Inspect inspeccionara las solicitudes de los clientes y las respuestas del servidor.

Dentro de HTTP Inspect, hay dos áreas de configuración: global y el servidor.

```
preprocessor http_inspect:    global \
                              iis_unicode_map unicode.map 1252
```

BACK ORIFICE.

Preprocesador especialmente diseñado para el troyano Back Orifice.

```
preprocessor bo
```

CONEXIÓN A REGLAS UTILIZADAS

Para la conexión a las distintas reglas que se utilizaran en el IPS se lo hará por la siguiente variable definida a continuación:

```
var RULE_PATH /etc/snort_inline/reglas
```

SALIDA Y ALMACENAMIENTO DE ALERTAS GENERADAS POR SNORT

El modo 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

```
output alert_full: snort_inline-full
```

El modo Alerta Rápida devuelve información sobre: tiempo, mensaje de la alerta, clasificación , prioridad de la alerta, IP y puerto de origen y destino.

```
output alert_fast: snort_inline-fast
```

CONFIGURACIÓN DE LOS OUTPUT PLUGINS

Aquí se definen a donde tienen que ir a parar los logs que Snort genera. Estos deciden si van a ser ficheros de texto (logs) o a una base de datos, y decide también en que formato irán escritos (binario, texto plano, xml...). Como nos interesa poder acceder a los datos desde BASE y éste está escrito en PHP, diremos que guarde la salida en la base de datos MySQL previamente definiendo una contraseña y un usuario.

```
output database: log, mysql, user=snort password=administrador dbname=snort
host=localhost
```

CONFIGURACIÓN DE REGLAS .

```
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/finger.rules
#include $RULE_PATH/local.rules
#include $RULE_PATH/ftp.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/rpc.rules
#include $RULE_PATH/rservices.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/sql.rules
#include $RULE_PATH/x11.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/netbios.rules
#include $RULE_PATH/oracle.rules
#include $RULE_PATH/mysql.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/smtp.rules
```

COMPILACION DE SNORT_INLINE

Al terminar la configuración del archivo snort_inline.conf se procedió a la compilación de snort con los parámetros establecidos, los comandos a utilizarse son los siguientes:

Procedimiento para la compilación:

Para la compilación se ubicó dentro de la carpeta snort_inline-2.6.1.5 con los siguientes comandos:

```
[root@localhost ]#cd snortinstall
[root@localhost  snortinstall ]#cd snort_inline-2.6.1.5
```

Comando para la compilación de Snort_inline con mysql:

```
[root@localhost  snortinline-2.6.1.5]# ./configure – with-mysql
[root@localhost  snortinline-2.6.1.5]#make
```

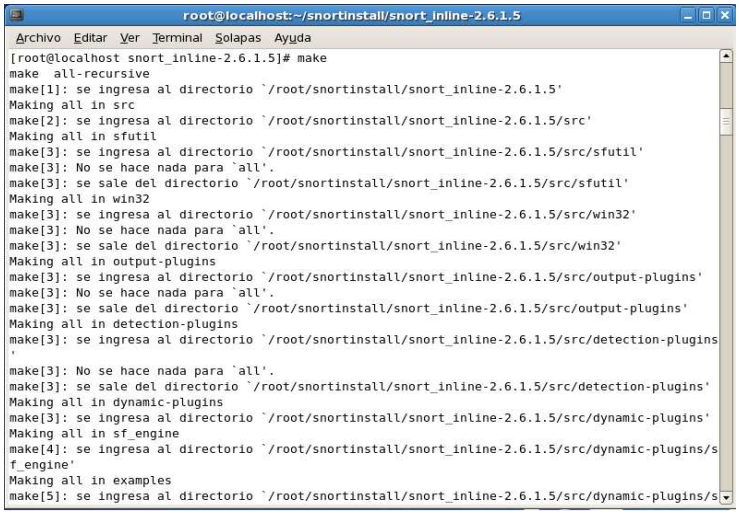


Figura V.15. Pantalla de Resultados al Digitar el Comando make.

```
[root@localhost  snortinline-2.6.1.5]#make install
```

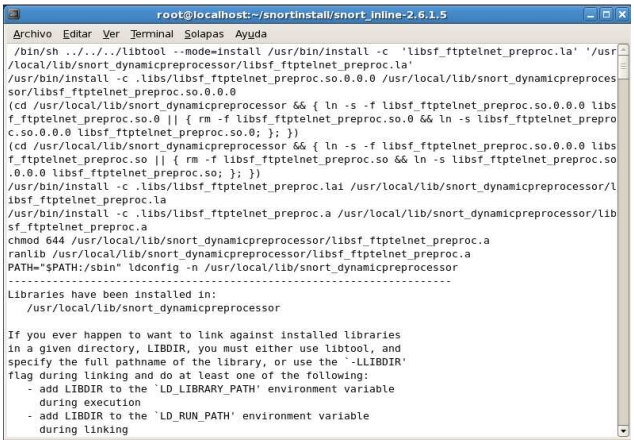


Figura V.16. Pantalla de Resultados al Digitar el Comando make install.

CONFIGURACIÓN DE MYSQL

La configuración de la base de datos se divide en varios apartados. Primero se debe elegir una contraseña adecuada, crear la base de datos necesaria y definir la estructura de las tablas. Nos conectamos como *root* al servicio de MySQL y creamos la base de datos y los permisos para *snortusr*. Para abrir la línea de comandos de MySQL ejecutaremos *mysql -u root -p* desde la terminal.

Luego se pide la contraseña del usuario root y entramos al intérprete de *mysql>*. En él introducimos los siguientes comandos para la finalización del primer apartado de la configuración (hemos de asegurarnos de que cada línea termina con un punto y coma ";").

Ingreso a Mysql con el usuario root.

```
[root@localhost ~]#mysql  -u root –p
```

Ingreso de contraseña

La contraseña a utilizar va a ser administrador

```
Enter password: administrador
```

Figura V.17. Ingreso a MySQL con el Usuario root y Contraseña.

Interfaz de MySQL

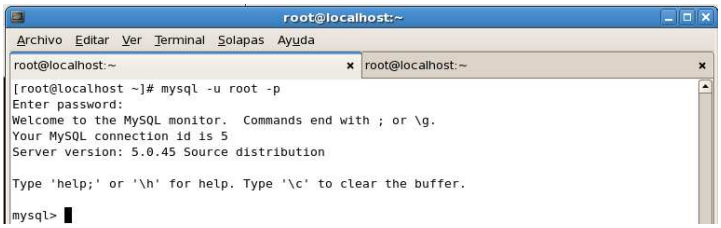


Figura V.18. Interfaz de MySQL.

CREACIÓN Y CONFIGURACIÓN DE LA BASE DE DATOS SNORT Y SUS RESPECTIVAS TABLAS

Mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('administrador');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('administrador');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql>exit
Bye

CREACIÓN DE TABLAS

La base de datos Snort creada va a necesitar de tablas para su almacenamiento de datos recogidos por el programa, los comandos utilizados para la creación de las tablas es el siguiente:

```
[root@localhost ~]#mysql -u root -p < ~/snortinstall/snort-2.6.1.5 /schemas /
create_mysql snort
Enter password: administrador
```

USO DE BASE DE DATOS SNORT

Con el siguiente comando se cambiará la base de datos a utilizar para el almacenamiento de las alertas, en este caso la base de datos será snort.

```
Mysql> use snort;
```

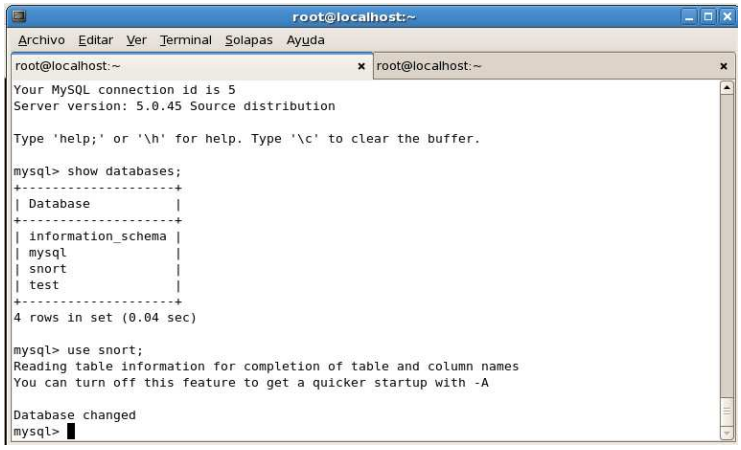


Figura V.19. Cambio de Base de Datos.

VISUALIZAR BASE DE DATOS SNORT

Mysql por defecto viene con dos bases de datos creadas como son Mysql y test, para la visualización de estas bases de datos digitamos el siguiente comando.

```
Mysql> show databases;
```

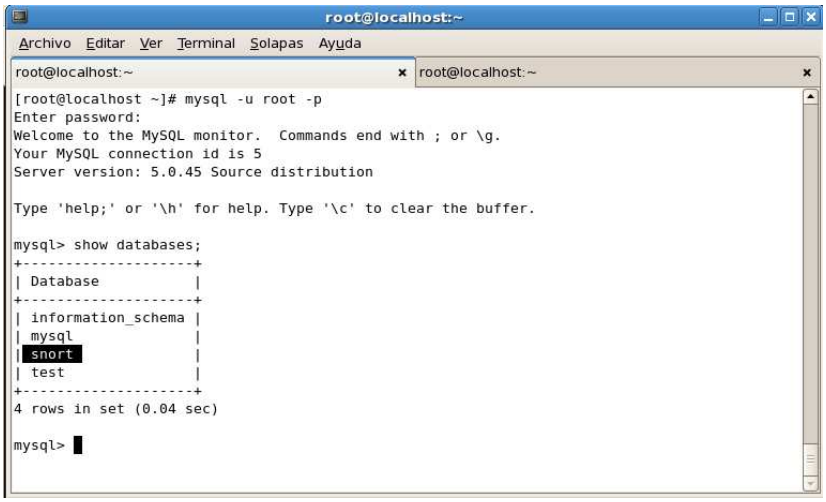


Figura V.20. Visualización de Base de Datos.

VISUALIZAR TABLAS CREADAS

Con el siguiente comando se presentara en pantalla todas las tablas creadas dentro de snort.

```
Mysql> show tables;
```

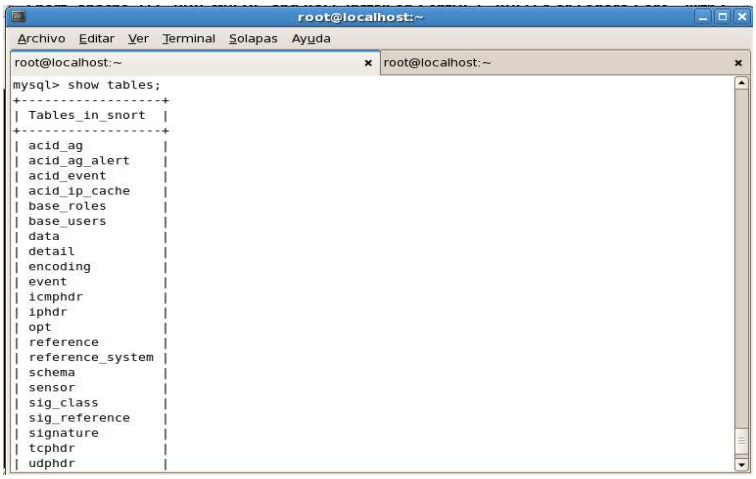


Figura V.21. Visualización de tablas de snort.

CREACION DE REGLAS

Para la creación de reglas se ingresó a la carpeta REGLAS ubicada dentro de Snort_inline.

Figura V.22. Acceso a la Carpeta REGLAS.

En este caso se creó las reglas específicas para el funcionamiento dentro de la red del M.I Municipio de Riobamba en el archivo web-attacks.rules.

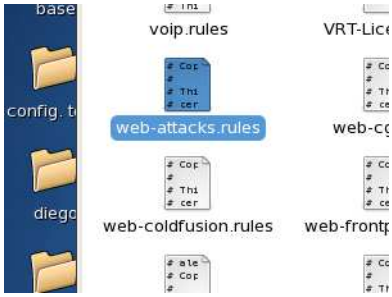


Figura. V.23. Archivo web-attacks.rules

REGLAS CREADAS

Las distintas reglas que se crearon para el bloqueo de diferentes puertos son las siguientes:

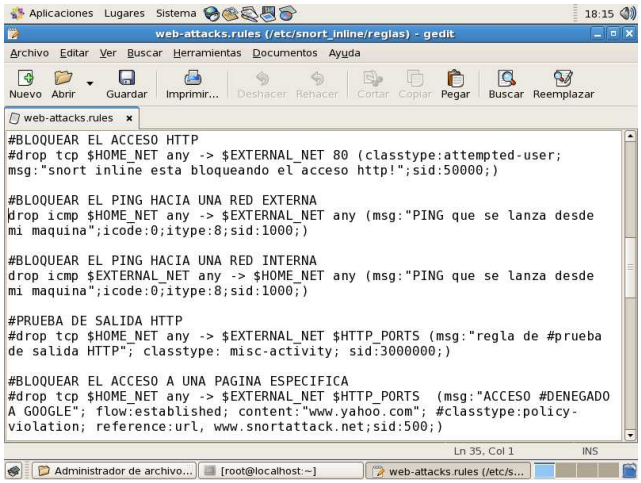


Figura V.24. Reglas Activas.

✓ **Bloqueo del Acceso HTTP**

Esta regla bloquea todo acceso hacia las páginas de internet a través del puerto 80.

Las reglas se conforman de dos partes como son la cabecera y las opciones.

- ***Acción de la regla:*** drop(esta opción envía el paquete por Iptables para su bloqueo)
- Protocolo: tcp
- **Dirección IP origen:** $HOME_NET (toda nuestra red)
- **Puerto IP origen:** any (cualquiera)
- **Dirección IP destino:** $EXTERNAL_NET (toda la red externa)
- **Puerto IP destino:** 80 (puerto que se utiliza para el acceso http)
- **Dirección de la operación:** -> (hacia la red externa)

Opciones

Mensaje: msg (Mensaje de la alerta)

Sid:(identificación de la regla)

✓ **Bloqueo de PING hacia la red interna o hacia la red externa.**

Esta regla como la anterior consiste en bloquear cualquier intento de PING hacia nuestra red y utiliza el protocolo ICMP.

- ***Acción de la regla:*** drop(bloquear el ping a través de Iptables)
- Protocolo: icmp
- **Dirección IP origen:** $EXTERNAL_NET (toda la red externa)
- **Puerto IP origen:** any (cualquiera)
- **Dirección IP destino:** $HOME_NET (toda nuestra red)
- **Puerto IP destino:** any (cualquiera)
- ***Dirección de la operación:*** -> (desde la red externa hacia nuestra red)

Opciones

Mensaje: msg:"ping que se lanza desde la red externa "

Itype: comprobación del valor del campo *type* de la cabecera ICMP en este caso 8.

Sid: identificación de la regla.

Icode: comprobación del valor del campo *code* de la cabecera ICMP en este caso 0.

Bloquear el acceso a una página especifica

- ***Acción de la regla:*** drop(bloquear el acceso a través de Iptables).
- Protocolo: tcp
- **Dirección IP origen:** $HOME_NET (toda nuestra red)
- **Puerto IP origen:** any (cualquiera)
- **Dirección IP destino:** $EXTERNAL_NET (toda la red)
- ***Puerto IP destino:*** HTTP_PORTS (variable puerto 80)
- ***Dirección de la operación:*** -> (dirección hacia la red externa)

Opciones

Mensaje*:* msg:"Acceso denegado a cualquier página especifica"

Content: www.google.com este parámetro nos indica que cualquier paquete que contenga en su campo datos" google.com" será bloqueado a través de su puerto relacionado.

Flow: establishied (conexiones TCP establecidas)

Classtype: policy-violation en este caso va a ser la categoría de la alerta.

Sid: 500 id de la alerta.

Reference: referencia de la regla o pagina de referencia.

- ✓ **Bloquear la descarga de archivos con extensión .mp3**

Acción de la regla: drop (bloquear la descarga a través de Iptables).

Protocolo: tcp

Dirección IP origen: $EXTERNAL_NET (toda la red)

Puerto IP origen: any (cualquiera)

Dirección IP destino: $HOME_NET (toda nuestra red)

Puerto IP destino: any (cualquiera)

Dirección de la operación: -> (dirección hacia la red interna)

Opciones

Mensaje: msg:"Cuidado están descargando archivos mp3 "

Content: extensión del archivo, en este caso" .mp3".

Flags: Establece el contenido de los flags o banderas TCP.

Sid: 333 id de la alerta.

- ✓ **Bloquear el acceso a Messenger**

Acción de la regla: drop(bloquear el acceso a Messenger través de Iptables).

Protocolo: tcp

Dirección IP origen: $EXTERNAL_NET (toda la red)

Puerto IP origen: 1863 (puerto que utiliza Messenger para el inicio de sesión)

Dirección IP destino: $HOME_NET (toda nuestra red)

Puerto IP destino: any(cualquiera)

Dirección de la operación: -> (dirección hacia la red interna)

Opciones

Mensaje: msg:"Inicio de sesión de Messenger "

Content:"http |3A|//", "MSG" contenido en el paquete de datos.

Flow: to_client, establishied(respuesta de servidores y conexiones TCP establecidas)

Classtype: trojan-activity en este caso va a ser la categoría de la alerta.

Sid: 15184 id de la alerta.

Depth:3 (extensión del tamaño de datos que se ha de inspeccionar, en este caso 3.)

Reference: referencia de la regla o página de referencia.

Rev:1 (identificación de la revisión o versión de la regla)

Metadata:(permite integrar información adicional sobre la regla.)

Pcre: (expresiones regulares o extensión de content que describe conjunto de cadenas dentro de content)

- ✓ **Bloquear el escaneo de puertos con nmap**

Acción de la regla: drop(bloquear el escaneo de puertos través de Iptables).

Protocolo: tcp

Dirección IP origen: $EXTERNAL_NET (toda la red)

Puerto IP origen: any(cualquiera)

Dirección IP destino: $HOME_NET (toda nuestra red)

Puerto IP destino: any(cualquiera)

Dirección de la operación: -> (dirección hacia la red interna)

Opciones

Mensaje: msg:"Escaneo Ping con nmap "

Classtype: attempted-recon en este caso va a ser la categoría de la alerta.

Sid: 628 id de la alerta.

Reference: arachnids,28 Referencia un a un Advisory, alerta tipo Bugtrac, etc.

Rev:1 (identificación de la revisión o versión de la regla)

Flags: Establece el contenido de los flags o banderas TCP.

Ack: (indica que se está confirmando la recepción correcta de datos hasta un determinado número de secuencia.)

ARRANQUE DE SNORT IN_LINE

- ✓ **Modos de Control de Snort In_Line**

Hay dos modos de Snort-Inline:

Drop Mode

Un paquete es descartado si coincide con una firma de ataque.

En el proyecto, se usó este modo.

Hay tres opciones disponibles en este modo:

- o **Drop:** Suelta un paquete, envía un restablecimiento de vuelta al servidor, registra el evento.
- o **Sdrop:** Suelta un paquete sin el envío de un restablecimiento de nuevo al servidor.
- o **Ignore:** Suelta un paquete, envía un restablecimiento de vuelta al servidor, no lo incluye en el registro de sucesos

Replace Mode

Un paquete es modificado si coincide con una firma de ataque.

- ✓ **Cargar el módulo del kernel ip_queue.**

Tenemos que cargar el módulo ip_queue y comprobar si se realiza con éxito:

```
[root@localhost ~]#modprobe ip_queue
[root@localhost ~]#lsmod | grep ip_queue
```

Para descargar ip_queue: "modprobe-r ip_queue"

✓ **Configurar iptables para poner a prueba Snort_Inline**

Configurar NetFilter con la herramienta iptables.

A continuación se expone una regla de Netfilter para enviar todo el tráfico entrante a la cola en la que se analizarán en contra de las reglas Snort_Inline.

```
iptables -A INPUT -j QUEUE
```

Comando para verificar las reglas iptables

```
[root@localhost ~]#iptables -L
```

Comando para arrancar el servicio snort_inline

```
[root@localhost ~]#snort_inline -Q -v -c /etc/snort_inline/snort_inline.conf -l
/var/log/snort_inline
```

Q -> el proceso de tráfico en espera

v -> verbose

l -> ruta de registro

c -> Ruta de configuración

SCRIPT DE INICIO PARA EL ARRANQUE DE SNORT_INLINE

Creación de un archivo llamado snort_inlined y añadir el script siguiente para empezar Snort_Inline fácilmente:

```
[root@localhost ~]#vi /etc/init.d/snort_inlined
```

```
#!/bin/bash # / bin / bash
# snort_inline
start(){
# Inicio demonios.
echo "Starting ip_queue module:"
lsmod | grep ip_queue >/dev/null || /sbin/modprobe ip_queue;
echo "A partir de  reglas de iptables:"
# Iptables el tráfico enviado a la cola:
# Aceptar conexiones internas localhost
iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
iptables -A OUTPUT -o lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
# Enviar todas las llamadas entrantes, salientes y redirigir el tráfico a la cola
iptables –A INPUT –i br0 –p 0 –m state –state NEW, RELEATED, ESTABLISHIED –j QUEUE

iptables –A FORWARD –i br0 –p 0 –m state –state NEW, RELEATED, ESTABLISHIED –j
QUEUE

iptables -A INPUT -j QUEUE
iptables -A FORWARD -j QUEUE
iptables -A OUTPUT -j QUEUE
# Inicio Snort_inline
echo "Iniciando snort_inline: "
snort_inline –Q –v -c /etc/snort_inline/snort_inline.conf  -l  / var / log / snort_inline

# -Q -> Proceso de tráfico en espera
# -D -> Ejecutar como demonio
# -v -> Verbose
# -l -> Ruta del registro
# -c ->Ruta de configuración
} )

stop() {
# Detener daemons.
# Detener Snort_Inline
# echo "Apagado de snort_inline: "
killall snort_inline
# Quitar todas las reglas de iptables
# Establece las políticas por defecto para aceptar Netfilter
echo "Extracción de reglas de iptables:"
iptables -F
# -F -> flush iptables
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#-P -> la política por defecto
}
restart(){
stop
start
} )
case "$1" in
start)
start
;;
stop)
stop
;;
restart)
restart
;;
*)
echo $"Usage: $0 {start|stop|restart|}"
exit 1
esac
```

INTERFAZ GRÁFICA BASE

BASE es una interfaz gráfica escrita en PHP utilizado para mostrar los registros generados por la IPS y enviados a la base de datos. Representa el análisis básico y motor de seguridad.

- ✓ **Descargar base**

Para descargar la última versión de BASE se accedió a la siguiente página: http://sourceforge.net/projects/secureideas/files/

Luego se descomprime los archivos y se los coloca en la carpeta correcta:

```
[root@localhost~]#tar-xvf base-1.3.5.tar.gz
[root@localhost ~]#mv /snortinstall/base-1.3.5 /var/www/base
```

- ✓ **Configuración Base**

Para configurar BASE se necesita ADOdb (Active Data Objects Data Base). ADOdb es en realidad una biblioteca de abstracción de bases de datos para PHP. ADODB será un intermediario entre BASE y MySQL, la instalación se realizó con los siguientes comandos:

```
[root@localhost ~]#tar -xvf adodb490.tgz
[root@localhost ~]#mv /snortinstall/adodb /var/www/base/
```

- ✓ **Modificación del archivo de configuración.**

Fijar el archivo base_conf.php.dist abrir base_config.php.dist en el directorio raíz de BASE y cambiar las líneas como se muestra a continuación.

```
$DBlib_path="./adodb";
$DBtype="mysql";
$alert_dbname = snort;
$alert_host = localhost;
$alert_port = "";
$alert_user = snort;
$alert_password = administrador;
$archive_dbname = snort;
$archive_host = localhost;
$archive_port = "";
$archive_user = snort;
$archive_password = administrador;
```

Luego cambiar el nombre del archivo de base_conf.php.dist a base_conf.php

```
[root@localhost ~]# mv /var/www/base/base_conf.php.dist
/var/www/base/base_conf.php
```

Importar las tablas de MySQL base en la base de datos snort:

```
[root@localhost ~]## mysql -u root -p snort <
/var/www/base/sql/create_base_tbls_mysql.sql
```

IMPLEMENTACIÓN DEL PUENTE

Después de configurar Snort_Inline, se debe tener cuidado de colocar el IPS en el lugar correcto en la red.

Un IDS sólo necesita ser conectado a un puerto del switch en el que recibe el tráfico procedente de un espejo de puerto.

Para el IPS, la configuración de la red para un ids no pueden ser utilizadas porque Snort_Inline debe comprobar los paquetes antes de decidirse a rechazar o aceptarlos. Debe ser colocado a lo largo del enlace de red que se desea analizar y configurado como un puente.

Así que se debió tener un mínimo de dos interfaces de redes, aunque tres es mejor porque puede dedicarse un puerto para la gestión del IPS.

- ✓ **Cargar el módulo puente.**

```
[root@localhost ~]#modprobe bridge
```

Se instaló la herramienta para la gestión de puentes:

```
[root@localhost ~]#yum install bridge-utils
```

- ✓ **Configuración de las tarjetas de red**

Configurar la red (/ etc / sysconfig/network-scripts / interfaces).

Ifcfg-br0

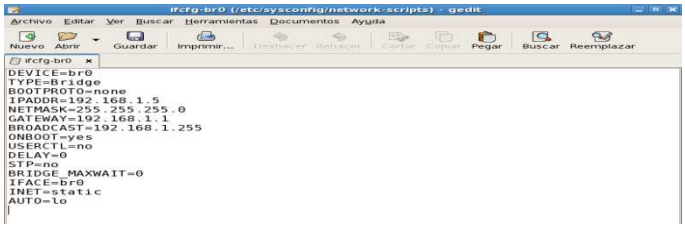


Figura V.25. Script de la Interfaz br0.

Ifcfg-eth0

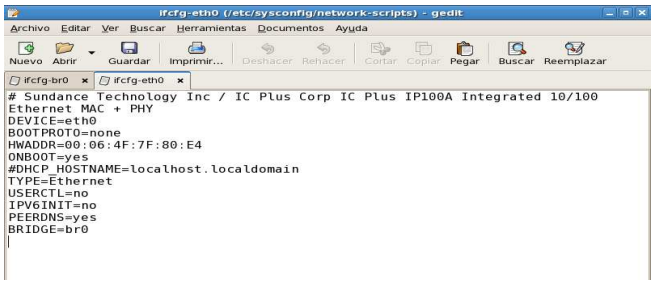


Figura V.26. Script de la Interfaz eth0.

Ifcfg-eth1

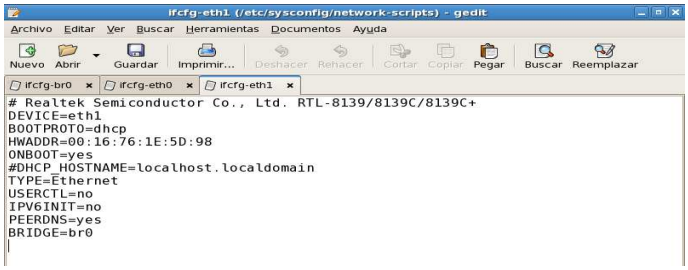


Figura V.27. Script de la Interfaz eth1.

Reinicio de servicios de red.

```
[root@localhost ~]#/etc/init.d/networking restart
```

Se utilizó el comando brctl para ver los miembros del puente.

Comandos Brctl.

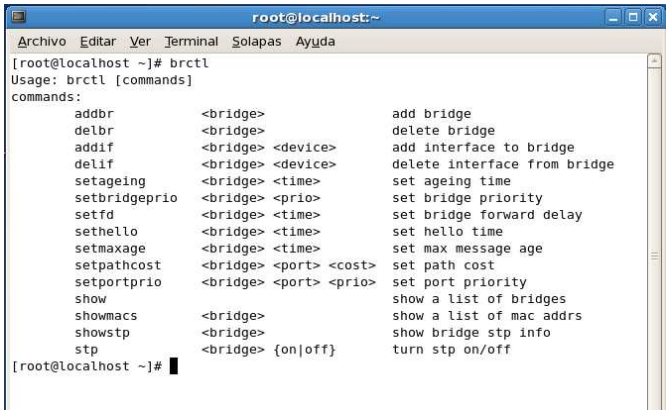


Figura V.28. Comandos Brctl.

Añadir puente br0 con comandos Brctl

```
[root@localhost ~]#brctl addbr br0
```

Añadir interfaces al Puente br0

```
[root@localhost ~]#brctl addif br0 eth0
```

Visualización de Puente e interfaces activadas

```
[root@localhost ~]#brctl show
```

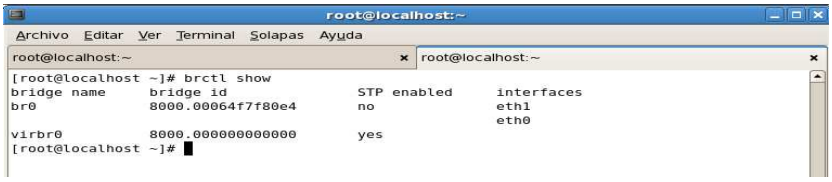


Figura V.29. Interfaces Activas en el Puente br0.

Interfaces de Red activas en el puente

```
[root@localhost ~]#ifconfig
```

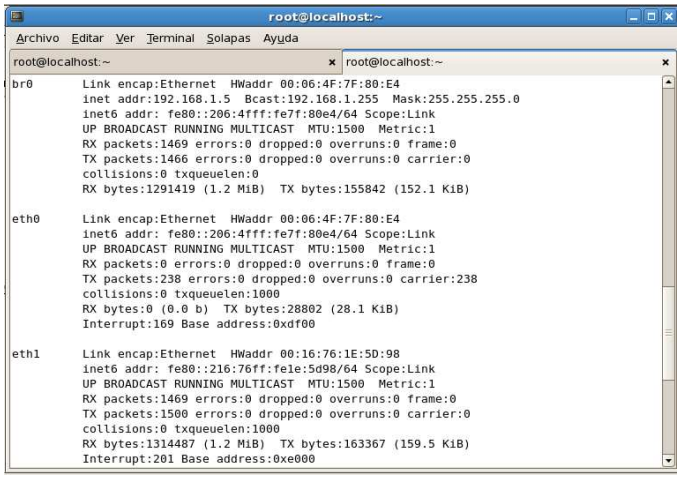


Figura V.30. Interfaces de Red.

✓ **Reiniciar el Servicio de Red**

```
[root@localhost ~]#service networtk restart
```

COMANDOS ESPECIALES SERVICO SNORT

Terminal del Centos.

Figura V.31. Terminal de Centos.

Inicio de servicio snort_inline

```
[root@localhost ~]# etc/init.d/snort_inlined start
```

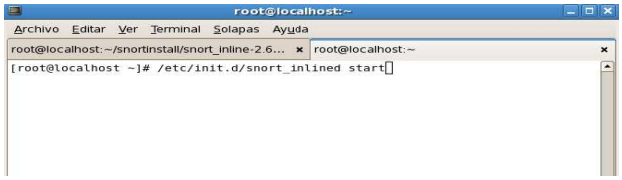


Figura V.32. Inicio del Servicio Snort.

Arrancar el servicio snort_inline

Detalles de compilación de base de datos mysql.

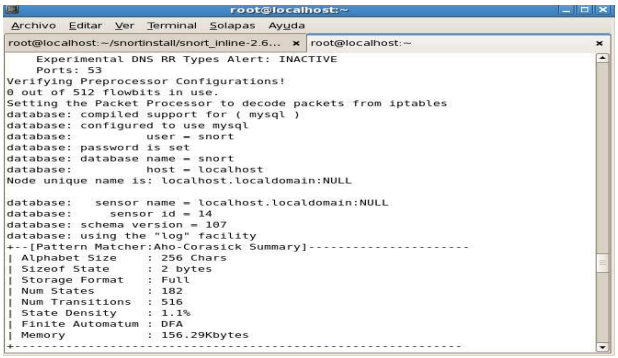


Figura V.33. Detalles de arranque de Snort.

Arranque completado.

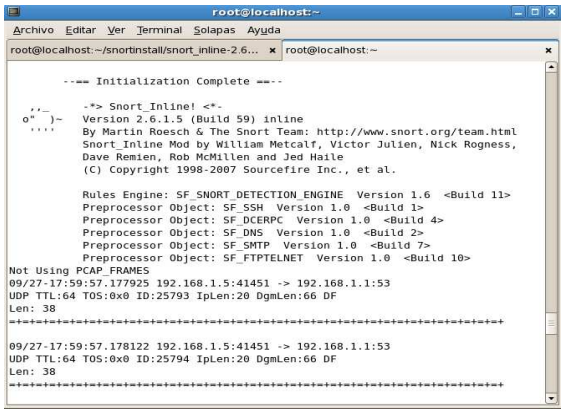


Figura V.34. Arranque Completo de Snort.

Trafico que pasa a través del sensor

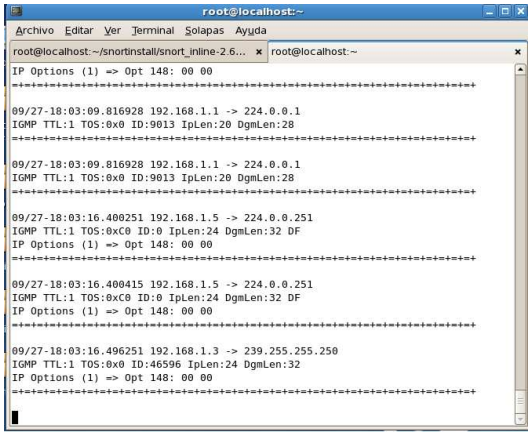


Figura V.35. Visualización de tráfico que pasa a través de nuestro IPS.

VISUALIZACIÓN DE ALERTAS EN LA PANTALLA TERMINAL

El comando necesario para visualizar las alertas sin tener que ingresar a BASE es el siguiente:

```
[root@localhost ~]# tail –f /var/log/snort_inline/snort_inline-fast
```

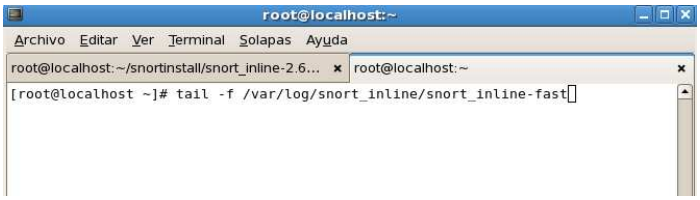


Figura V.36. Comando Para Visualizar Alertas Generadas por Snort.

Alertas según la regla de ping

Estas alertas son generadas por snort al realizar un ping desde una estación de trabajo como atacante.

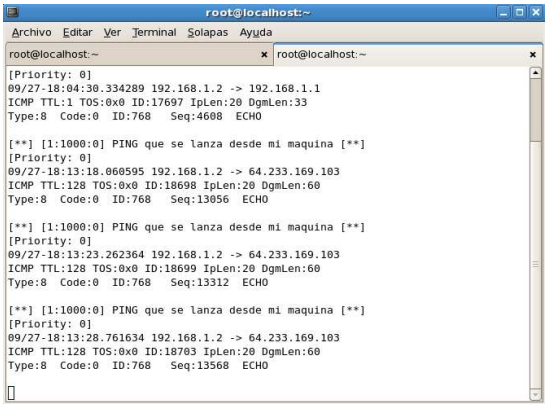


Figura V.37. Alertas generadas por Snort.

Detener el servicio snort_inline

El siguiente comando se utiliza para dejar de utilizar el servicio SNORT_INLINE

```
[root@localhost ~]#/etc/init.d/snort_inlined stop
```

Figura V.38. Pantalla de Finalización de Servicio.

INGRESO Y ADMINISTRACION DE BASE

Acceso

El ingreso a Base se lo realiza colocando la siguiente dirección de Url en el navegador firefox:

```
Http://localhost/base
```

El ingreso a Base a través de otra máquina de la red se lo realiza de la siguiente manera:

Http://192.168.0.5/base

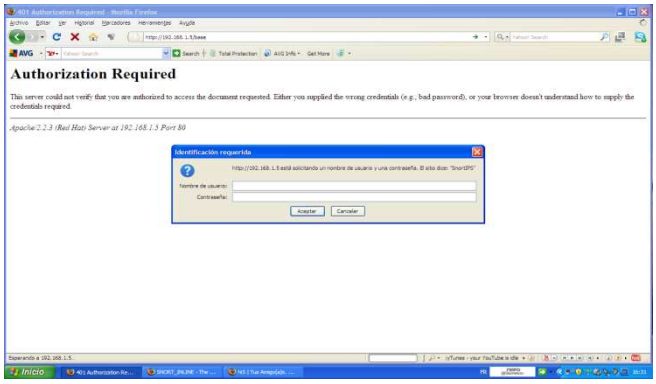


Figura V.39. Pantalla de Ingreso a Base.

Para el acceso a la página principal de base se ingresa el nombre de usuario y contraseña los cuales son:

Nombre de usuario: **base**

Contraseña: **administradorbase**

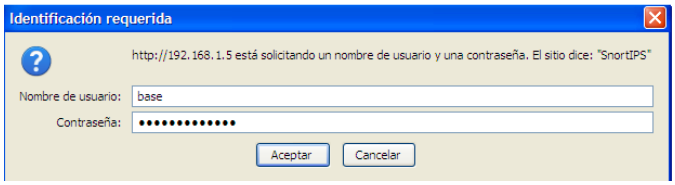


Figura V.40. Ingreso a BASE Mediante Nombre de Usuario y Contraseña.

Página Principal De BASE

En la página principal de base podemos visualizar el sensor que está trabajando así como el porcentaje de las diferentes alertas con cada uno de sus protocolos.

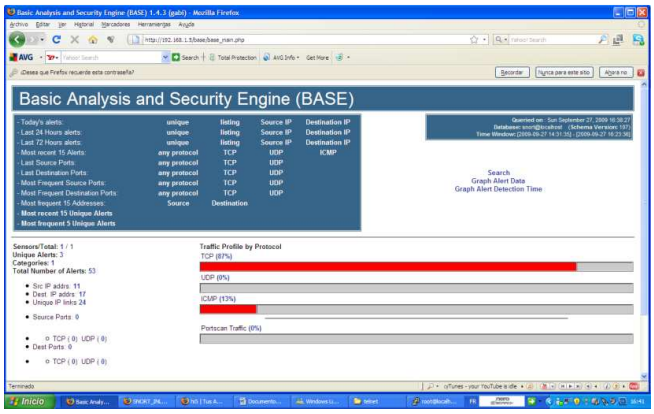


Figura V.41. Pantalla principal de BASE.

Para visualizar todas las alertas clasificadas por protocolo solamente realizamos un click sobre TCP (%) y se nos mostrara todas las alertas que se han generado, seguido de la fecha, direcciones IP origen, destino y su respectivo protocolo, en este caso TCP.

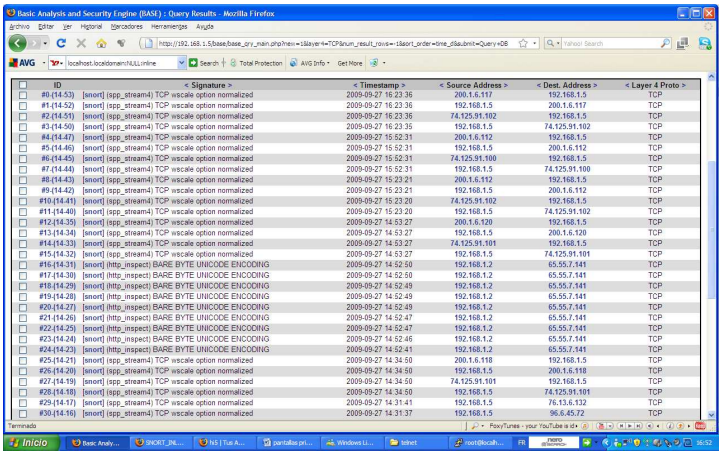


Figura V.42. Alertas Generadas por Snort.

Al momento de seleccionar otro protocolo en este caso sobre ICMP se visualizan todas las alertas generadas por la ejecución de un Ping hacia la red interna o viceversa, conjuntamente con todos los parámetros descritos anteriormente.

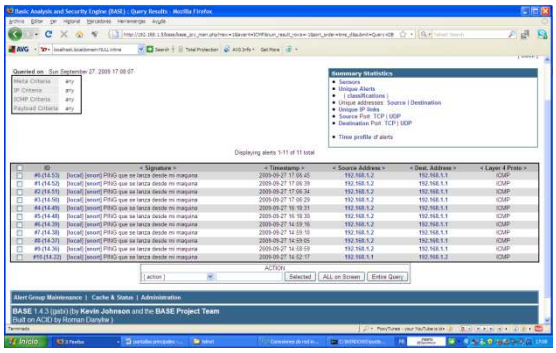


Figura V.43. Alertas Generadas por PING desde un Atacante.

Resumen Estadístico

En este cuadro tenemos muchas opciones para la visualización de los sensores que están trabajando así mismo estadísticas generales de todas las alertas, direcciones IP, protocolos de origen y destino.

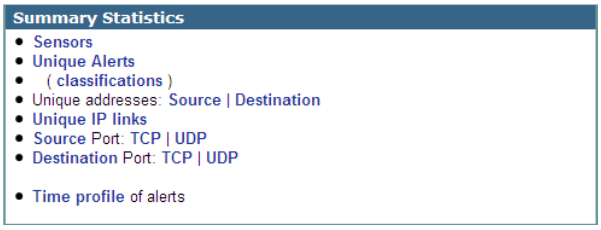


Figura V.44. Estadísticas de BASE.

Sensores

Se visualiza el sensor que está trabajando en el servidor y va a tener el nombre de localhost.localdomain: NULL:inline con el número total de eventos o alertas, así mismo con las direcciones IP origen y destino.

Figura V.45. Sensores activos en BASE.

Alertas Únicas

En esta sección se visualiza todas las alertas que han pasado a través del sensor.

Figura V.46. Visualización de Alertas que Cruzaron por un Sensor Especifico.

Búsqueda de Alertas

La búsqueda de las alertas las podemos realizar por detalles es decir por el sensor que las generó, fecha en la que se generó la alerta, grupo al que pertenece, es decir para la búsqueda especifica según lo amerite el caso.

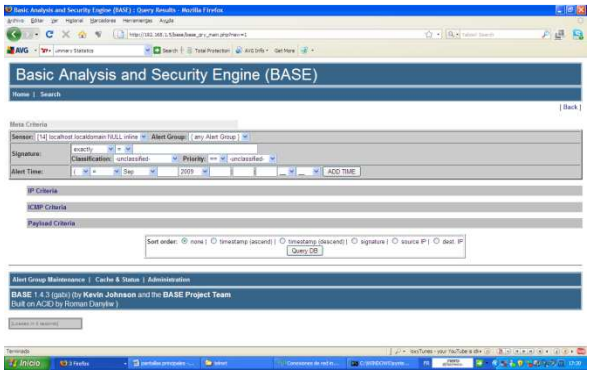


Figura V.47. Búsqueda de Alertas.

CONCLUSIONES

- ✓ La implementación de la metodología de Prevención de Intrusos propuesta en el proyecto mejoró el nivel de seguridad de la información que maneja el I. Municipio de Riobamba en un 25%.
- ✓ El análisis de seguridad realizado en el I. Municipio de Riobamba fue de gran importancia para la posterior creación de reglas específicas para los distintos bloqueos de conexiones no seguras.
- ✓ Cada una de las fases de la metodología desarrollada conlleva a un estudio específico del funcionamiento de la entidad en base a su topología de red.
- ✓ El uso de herramientas de software libre permite diferenciar claramente la relación rendimiento/costo, además de tener la certeza de desarrollar aplicaciones legales en la mayoría de los casos.
- ✓ La decisión del uso de software libre para el desarrollo del IPS se debe en gran parte a la variada y certera información que podemos encontrar en la web sobre estos productos.
- ✓ Una metodología de prevención de intrusos protege a la red pero solo dentro del ámbito de la protección lógica.
- ✓ Promocionar una cultura de seguridad requiere de un liderazgo fuerte con una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planificación y administración de la Seguridad.
- ✓ Los fundamentos de las diferentes normas y metodologías vigentes en la actualidad permitió crear una metodología de prevención de intrusos sólida y confiable para mejorar la seguridad del I. Municipio de Riobamba.
- ✓ Los requerimientos de Hardware del servidor se eligió en base a la carga de tráfico existente dentro de la red del I. Municipio de Riobamba.

- ✓ Los resultados obtenidos al poner en marcha el IPS implementado permitieron determinar el grado de mejora de la seguridad de la información en el IMR.
- ✓ Durante las pruebas realizadas el servidor en funcionamiento no produjo una baja en el rendimiento de la red del I. Municipio de Riobamba, lo que motivó a su pronta adopción como parte de las mejoras de la seguridad.

RECOMENDACIONES

- ✓ Para el buen funcionamiento de un IPS se debe manejar responsablemente el archivo de configuración para que los paquetes que pasan por la red no sean bloqueados por error.
- ✓ Para poder instalar Snort sin problemas se debe tener configurado anteriormente todas las librerías necesarias y así ayudar a su rápida ejecución.
- ✓ Los requerimientos de hardware para el servidor donde se montará el IPS deben ser en base al tráfico que circula por la red ya que la acumulación de alertas podría sobrecargar el servidor.
- ✓ Al momento de la ejecución del IPS se debe tener cuidado con las alertas llamadas "falsos positivos" ya que son falsas alarmas generadas el software y se les debe dar un adecuado tratamiento.
- ✓ Se recomienda seguir minuciosamente todos los pasos descritos en el desarrollo de la metodología, puesto que cada una de las fases citadas depende directa o indirectamente de la anterior.
- ✓ Se debe realizar un estudio de la topología de red para determinar la ubicación del IPS y así bloquear todas las conexiones no seguras que provienen del internet.
- ✓ Antes del diseño de una metodología de seguridad, es necesario determinar adecuadamente las metodologías que servirán de base para el desarrollo dando prioridad a aquellas que están en vigencia en el país y que se enmarquen en nuestros objetivos.
- ✓ Se recomienda seguir aportando al desarrollo de software libre, pues en un futuro cercano se cree que será predominante al software propietario.
- ✓ Se recomienda complementar esta metodología con el desarrollo de un sistema orientado a seguridad física y ambiental de la red.

RESUMEN

Se ha implementado una Metodología de Prevención de Intrusos en la red informática del M.I. Municipio de Riobamba, con el objetivo de mejorar el nivel de seguridad de la información digital de la entidad.

Se usó un computador Pentium IV donde se instalaron Cento5 y Snort, que permitieron que ésta actué como un sistema de prevención de intrusos informáticos; se investigó aplicando métodos inductivo y deductivo y técnicas del análisis de paquetes web y comparación de metodologías de seguridad estandarizadas.

El análisis previo del nivel de seguridad en la red informática indicó que éste se mantiene en un 45%, por lo que se implementó una metodología que consta de dos fases: la de análisis y la de gestión del riesgo; la primera comprende el análisis del entorno y la seguridad; la segunda, el plan de gestión y la implementación del Sistema de Prevención de Intrusos, fase que se la desarrolló, obteniéndose como resultado el incremento del nivel de seguridad a un 70%, consiguiéndose una mejora del 25%.

Se recomienda al Departamento de Sistemas de la entidad, mantenga la aplicación de la metodología y complemente con el desarrollo de un sistema orientado a seguridad física y ambiental de la red, puesto que la seguridad lógica se halla ya protegida en esta investigación, lo que permitiría una funcionalidad del 100% de la misma.

SUMMARY

A methodology of virus prevention has been implemented in computer science's net With the objective of improving the level of security of the digital information of the entity.

It was used a computer Pentium IV in which it is installed cento5 and Snort that allowed that this acted as a system of computer virus prevention in computer science's net ; it was investigated applying inductive and deductive and technical methods of analysis of packages web and comparison of methodology of standard security .

The previous analysis of the level of security in the computer net indicates that this stays in 45% for what you implements a methodology that consists of two phases; one of them is analysis and rescue intervention; the first is environment and security; the second, the administration plan and the implementation of the system of virus prevention phase that it was developed being obtained the increment of level of security as a result 70% being gotten an improvement of 25%.

It is recommended to the Department of systems of the entity, maintain the application of the methodology and supplement with the development of a system guided to physical and environmental security of the net, since the logical security it is already protected in this investigation, what would allow a functionality of the 100% the same one.

GLOSARIO

Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Framework: estructura conceptual y tecnológica de soporte definida, normalmente con artefactos o módulos de software concretos, en base a la cual otro proyecto de software puede ser organizado y desarrollado.

Impacto: medir la consecuencia al materializarse una amenaza.

IPTABLES: Herramienta de cortafuegos que permite filtrar paquetes, realizar traducción de direcciones de red (NAT) para IPv4 y mantener registros de log.

Libipq: librería de desarrollo para iptables paquete de espacio de usuario de cola.

Linux: Término empleado para referirse al sistema operativo libre similar a Unix que usualmente utiliza herramientas de sistema GNU.

MySQL: Sistema de gestión de base de datos relacional, multihilo y multiusuario.

Netfilter: framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red.

Nmap: programa de código abierto que sirve para efectuar rastreo de puertos.

Riesgo: Cuando no se tiene alguna aplicación informática como antivirus y/o similares para proteger el equipo.

root: Nombre convencional de la cuenta de usuario en Centos que posee todos los derechos en todos los modos.

Snort: Sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión).

TELNET: Protocolo de red, utilizado en Internet para acceder remotamente a una máquina o servidor.

Unix: Sistema operativo portable, multitarea y multiusuario.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

ANEXOS

MANUAL DE USUARIO

MANUAL DE USUARIO

INTRODUCCION

La seguridad en las redes ha comenzado a ser un problema importante en el mundo moderno. El número de computadoras, la conectividad entre ellas y la importancia que han adquirido en el desarrollo tanto investigativo como empresarial, convirtiéndolas en las principales portadoras de información sensible que requiere no ser alterada y muchas veces no ser consultada por personal no autorizado.

Esto ha hecho que los ordenadores y las redes puedan verse involucrados en un ataque informático siendo las herramientas utilizadas para cometer dicho ataque, siendo las víctimas del ataque o pudiendo ser utilizadas para propósitos incidentales relacionados con la irrupción.

En el M.I Municipio de Riobamba conjuntamente con su departamento de Sistemas manejan bases de datos de mucha importancia que requieren ser protegidas de posibles ataques informáticos, razón por la cual se ha decidido proponer una metodología de seguridad.

Esta metodología consiste en la implementación de un sistema de prevención de intrusos (PS), estos sistemas conforman la nueva tecnología de seguridad informática para protección de servidores y redes que bloquean de forma eficiente ataques externos e internos y todo tipo de amenazas conocidas y desconocidas.

Los IPS aparecieron como una evolución de los IDS, los IPS no se limitan a escuchar y monitorear el tráfico de la red sino que intervienen activamente ya que el tráfico circula a

Través del sistema y cualquier intento de ataque será bloqueado por el IPS en el mismo momento en que el evento ocurre.

Para lograr este objetivo se ha decidido trabajar con la plataforma LINUX bajo la distribución de CENTOS 5.3, fue necesaria además la utilización de un sniffer de paquetes basado en red llamado Snort.
El Snort es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL.

Conjuntamente con Snort trabaja un conjunto de reglas creadas en acuerdo con el administrador de la red institucional y los proponentes del proyecto con el fin de bloquear puertos que permitan el acceso a servidores y a la LAN interna del municipio de Riobamba.

Para levantar el servicio se implementó un puente red o bridge a través de dos interfaces de red para el tráfico de los paquetes que serán analizados por el Snort; con el fin de que se realice adecuadamente la generación de alertas para su posible toma de decisión de acceso o deniego de éstos, a través del IP Tables y según las normas que se han creado.

Las alertas generadas se almacenan en una base de datos diseñada en MySQL y éstas a su vez se visualizan a través de una interfaz gráfica denominada BASE (de su acrónimo en inglés Base Analysis and Security Engine)

Gracias a esta herramienta somos capaces de ver los detalles de un ataque como son las direcciones IP origen y destino, así como los protocolos y puertos que se han utilizado para el tráfico de las tramas; nos sirve además para realizar una administración en lo referente a creación de usuarios, así como también nos permite realizar búsquedas detalladas de las alertas generadas por el Snort, permitiendo su visualización por fechas específicas, direcciones que generan la alerta y sensores por los cuales accedió el tráfico de los paquetes.

Para el caso particular y según las necesidades del municipio de Riobamba las reglas que estamos utilizando son las siguientes:

- Bloqueo del protocolo ICMP para evitar el ping desde una red externa hacia la red externa y viceversa.
- Bloqueo para la descarga de archivos con extensión .mp3 para evitar consumo de ancho de banda innecesario.
- Bloqueo de acceso o inicio de sesión en Windows Live Messenger.
- Bloqueo de acceso a páginas web específicas como por ejemplo www.hi5.com, www.facebook.com, www.sexofree.org, www.cdadulto.com, pomstarstart.com, www.actrizpornoxxx.com.
- Bloqueo de escaneos de puertos con nmap.

Luego de esta breve descripción se procederá a realizar un sumario explicativo de todo los pasos concernientes para la implementación del IPS así como también de su manejo luego de concluido.

CARACTERISTICAS DEL EQUIPO UTILIZADO

Para instalar un servidor de Snort es importante tener en cuenta qué tráfico esperamos manejar. Snort puede ejecutarse en casi cualquier tipo de hardware.

Pero de todos modos, si queremos tener un IPS rápido y fiable sin un alto porcentaje de paquetes perdidos, Snort necesitará un procesador relativamente potente. Sobra decir que necesitaremos además espacio de almacenamiento para los registros y alertas. El elemento más crítico, sin embargo, es una buena interfaz de red. Siempre que nos sea posible, nos aseguraremos de que la interfaz de red es dedicada, y nunca integrada en la placa base. La mayoría de los fabricantes actuales ofrecen una tarjeta de red especial para servidores, con un procesador integrado específicamente diseñado para el procesamiento del tráfico de red.

Como requerimientos mínimos del sistema del equipo que sirvió como un IPS fueron los siguientes:

Procesador	Intel Inside Pentium IV 3.0 GHZ
Disco Duro	ATA Samsung 80 Gb
Tarjetas de Red	Realtek Semicponductor
	Sundance Technology PCI
RAM	512 Mb

Tabla V.1. Requerimientos de hardware.

DESCARGA Y AlMACENAMIENTO DE PROGRAMAS Y DEPENDENCIAS

Creación de la Carpeta **Snortinstall** para el almacenamiento de los diferentes programas y dependencias descargados.

Todo el procedimiento de creación de carpetas y configuración se lo realiza bajo el usuario root.

En la consola Terminal se creó el directorio bajo /root llamado snortinstall, el comando para la creación es el siguiente:

```
[root@localhost ~]# mkdir
```

En la carpeta snortinstall se ubicó los siguientes archivos de instalación descargados:

Snort_Inline-2.6.1.5

BASE

ADODB

Programas necesarios para ejecutar Snort_Inline y BASE:

La instalación de los programas se lo realizó a través de paquetes YUM.

MySQL 5.0.9

MySQL Servidor de base de datos.

Comando para instalación

```
[root@localhost ~]#yum  -y install mysql mysql-server
```

PHP 5.2

Lenguaje de secuencia de comandos

Comando para instalación

```
[root@localhost ~]#yum install php5
```

Compiladores y PHP5-MySQL

Compiladores para poder instalar todos los paquetes utilizados en Snort_Inline

Comando para instalación

```
[root@localhost ~]#yum install *gcc* *pcre* libdnet php-adodb php-mysql php-gd
```

BUILD-ESSENTIAL 11,1

Meta paquete que contiene las herramientas para compilar e instalar programas.

Comando para instalación

```
[root@localhost ~]#yum install build-essential
```

PCRE 6.4.1

Biblioteca de funciones que usa la misma sintaxis y semántica que Perl 5.

Comando para instalación

```
[root@localhost ~]#yum install libpcre3-dev
```

IPTABLES-DEV 1.3.5

Conjunto de reglas de filtrado de paquetes de Linux.

Comando para instalación

```
[root@localhost ~]#yum install iptables-dev
```

LIBDNET 1.0.2a-7

Genérico API de red que proporciona acceso a varios protocolos.

Comando para instalación

```
[root@localhost ~]#yum install libdnet-dev
```

MYSQLCLIENT LIBRARY 4.0.24

Bibliotecas de desarrollo de MySQL y archivos de cabecera.

Comando para instalación

```
[root@localhost ~]#yum install libmysqlclient10-dev
```

LIBDNET 1,11

Interfaz con varias rutinas de red de bajo nivel incluyendo:

Manipulación de direcciones de red.

Cortafuegos de red.

Búsqueda y manipulación de interfaces de red.

Transmisión de tramas Ethernet.

Instalación

Como no hay paquetes disponibles para libdnet se instaló de forma manual:

Descargar libdnet y descomprimirlo

```
[root@localhost ~]#tar -xvf libdnet-1.11.tar.gz
```

Ubicarse en el directorio de acceso lidbnet e instalar la biblioteca:

```
[root@localhost~]#cd/libdnet-1.11
[root@localhost libdnet-1.11~]#./configure
[root@localhost libdnet-1.11~]#make
```

INSTALACIÓN DE SNORT_INLINE

Para que Snort_inline analice el tráfico de un segmento de red, debió ser añadido, de forma transparente y por medio de dos tarjetas en modo bridge, con funcionalidad inline. Dicha funcionalidad se consiguió conduciendo el tráfico a través de iptables (ip_queue). Sin embargo, esto no es suficiente porque necesitamos saber, a través de las iptables, que tráfico añadir. Gracias a este modo, Snort_inline, se puede convertir como

cualquier otro sistema de prevención de intrusiones y bloquear las conexiones que reciba. Para actuar de este modo, Snort fue compilado para conseguir respuestas flexibles que permitan restaurar el tráfico que debería ser bloqueado.

Para concluir, podemos decir que Snort_inline es definitivamente el modo más efectivo y preciso disponible; ya que controla el tráfico basándose en reglas cargadas previamente.

Una vez descargados e instalados las herramientas adicionales a necesitar para que Snort_Inline se configure con éxito, se procedió a la instalación de nuestro IPS.

Descarga y Configuración

La versión de snort que se utilizó en el proyecto fue **snort_inline-2.6.1.5.**

Descargar Snort_Inline y descomprimirlo.

```
[root@localhost snortinstall ~]#tar -xvf snort_inline-2.6.1.5.tar.gz
```

Crear dos directorios, uno para almacenar los archivos de configuración, y el otro para almacenar las reglas de Snort.

```
[root@localhost ~]#mkdir /etc/snort_inline
[root@localhost ~]#mkdir
```

Directorio para el almacenamiento de alertas.

Todas las alertas generadas por snort se almacenaran en esta carpeta.

```
[root@localhost ~]#mkdir
```

Copiar los archivos de configuración de Snort_Inline-2.6.1.5 dentro del directorio creado:

```
[root@localhost ~]#cp snort_inline-2.6.1.5/etc/* /etc/snort_inline/
```

ARCHIVO DE CONFIGURACION DE SNORT_INLINE

La configuración del IPS se cambió de acuerdo a la red del IMR a proteger, el archivo maestro que se editó fue snort_inline.conf con los siguientes parámetros:

Variables de Red

var HOME_NET 192.168.1.0/24

Red Interna a proteger, en este caso se definió la dirección de red que está en uso dentro del IMR.

var EXTERNAL_NET any

Red externa (Internet por ejemplo):

var SMTP_SERVERS any

Proteccion de servidores SMTP que se encuentran dentro de nuestra red, en este caso definimos any.

var TELNET_SERVERS any

Proteccion de servicios TELNET en la red interna.

var HTTP_SERVERS any

Proteccion de servicios Web dentro de nuestra red.

var SQL_SERVERS any

Proteccion de servidores de Base de Datos existentes en la red.

var DNS_SERVERS any

Proteccion de servicios DNS.

var HTTP_PORTS 8080

Variable del puerto 8080

var SHELLCODE_PORTS !80

Variable activa para puertos de codigo Shell

var ORACLE_PORTS 1521

Variable activa para puertos Oracle

var SSH_PORTS 22

Variable para puertos de conexiones no seguras SSH

Preprocesadores

Se trata de pequeños plugins programados normalmente en C que sirven para tratar los paquetes provenientes del Decodificador. El tratamiento que realiza sobre los paquetes es para darle forma de manera que se pueda interpretar la información de los paquetes de forma más sencilla y lógica. Una vez reordenados los paquetes, al pasar por el motor de Detección se le aplicarán las Reglas en busca de patrones de ataques,virus, información, etc.

Los preprocesadores pueden defragmentar paquetes, ordenarlos, decodificar URLs, reensamblar, etc.

Estos preprocesadores se configuran en el archivo maestro de configuración etc/snort_inline.conf

Preprocesadores utilizados

Flow

Este preprocesador es requerido para que otros preprocesadores puedan funcionar, tales como flowbits detection plug-in y flow-portscan, los preprocesadores Flow permiten a Snort mantener sus mecanismos de adquisición de datos. Sus funciones son:

• stats_interval: este parámetro especifica el intervalo de tiempo expresado en segundos tras el que queremos que Snort vuelque las estadísticas en stdout.

• Hash: este parámetro especifica el método hash, usando el valor 1 definimos un hash por byte.

```
preprocessor flow: stats_interval 0 hash 2
```

Stream4

Este preprocesador da a Snort la habilidad de ver la base del paquete y donde fue generado (cliente o servidor), este preprocesador tiene la capacidad de re-ensamblaje de streams y almacenar los más recientes ataques no declarados. Sus funciones son:

• disable_evasion_alerts: esta opción se usa para desactivar las alertas escritas en stream4.

midstream_drop_alerts: le dice al preprocesador que bloquee las conexiones generadas sin establecer un flow determinado.

• Rpc decode: este preprocesador re-ensambla un flujo rpc en un sólo paquete para que sea más fácil de analizar, si el preprocesador stream4 está presente, sólo analizará el tráfico proveniente del cliente.

• Telnet decode: este preprocesador normaliza el flow de caracteres de un protocolo telnet en una sesión. Debemos especificar los puertos a analizar.

log: hace un log en un archivo o base de datos.

• Pass: ignora el tráfico que ha encontrado.

• Drop: pasa el paquete a través de las iptables y lo guarda en un archivo o base de datos.

• Reject: si es un TCP resetea la conexión a través de las iptables, si es UDP manda un mensaje icmp host unreachable y hace un log en un archivo o base de datos.

• Sdrop: pasa el paquete a través de iptables y no lo archiva.

```
preprocessor stream4:  disable_evasion_alerts, \
                       stream4inline, \
                       enforce_state drop, \
                       memcap 134217728, \
                       timeout 3600, \
                       truncate, \
                       window_size 3000,\
                       disable_ooo_alerts
```

HTTP Inspect es un decodificador HTTP genérico para aplicaciones de usuario. Dado un búfer de datos, HTTP Inspect decodificará el buffer, encontrara campos de HTTP, y los normalizara. HTTP Inspect inspeccionara las solicitudes de los clientes y las respuestas del servidor.

Dentro de HTTP Inspect, hay dos áreas de de configuración: global y el servidor.

```
preprocessor http_inspect: global \

                    iis_unicode_map unicode.map 1252
```

preprocesador especialmente diseñado para el troyano *Back Orifice*.

```
preprocessor bo
```

Conexión a Reglas utilizadas

Para la conexión a las distintas reglas que se utilizaran en el IPS se lo hará por la siguiente variable definida a continuación:

```
var RULE_PATH /etc/snort_inline/reglas
```

Salida y almacenamiento de las diferentes alertas generadas por Snort.

El modo de Alerta Completa nos devolverá 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

```
output alert_full: snort_inline-full
```

El modo Alerta Rápida nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación , prioridad de la alerta, IP y puerto de origen y destino.

```
output alert_fast: snort_inline-fast
```

Configuracion de los *Output Plugins*, que definen a donde tienen que ir a parar los logs que Snort genera. Estos deciden si van a ser ficheros de texto (logs) o a una base de datos, y decide también en que formato irán escritos (binario, texto plano, xml...). Como nos interesa poder acceder a los datos desde BASE y éste está escrito en PHP, diremos que guarde la salida en la base de datos MySQL previamente definiendo una contraseña y un usuario.

```
output database: log, mysql, user=snort password=administrador
dbname=snort host=localhost
```

Reglas utilizadas para la protección de la red del IMR.

```
#include $RULE_PATH/exploit.rules
#include $RULE_PATH/finger.rules
#include $RULE_PATH/local.rules
#include $RULE_PATH/ftp.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/rpc.rules
#include $RULE_PATH/rservices.rules
#include $RULE_PATH/dos.rules
#include $RULE_PATH/ddos.rules
#include $RULE_PATH/dns.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/web-iis.rules
#include $RULE_PATH/web-frontpage.rules
#include $RULE_PATH/web-misc.rules
#include $RULE_PATH/web-client.rules
#include $RULE_PATH/web-php.rules
#include $RULE_PATH/sql.rules
#include $RULE_PATH/x11.rules
```

```
### Disabled

#include $RULE_PATH/other-ids.rules

#include $RULE_PATH/backdoor.rules

#include $RULE_PATH/shellcode.rules

#include $RULE_PATH/policy.rules

include $RULE_PATH/porn.rules

#include $RULE_PATH/info.rules

#include $RULE_PATH/icmp-info.rules

#include $RULE_PATH/chat.rules

#include $RULE_PATH/multimedia.rules

#include $RULE_PATH/p2p.rules

#include $RULE_PATH/spyware-put.rules

### Bleeding Rules

# include $RULE_PATH/bleeding.rules

include $RULE_PATH/scan.rules

# include $RULE_PATH/bleeding-attack_response.rules

# include $RULE_PATH/bleeding-botcc.rules

# include $RULE_PATH/bleeding-dos.rules

# include $RULE_PATH/bleeding-dshield.rules

# include $RULE_PATH/bleeding-exploit.rules

# include $RULE_PATH/bleeding-game.rules

# include $RULE_PATH/bleeding-inappropriate.rules

# include $RULE_PATH/bleeding-malware.rules
```

COMPILACION DE SNORT_INLINE

Al terminar la configuración del archivo snort_inline.conf se procedió a la compilación de snort con los parámetros establecidos, los siguientes comandos a utilizarse son los siguientes:

Procedimiento para la compilación:

Para la compilación se ubico dentro de la carpeta snort_inline-2.6.1.5 con los siguientes comandos:

```
[root@localhost ]#cd snortinstall

[root@localhost  snortinstall ]#cd snort_inline-2.6.1.5
```

Comando para la compilacion de Snort_inline con mysql:

```
[root@localhost  snortinline-2.6.1.5]# ./configure – with-mysql

[root@localhost  snortinline-2.6.1.5]#make
```

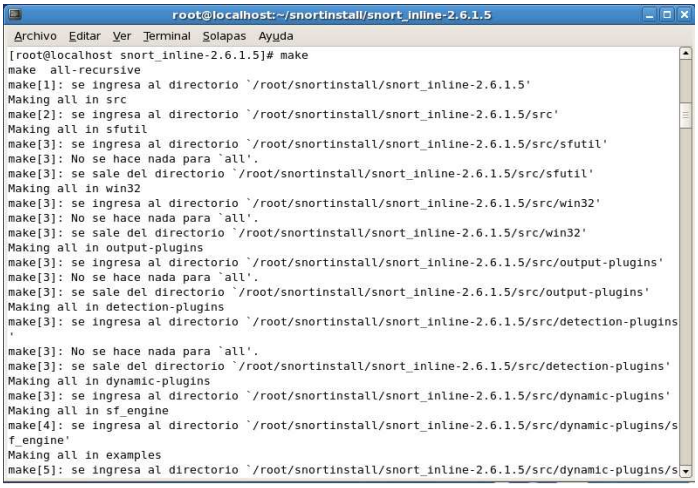


Figura V.1. Pantalla de resultados al digitar el comando make.

```
[root@localhost  snortinline-2.6.1.5]#make install
```

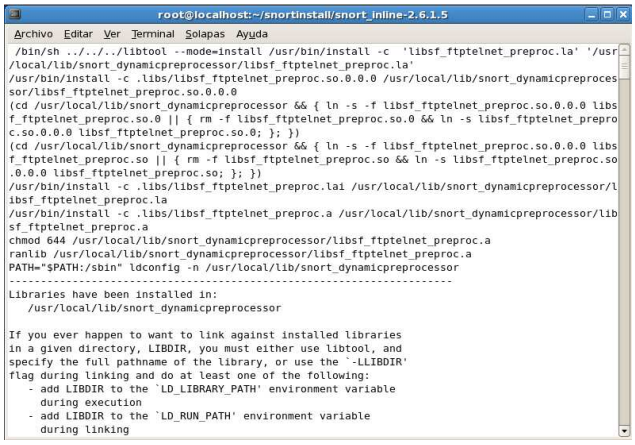


Figura V.2. Pantalla de resultados al digitar el comando make install.

Configuración MYSQL

La configuración de la base de datos se divide en varios apartados. Primero debemos elegir una contraseña adecuada, crear la base de datos necesaria y definir la estructura de las tablas. Nos conectamos como *root* al servicio de MySQL y creamos la base de datos y los permisos para *snortusr*. Para abrir la línea de comandos de MySQL ejecutaremos *mysql -u root -p* desde la terminal.

Luego se pide la contraseña del usuario root y entramos al intérprete de *mysql*>. En él introducimos los siguientes comandos para la finalización del primer apartado de la configuración (hemos de asegurarnos de que cada línea termina con un punto y coma ";").

Ingreso a Mysql con el usuario root.

```
[root@localhost ~]#mysql  -u root –p
```

Ingreso de contraseña

La contraseña a utilizar va a ser **administrador**

```
Enter password: administrador
```

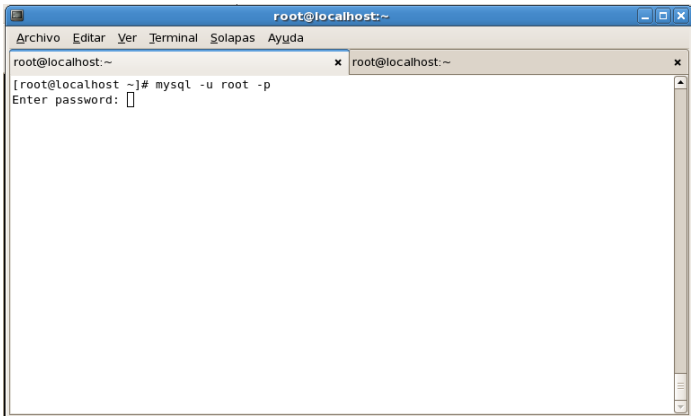


Figura V.3. Ingreso a MySql con el usuario root y contraseña .

Interfaz de Mysql

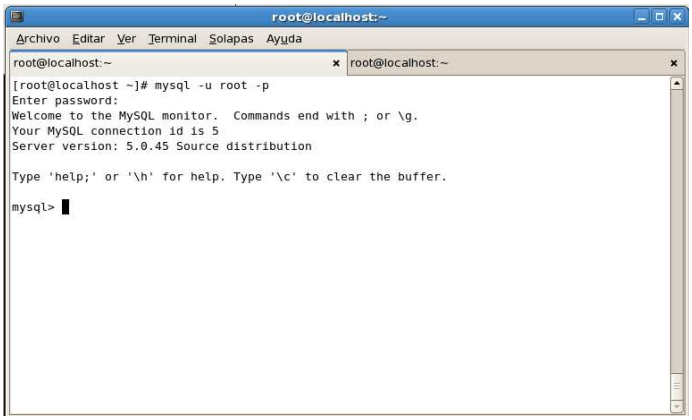


Figura V.4. Interfaz de MySql.

Creación y configuración de la base de datos snort y sus respectivas tablas:

```
Mysql
 mysql>SET PASSWORD FOR root@localhost=PASSWORD('administrador');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
 mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('administrador');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
```

Creación de tablas

La base de datos snort creada va a necesitar de tablas para su almacenamiento de datos recogidos por el programa, los comandos utilizados para la creación de las tablas es el siguiente:

```
[root@localhost ~]#mysql -u root -p < ~/snortinstall/snort-2.6.1.5 /schemas / create_mysql snort
```

Uso de base de datos snort.

Con el siguiente comando se cambiará la base de datos a utilizar para el almacenamiento de las alertas, en este caso la base de datos será snort.

```
Mysql> use snort;
```

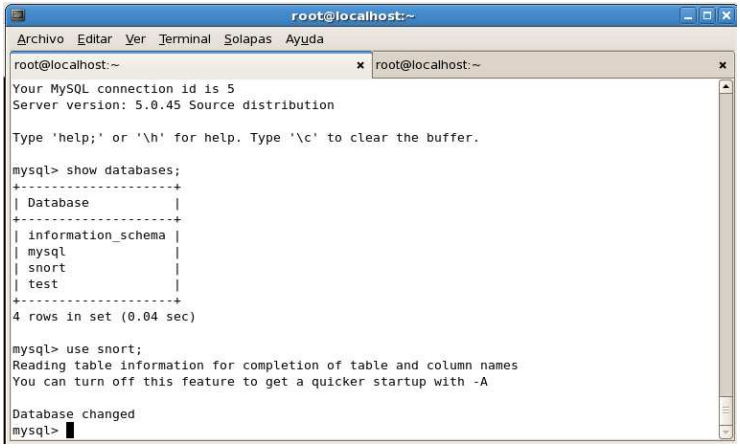


Figura V.5. Cambio de bases de datos por snort.

Visualizar Base de datos Snort

Mysql por defecto viene con dos bases de datos creadas como son Mysql y test, para la visualización de estas bases de datos digitamos el siguiente comando.

```
Mysql> show databases;
```

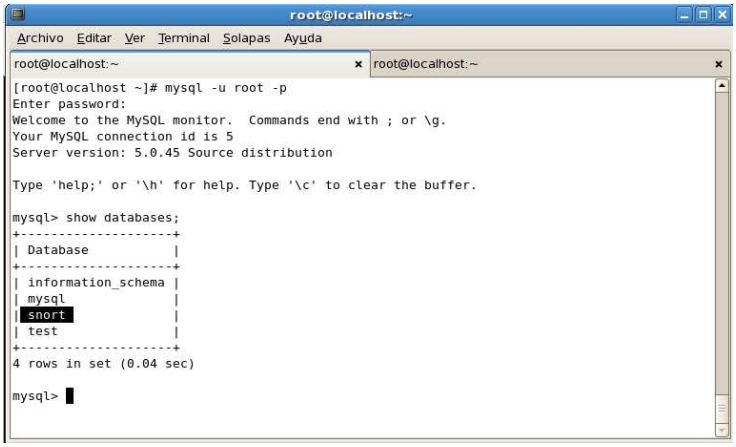


Figura V.6. Visualización de Base de Datos.

Visualizar Tablas creadas

Con el siguiente comando se presentara en pantalla todas las tablas creadas dentro de snort.

```
Mysql> show tables;
```

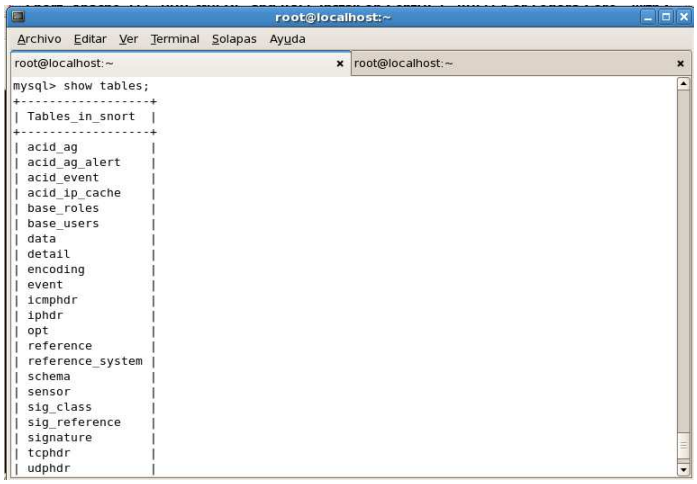


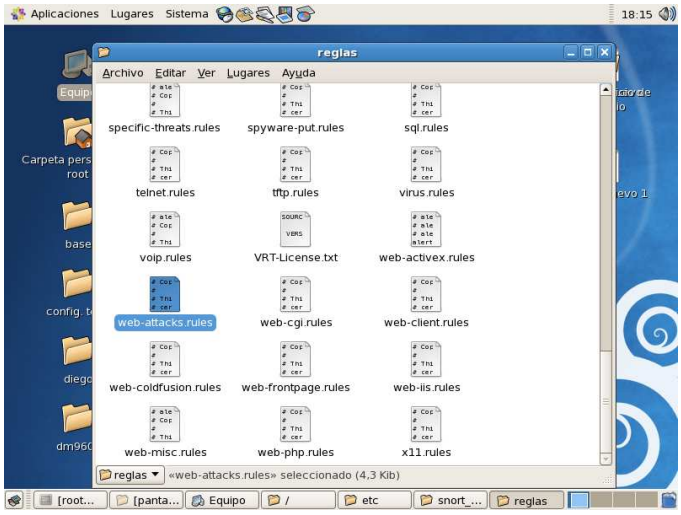
Figura V.7. Visualización de tablas de snort.

CREACION DE REGLAS

Para la creación de reglas se ingresó a la carpeta REGLAS ubicada dentro de snort_inline.

Figura V.8. Acceso a la carpeta REGLAS.

En este caso se creó las reglas específicas para el funcionamiento dentro de la red del M.I Municipio de Riobamba en el archivo web-attacks.rules



Reglas creadas

Las distintas reglas que se crearon para el bloqueo de diferentes puertos son las siguientes:

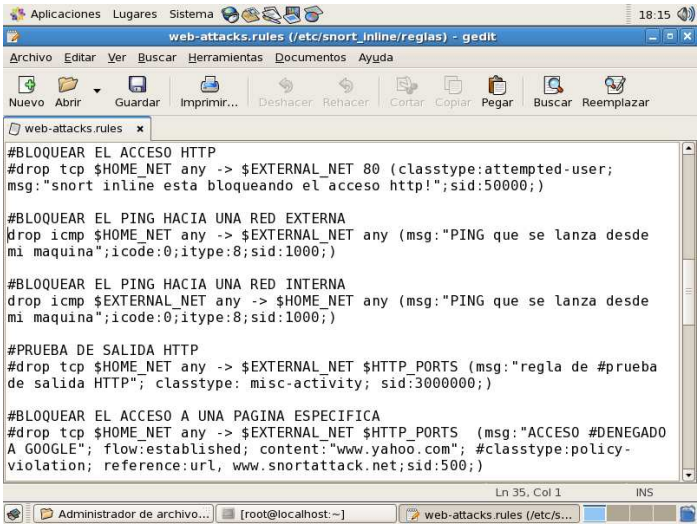


Figura V.9. Reglas activas.

Bloqueo del Acceso HTTP

Esta regla bloquea todo acceso hacia las páginas de internet a través del puerto 80.

Las reglas se conforman de dos partes como son la cabecera y las opciones.

- ***Acción de la regla:*** drop(esta opción envía el paquete por Iptables para su bloqueo)
- ***Protocolo:*** tcp
- ***Direccion IP origen:*** $HOME_NET *(toda nuestra red)*
- ***Puerto IP origen:*** any *(cualquiera)*
- ***Direccion IP destino:*** $EXTERNAL_NET *(toda la red externa)*
- ***Puerto IP destino:*** 80 *(puerto que se utiliza para el acceso http)*
- ***Dirección de la operación:*** *-> (hacia la red externa)*

Opciones

- ***Mensaje:*** msg (Mensaje de la alerta)
- ***Sid:(****identificación de la regla****)***

✓ Bloqueo de PING hacia la red interna o hacia la red externa.

Esta regla como la anterior consiste en bloquear cualquier intento de PING hacia nuestra red y utiliza el protocolo ICMP.

- ***Acción de la regla:*** drop(bloquear el ping a través de Iptables)
- ***Protocolo:*** icmp
- ***Direccion IP origen:*** $EXTERNAL_NET *(toda la red externa)*
- ***Puerto IP origen:*** any *(cualquiera)*
- ***Direccion IP destino:*** $HOME_NET *(toda nuestra red)*
- ***Puerto IP destino:*** any *(cualquiera)*
- ***Dirección de la operación:*** -> (desde la red externa hacia nuestra red)

Opciones

- ***Mensaje:*** msg:"ping que se lanza desde la red externa "
- ***Itype:*** comprobación del valor del campo *type* de la cabecera ICMP en este caso 8.
- ***Sid:*** identificación de la regla.
- ***Icode:*** comprobación del valor del campo *code* de la cabecera ICMP en este caso 0.

✓ Bloquear el acceso a una página especifica

- ***Acción de la regla:*** drop(bloquear el acceso a través de Iptables).
- ***Protocolo:*** tcp
- ***Direccion IP origen:*** $HOME_NET *(toda nuestra red)*
- ***Puerto IP origen:*** any *(cualquiera)*
- ***Direccion IP destino:*** $EXTERNAL_NET *(toda la red)*
- ***Puerto IP destino:*** HTTP_PORTS (variable puerto 80)
- ***Dirección de la operación:*** -> (dirección hacia la red externa)

Opciones

- ***Mensaje:*** msg:"Acceso denegado a cualquier página especifica "
- ***Content:*** www.google.com este parámetro nos indica que cualquier paquete que contenga en su campo datos" google.com" será bloqueado a través de su puerto relacionado.
- ***Flow:*** *establishied(conexiones TCP establecidas)*
- ***Classtype:*** policy-violation en este caso va a ser la categoría de la alerta.
- ***Sid:*** 500 id de la alerta.
- ***Reference:*** referencia de la regla o pagina de referencia.

✓ Bloquear la descarga de archivos con extensión .mp3

- ***Acción de la regla:*** drop(bloquear la descarga a través de Iptables).
- ***Protocolo:*** tcp
- ***Direccion IP origen:*** $EXTERNAL_NET *(toda la red)*
- ***Puerto IP origen:*** any *(cualquiera)*
- ***Direccion IP destino:*** $HOME_NET *(toda nuestra red)*

- ***Puerto IP destino:*** any (cualquiera)
- ***Dirección de la operación:*** -> (dirección hacia la red interna)

Opciones

- ***Mensaje:*** msg:"Cuidado están descargando archivos mp3 "
- ***Content:*** *extensión del archivo, en este caso" .mp3".*
- ***Flags:*** Establece el contenido de los flags o banderas TCP.
- ***Sid:*** 333 id de la alerta.

✓ **Bloquear el acceso a Messenger**

- ***Acción de la regla:*** drop(bloquear el acceso a Messenger través de Iptables).
- ***Protocolo:*** tcp
- ***Direccion IP origen:*** $EXTERNAL_NET *(toda la red)*
- ***Puerto IP origen:*** 1863 *(puerto que utiliza messenger para el inicio de sesión)*
- ***Direccion IP destino:*** $HOME_NET *(toda nuestra red)*
- ***Puerto IP destino:*** any(cualquiera)
- ***Dirección de la operación:*** -> (dirección hacia la red interna)

Opciones

- ***Mensaje:*** msg:"*Inicio de sesión de Messenger "*
- ***Content:"****http |3A|//", "MSG" contenido en el paquete de datos.*
- ***Flow:*** *to_client, establishied(respuesta de servidores y conexiones TCP establecidas)*
- ***Classtype:*** *trojan-activity en este caso va a ser la categoría de la alerta.*

- ***Sid:*** 15184 id de la alerta.
- ***Depth:***3 (*extensión del tamaño de datos que se ha de inspeccionar, en este caso 3.*)
- ***Reference:*** referencia de la regla o página de referencia.
- ***Rev:***1 (*identificación de la revisión o versión de la regla*)
- ***Metadata:***(permite integrar información adicional sobre la regla.)
- ***Pcre***: (expresiones regulares o extensión de **content** que describe conjunto de cadenas dentro de **content**)

✓ **Bloquear el escaneo de puertos con nmap**

- ***Acción de la regla:*** drop(bloquear el escaneo de puertos través de Iptables).
- ***Protocolo:*** tcp
- ***Direccion IP origen:*** $EXTERNAL_NET *(toda la red)*
- ***Puerto IP origen:*** any*(cualquiera)*
- ***Direccion IP destino:*** $HOME_NET *(toda nuestra red)*
- ***Puerto IP destino:*** any(cualquiera)
- ***Dirección de la operación:*** -> (dirección hacia la red interna)

Opciones

- ***Mensaje:*** *msg:"Escaneo Ping con nmap "*
- ***Classtype:*** *attempted-recon en este caso va a ser la categoría de la alerta.*
- ***Sid:*** *628 id de la alerta.*
- ***Reference:*** *arachnids,28 Referencia un a un Advisory, alerta tipo Bugtrac, etc.*
- ***Rev:***1 (*identificación de la revisión o versión de la regla*)
- ***Flags:*** *Establece el contenido de los flags o banderas TCP*.

- **Ack:** (*indica que se está confirmando la recepción correcta de datos hasta un determinado número de secuencia.)*

ARRANCAR SNORT IN_LINE

Netfilter y Snort_Inline

Netfilter es un módulo del kernel de Linux disponible desde la versión de kernel 2.4. Proporciona tres funciones principales:

Packet filtering Acepta o rechaza paquetes
NAT Cambios en la dirección IP de origen o destino de los paquetes de red
Packet Mangling Modifica los paquetes por ejemplo por la calidad de servicio, QoS

Iptables es una herramienta necesaria para configurar Netfilter, este puede ser iniciado como root.

Netfilter enlaza paquetes a Snort_Inline en el espacio del usuario con la ayuda del módulo del kernel ip_queue y libipq.

Entonces, si un paquete coincide con una firma de ataque Snort_Inline, es marcada por libipq y vuelve a Netfilter donde se dejó caer.

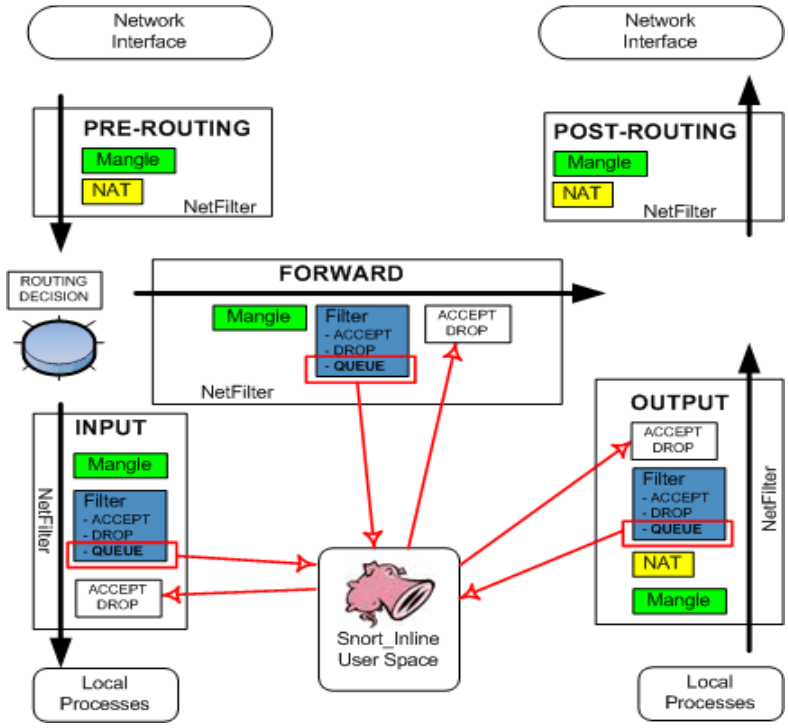


Figura V.9. Función de Netfilter.

Hay dos modos de Snort-Inline:

Drop Mode

Un paquete es descartado si coincide con una firma de ataque.

En nuestro tutorial, vamos a usar este modo.

Hay tres opciones disponibles en este modo:

Drop: Suelta un paquete, envía un restablecimiento de vuelta al servidor, registra el evento.

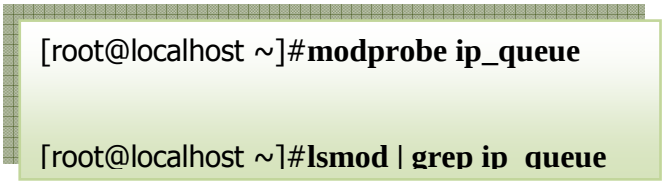
Sdrop: Suelta un paquete sin el envío de un restablecimiento de nuevo al servidor. **Ignore:** Suelta un paquete, envía un restablecimiento de vuelta al servidor, no lo incluye en el registro de sucesos

Replace Mode

Un paquete es modificado si coincide con una firma de ataque.

Cargar el módulo del kernel ip_queue.

Tenemos que cargar el módulo ip_queue y comprobar si se realiza con éxito:



Para descargar ip_queue: "modprobe-r ip_queue"

Configurar iptables para poner a prueba Snort_Inline

Configurar NetFilter con la herramienta iptables.
A continuación se expone una regla de Netfilter para enviar todo el tráfico entrante a la cola en la que se analizarán en contra de las reglas Snort_Inline.

```
iptables -A INPUT -j QUEUE
```

Revise sus reglas:

```
[root@localhost ~]#iptables -L
```

Iniciar Snort_inline

```
[root@localhost ~]#snort_inline -Q -v -c /etc/snort_inline/snort_inline.conf -l
/var/log/snort_inline
```

Q -> el proceso de tráfico en espera

v -> verbose

l -> ruta de registro

c -> Ruta de configuación

SCRIPT DE INICIO PARA EL ARRANQUE DE SNORT_INLINE

Creación de un archivo llamado snort_inlined y añadir el script siguiente para empezar Snort_Inline fácilmente:

```
[root@localhost ~]#vi /etc/init.d/snort_inlined
```

```
#!/bin/bash # / bin / bash
# snort_inline
start(){
# Inicio demonios.
echo "Starting ip_queue module:"
lsmod | grep ip_queue >/dev/null || /sbin/modprobe ip_queue;
echo "A paritr de  reglas de iptables:"
# Iptables el tráfico enviado a la cola:
# Aceptar conexiones internas localhost
iptables -A INPUT -i lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
iptables -A OUTPUT -o lo -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
# Enviar todas las llamadas entrantes, salientes y redirigir el tráfico a la cola
iptables –A INPUT –i br0 –p 0 –m state –state NEW, RELEATED, ESTABLISHIED –j
QUEUE
iptables –A FORWARD –i br0 –p 0 –m state –state NEW, RELEATED,
ESTABLISHIED –j QUEUE
iptables -A INPUT -j QUEUE
iptables -A FORWARD -j QUEUE
iptables -A OUTPUT -j QUEUE
# Inicio Snort_inline
echo "Iniciando snort_inline: "
snort_inline –Q –v -c /etc/snort_inline/snort_inline.conf  -l  / var / log / snort_inline
# -Q -> Proceso de tráfico en espera
# -D -> Ejecutar como demonio
# -v -> Verbose
# -l -> Ruta del registro
# -c ->Ruta de configuración
} )
```

(Continuación)

```
stop() {
# Detener daemons.
# Detener Snort_Inline
# echo "Apagado de snort_inline: "
killall snort_inline
# Quitar todas las reglas de iptables
# Establece las políticas por defecto para aceptar Netfilter
echo "Extracción de reglas de iptables:"
iptables -F
# -F -> flush iptables
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#-P -> la política por defecto
}

restart(){
stop
start
} )
case "$1" in
start)
start
;;
stop)
stop
;;
restart)
restart
;;
*)
echo $"Usage: $0 {start|stop|restart|}"
exit 1
esac
```

Analizador del Log:

Se comprueba que Snort_Inline está trabajando bien.

Proponemos aquí dos maneras de hacerlo:

Primera Prueba

Podemos simular un ataque, simplemente accediendo a una página web ubicada en la máquina Snort_Inline de esta misma máquina, porque esto coincide con un ataque de la firma de Snort.

Por ejemplo, usted puede abrir Firefox y escriba http://localhost

Registro rápido

```
[root@localhost ~]#tail -f /var/log/snort_inline/snort_inline-fast
```

Registro completo

```
[root@localhost ~]#tail -f /var/log/snort_inline/snort_inline-full
```

Salida Base

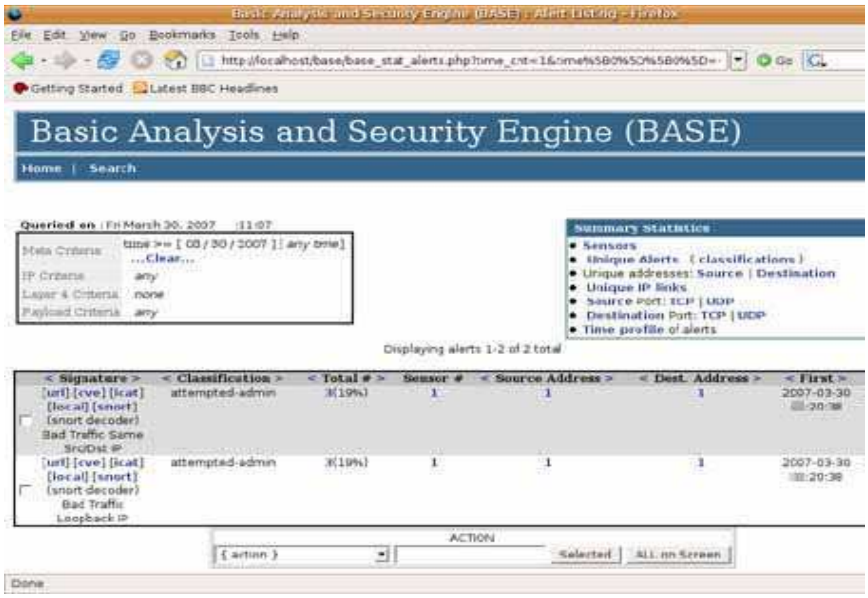


Figura V.10. Salida de Alertas en BASE.

Segunda Prueba

Añadimos una regla de firma para rechazar todo el tráfico web entrante: Añadimos la siguiente regla: /etc/snort_inline/rules/web-attacks.rules

```
[root@localhost ~]#vi /etc/snort_inline/rules/web-attacks.rules
```

```
drop tcp any any -> any 80 (classtype:attempted-user; msg:"Snort_Inline is blocking the http link!";)
```

Registro rápido

```
[root@localhost ~]#tail -f /var/log/snort_inline/snort_inline-fast
```

Registro completo

```
[root@localhost ~]#tail -f /var/log/snort_inline/snort_inline-full
```

Salida Base

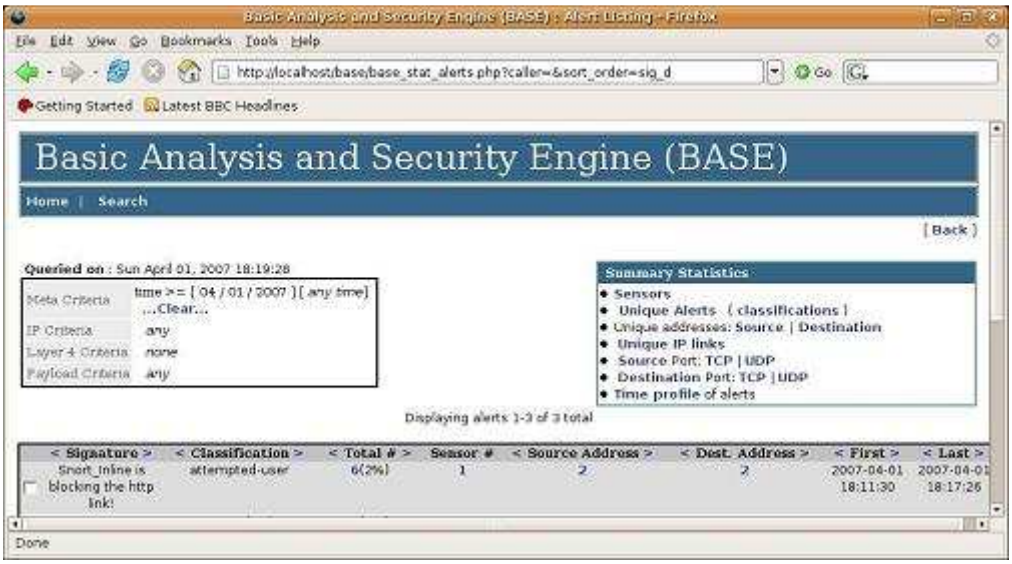


Figura V.10. Salida BASE.

Inicie la secuencia de comandos snort_inlined:

```
[root@localhost
```

Se comprueba que Snort_inline se está ejecutando con el siguiente comando:

```
[root@localhost ~]##ps -ef | grep
```

Comando para revisar reglas de iptables:

```
[root@localhost ~]#iptables-L
```

INTERFAZ GRAFICA BASE

BASE es una interfaz gráfica escrita en PHP utilizado para mostrar los registros generados por la IPS y enviados a la base de datos. Representa el análisis básico y motor de seguridad.

Descargar base

Para descargar la última versión de BASE accedemos a la siguiente página: http://sourceforge.net/projects/secureideas/files/

Ahora tenemos que descomprimir los archivos y ponerlos en la carpeta correcta:

```
[root@localhost ~]#tar -xvf base-1.3.5.tar.gz
[root@localhost ~]#mv /snortinstall/base-1.3.5
/var/www/base
```

CONFIGURACION BASE

Necesitamos ADOdb (Active Data Objects Data Base) para BASE. ADOdb es en realidad una biblioteca de abstracción de bases de datos para PHP. Download "ADOdb para PHP": http://adodb.sourceforge.net/ # download Una vez más, ahora tenemos que descomprimir los archivos y ponerlos en la carpeta correcta:

ADODB será un intermediario entre BASE y MySQL, su instalación es muy sencilla e independiente de la distribución de Linux que utilicemos, basta con escribir los siguientes comandos:

```
[root@localhost ~]#tar -xvf adodb490.tgz
[root@localhost ~]#mv /snortinstall/adodb /var/www/base/
```

Modificación del archivo de configuración.

La primera cosa a hacer es fijar el archivo base_conf.php.dist Abra base_config.php.dist en el directorio raíz de BASE y cambiar las líneas como se muestra a continuación.

```
$DBlib_path="./adodb";

$DBtype="mysql";

$alert_dbname = snort;

$alert_host = localhost;

$alert_port = "";

$alert_user = snort;

$alert_password = administrador;
```

Luego cambiar el nombre del archivo de base_conf.php.dist a base_conf.php

```
[root@localhost ~]# mv /var/www/base/base_conf.php.dist
/var/www/base/base_conf.php
```

La segunda cosa a hacer es importar las tablas de MySQL base en la base de datos snort:

```
[root@localhost ~]## mysql -u root -p snort <
/var/www/base/sql/create_base_tbls_mysql.sql
```

Representación Gráfica de Base

Primero se instala la biblioteca de gráficos php5-gd para el manejo de gráficos directamente desde scripts PHP.

```
[root@localhost ~]# yum install php5-gd
```

A continuación, reinicie el servidor web Apache:

```
[root@localhost ~]#/etc/init.d/apache2 restart
```

Descargar las bibliotecas PEAR PHP.

PEAR stands for "PHP Extension and Application Repository".

Para descargar e instalar las librerías fácilmente, lo mejor es instalar el paquete php-pear:

```
[root@localhost ~]#yum install php-pear
```

Luego se instala los siguientes paquetes:

Image_Graph, Image_color and Image_Canvas

```
[root@localhost ~]#pear install --force Image_Color
[root@localhost ~]#pear install --force Image_Canvas
```

Dado que hay algunas dependencias, es necesario instalar las librerías siguiendo las secuencias de comandos en el orden indicado para tener acceso a los graficos.

IMPLEMENTACION DEL PUENTE

Después de configurar Snort_Inline, debemos tener cuidado de colocar el IPS en el lugar correcto en la red.

Un IDS sólo necesita ser conectado a un puerto del switch en el que recibe el tráfico procedente de un espejo de puerto.

Para nuestro IPS, la configuración de la red para un ids no pueden ser utilizadas porque Snort_Inline debe comprobar los paquetes antes de decidirse a rechazar o aceptarlos. Debe ser colocado a lo largo del enlace de red que queremos analizar y configurado como un puente.

Así que usted debe tener un mínimo de dos interfaces de redes, tres es mejor porque puede dedicar un puerto para la gestión del IPS.

Cargar el módulo puente.

```
[root@localhost ~]#modprobe bridge
```

Se instaló la herramienta para la gestión de puentes:

```
[root@localhost ~]#yum install bridge-
```

Configuración de las tarjetas de red

Configurar la red (/ etc / sysconfig/network-scripts / interfaces).

Ifcfg-br0

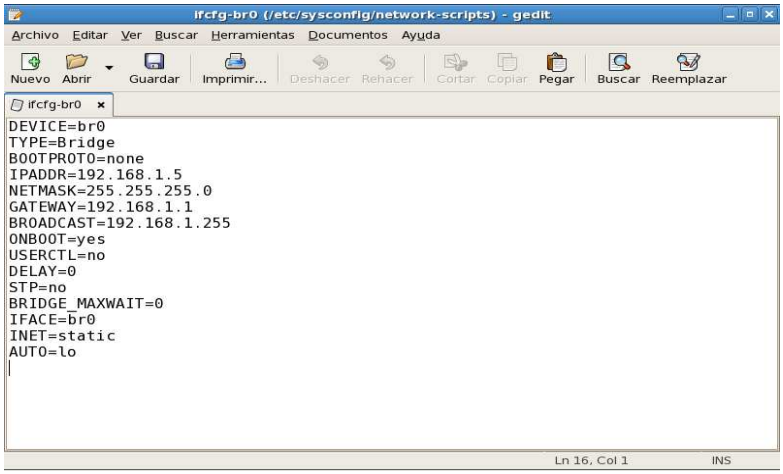


Figura V.11. Script de la interfaz br0.

Ifcfg-eth0

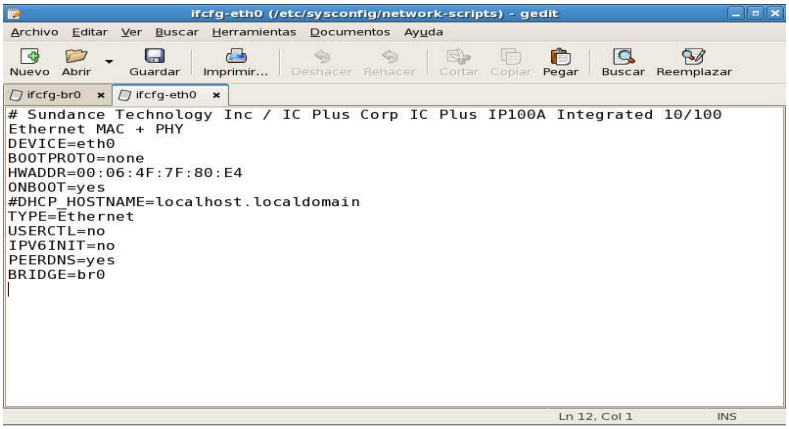


Figura V.12. Script de la interfaz eth0.

Ifcfg-eth1

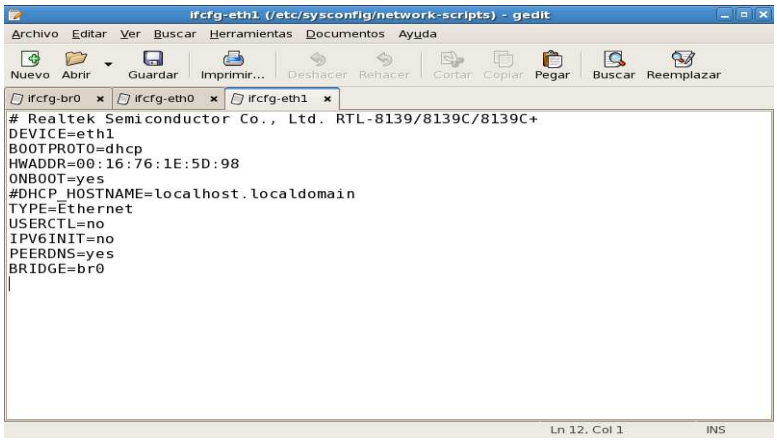


Figura V.12. Script de la interfaz eth1.

Reinicio de servicios de red.

```
[root@localhost ~]#/etc/init.d/networking restart
```

El puente de la dirección MAC es la dirección MAC más pequeña de sus miembros.

```
[root@localhost ~]#ifconfig
```

Utilice el comando brctl para ver los miembros del puente.

Comandos Brctl.

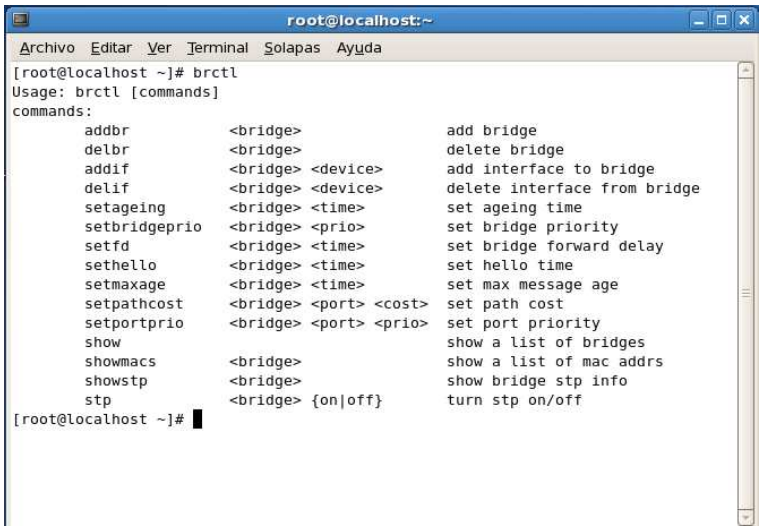


Figura V.13. Comandos Brctl.

Añadir puente br0 con comandos Brctl

```
[root@localhost ~]#brctl addbr br0
```

Añadir interfaces al Puente br0

```
[root@localhost ~]#brctl addif br0 eth0
```

Visualizacion de Puente e interfaces activadas

```
[root@localhost ~]#brctl show
```

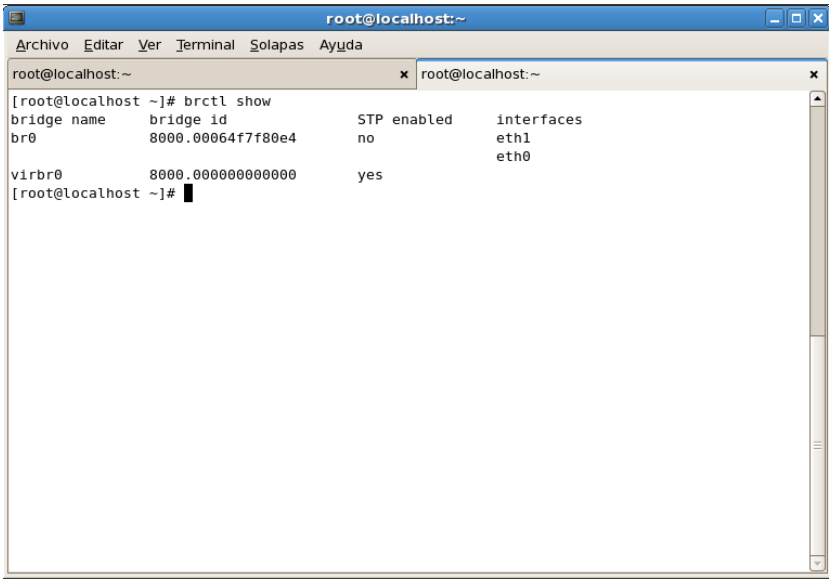


Figura V.14. Interfaces activas en el puente br0.

Interfaces de Red activas en nuestro puente

```
[root@localhost ~]#ifconfig
```

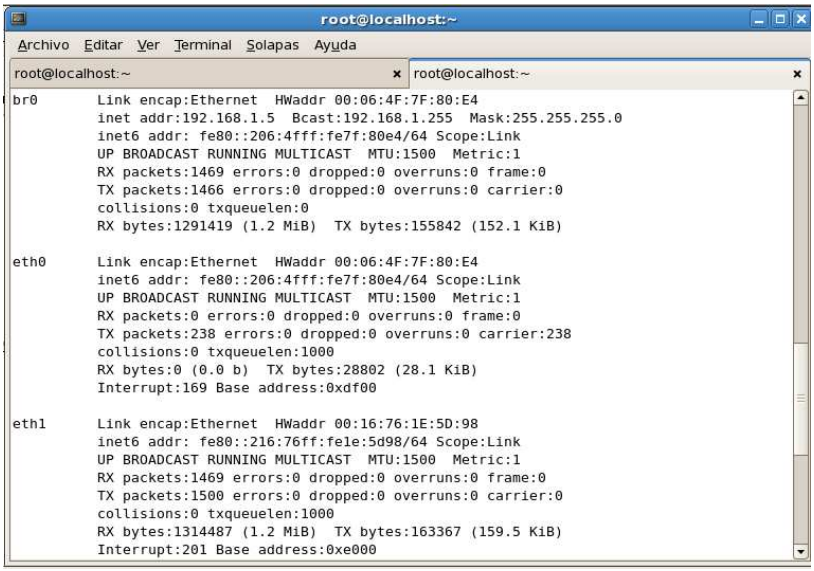


Figura V.14. Interfaces de Red.

Reiniciar el servicio de red

```
[root@localhost ~]#service networtk restart
```

COMANDOS ESPECIALES SERVICO SNORT

Terminal del Centos.

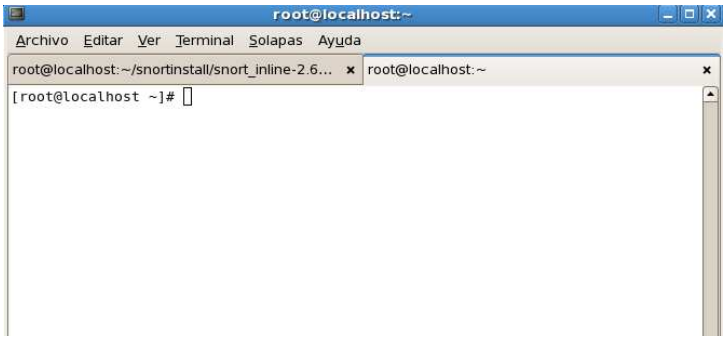


Figura V.15. Terminal de Centos.

Inicio de servicio snort_inline

```
[root@localhost ~]# etc/init.d/snort_inlined start
```

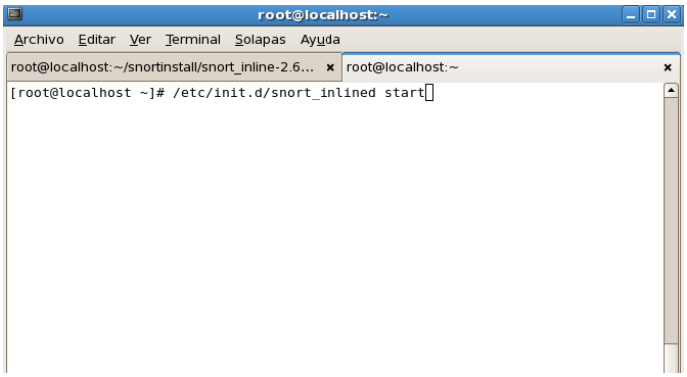


Figura V.16. Inicio del Servicio Snort.

Arrancando el servicio snort_inline

Detalles de compilación de base de datos mysql.

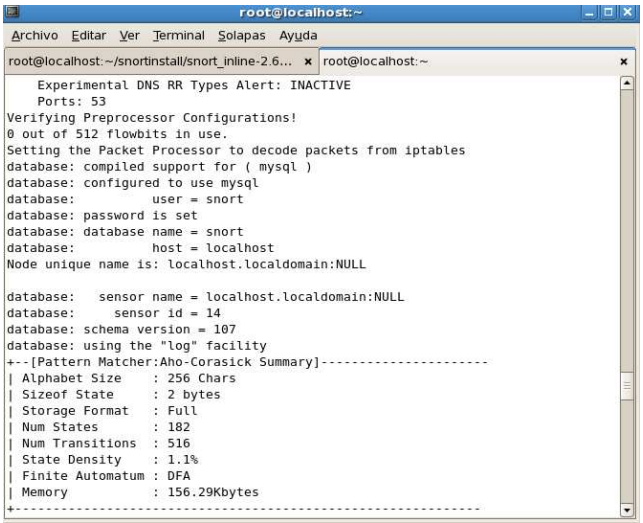


Figura V.17. Detalles de arranque de Snort.

Arranque completado.

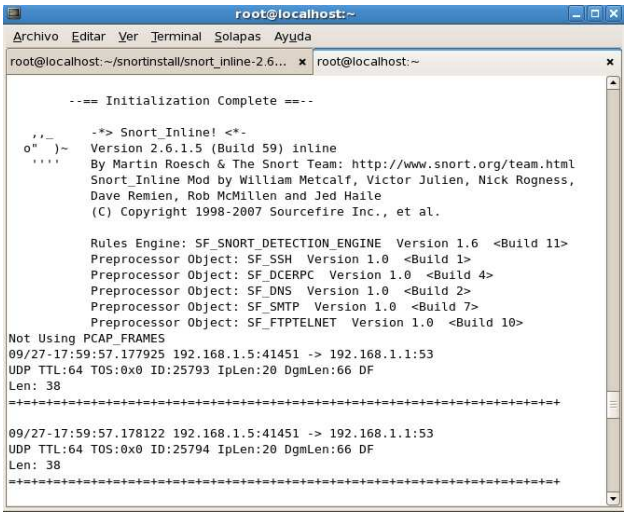


Figura V.18. Arranque completo de snort.

Trafico que pasa a través del sensor

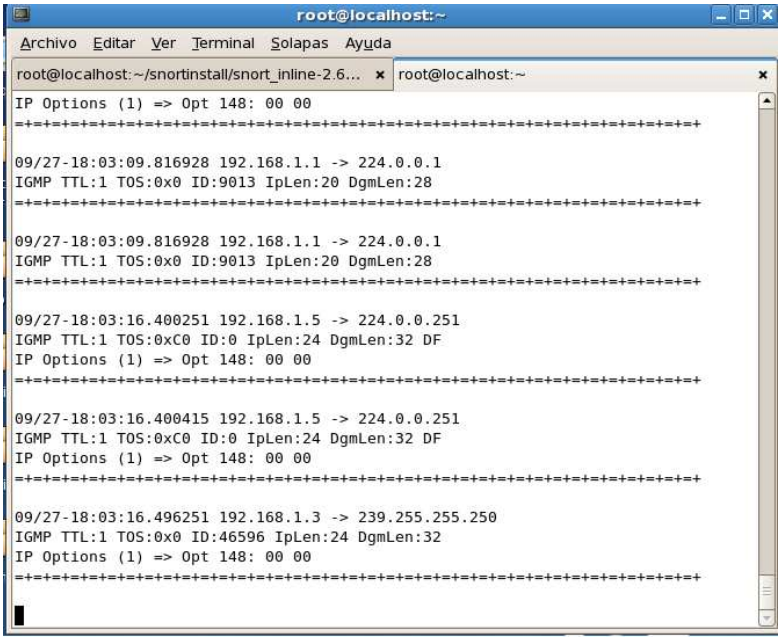


Figura V.19. Visualización de trafico que pasa a través de nuestro IPS .

VISUALIZAR LAS ALERTAS EN EL TERMINAL

El comando necesario para visualizar las alertas sin tener que ingresar a BASE es el siguiente:

```
[root@localhost ~]# tail –f /var/log/snort_inline/snort_inline-fast
```

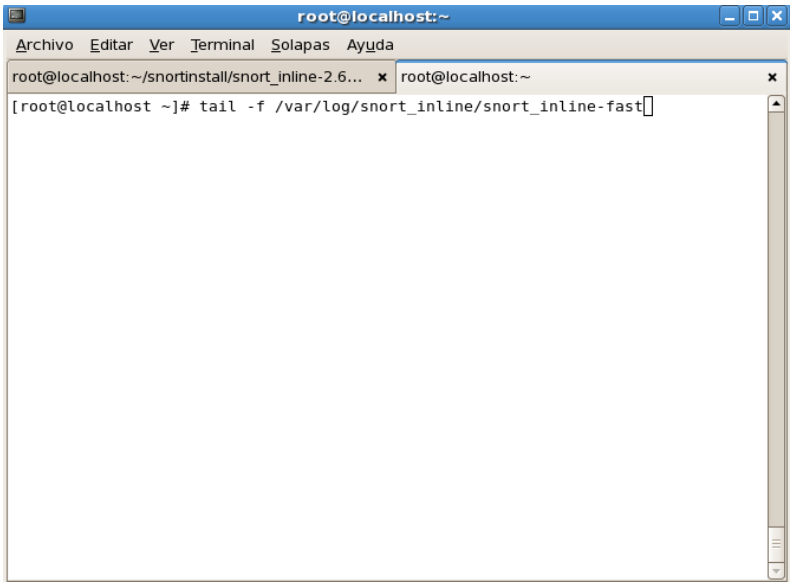


Figura V.21. Comando para visualizar alertas generadas por snort.

Alertas según la regla de ping

Estas alertas son generadas por snort al realizar un ping desde una estación de trabajo como atacante.

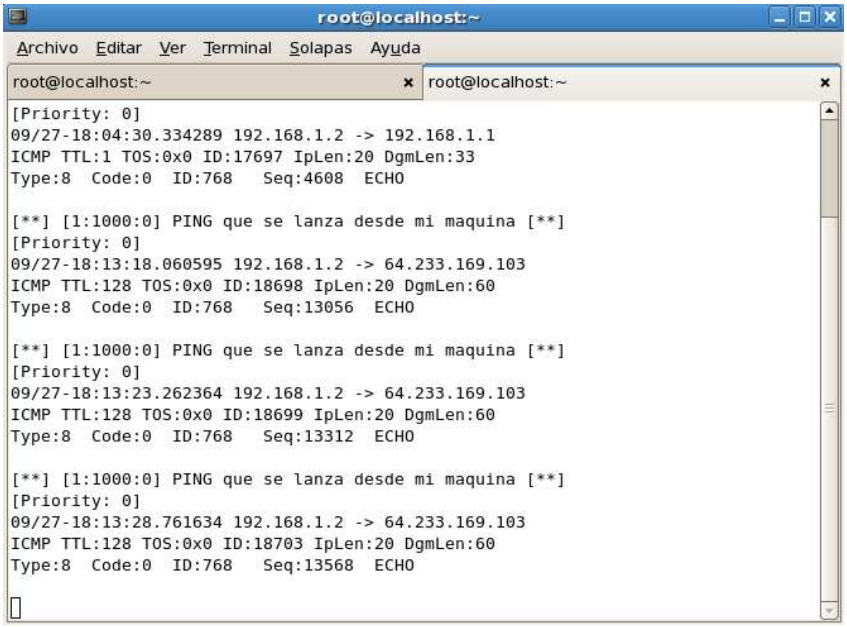


Figura V.22. Alertas generadas por snort.

Detener el servicio snort_inline

El siguiente comando se utiliza para dejar de utilizar el servicio SNORT_INLINE

```
[root@localhost ~]#/etc/init.d/snort_inlined stop
```

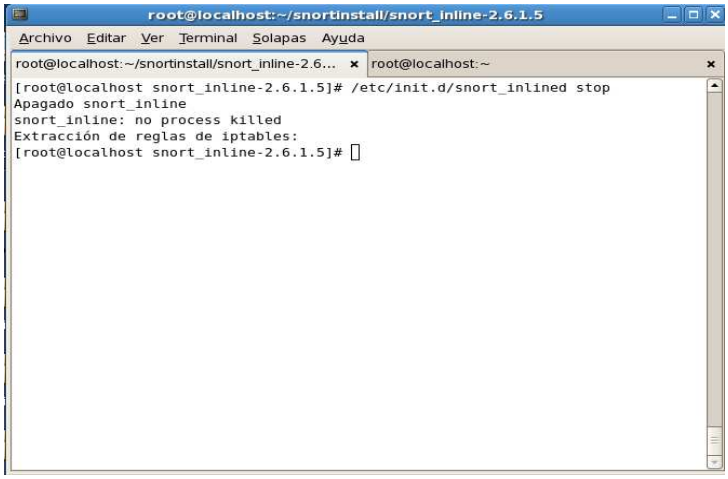


Figura V.22. Pantalla de finalización de servicio.

INGRESO Y ADMINISTRACION DE BASE

Acceso

El ingreso a Base se lo realiza colocando la siguiente dirección de Url en el navegador firefox:

Http://localhost/base

El ingreso a Base a través de otra máquina de la red se lo realiza de la siguiente manera:

Http://192.168.1.5/base

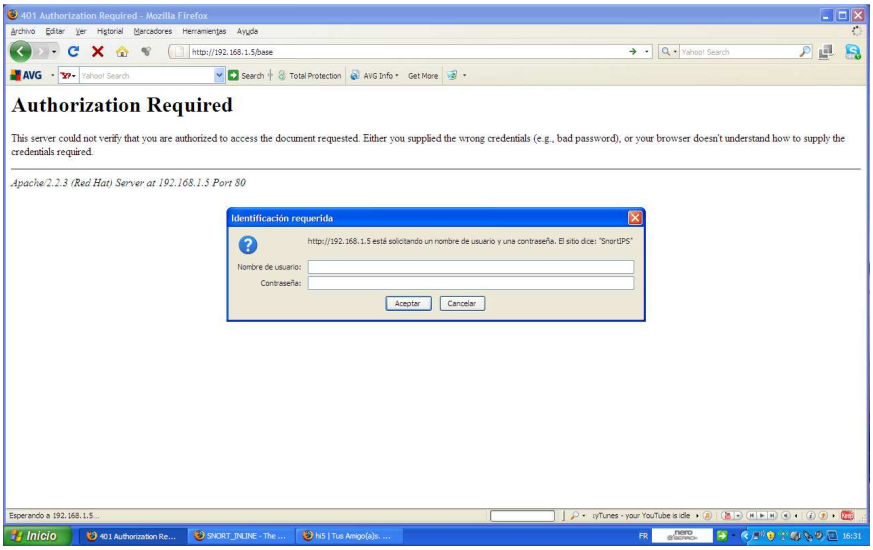


Figura V.23. Pantalla de ingreso a Base.

Para el acceso a la página principal de base se ingresa el nombre de usuario y contraseña los cuales son:

Nombre de usuario: **base**

Contraseña: **administradorbase**

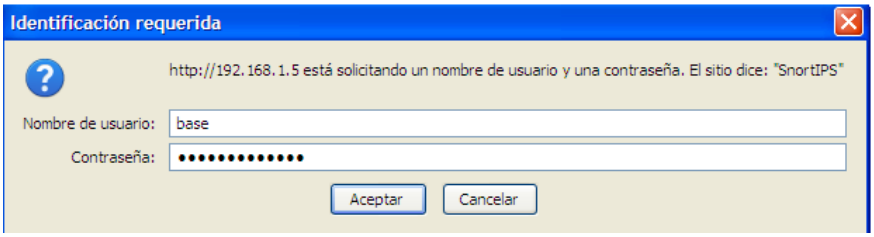


Figura V.24. Ingreso a BASE digitando el nombre de usuario y contraseña.

Página Principal De Base

En la página principal de base podemos visualizar el sensor que está trabajando así como el porcentaje de las diferentes alertas con cada uno de sus protocolos.

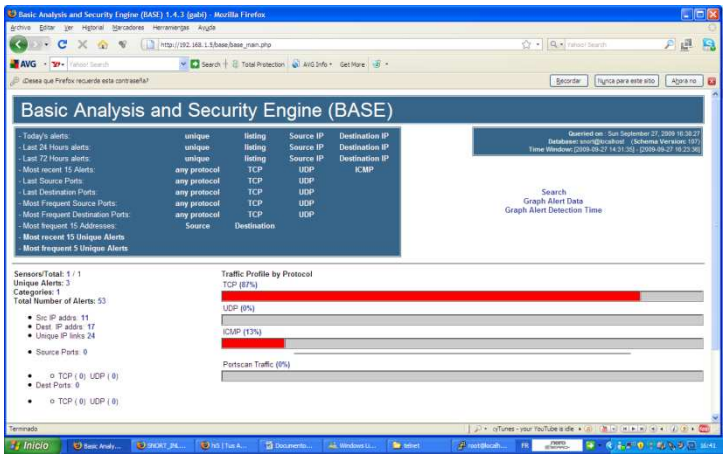


Figura V.25. Pantalla principal de BASE.

Para visualizar todas las alertas clasificadas por protocolo solamente realizamos un click sobre TCP (%) y se nos mostrara todas las alertas que se han generado, seguido de la fecha, direcciones IP origen, destino y su respectivo protocolo, en este caso TCP.

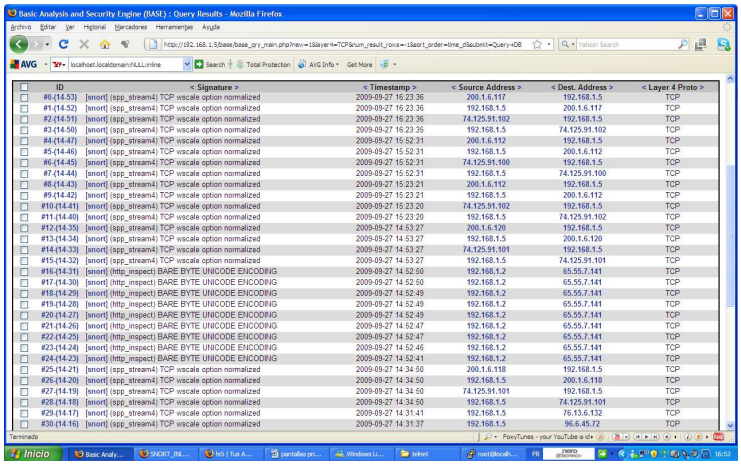


Figura V.26. Alertas generadas por snort.

Al momento q hacemos click sobre otro protocolo en este caso sobre ICMP se va a visualizar todas las alertas generadas por la ejecución de un Ping hacia la red interna o viceversa, conjuntamente con todos los parámetros descritos anteriormente.

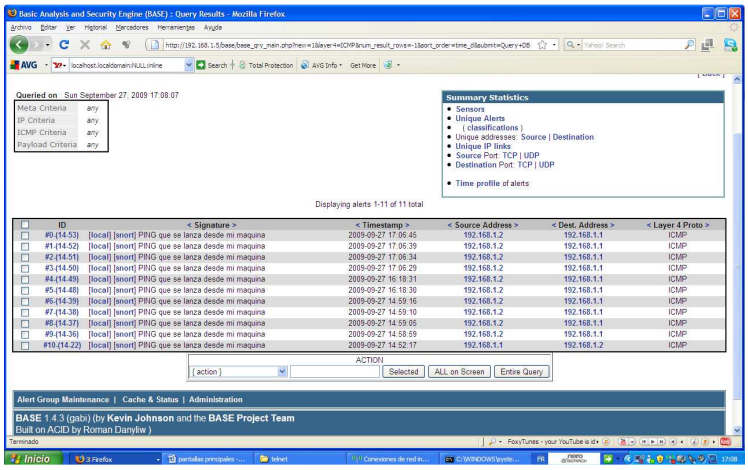


Figura V.27. Alertas generadas por PING desde un atacante.

Resumen Estadístico

En este cuadro tenemos muchas opciones para la visualización de los sensores que están trabajando así mismo estadísticas generales de todas las alertas, direcciones IP, protocolos de origen y destino.

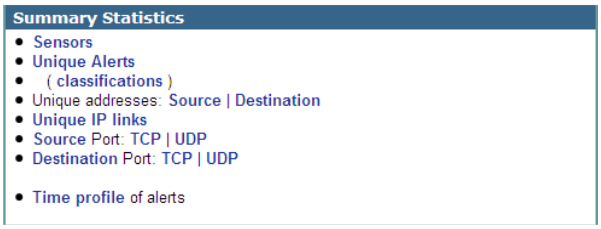


Figura V.28. Estadísticas de BASE.

Sensores

Aquí podemos visualizar el sensor que está trabajando en el servidor y va a tener el nombre de localhost.localdomain:NULL:inline con el número total de eventos o alertas, así mismo con las direcciones IP origen y destino.

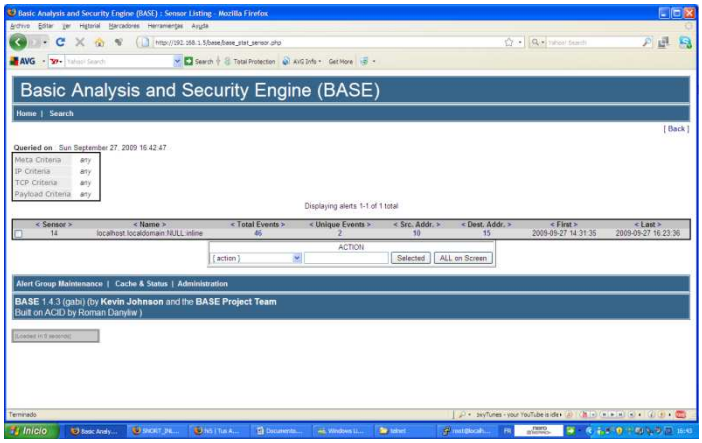


Figura V.29. Sensores activos en BASE.

Alertas Únicas

En esta sección se visualiza todas las alertas que han pasado a través del sensor.

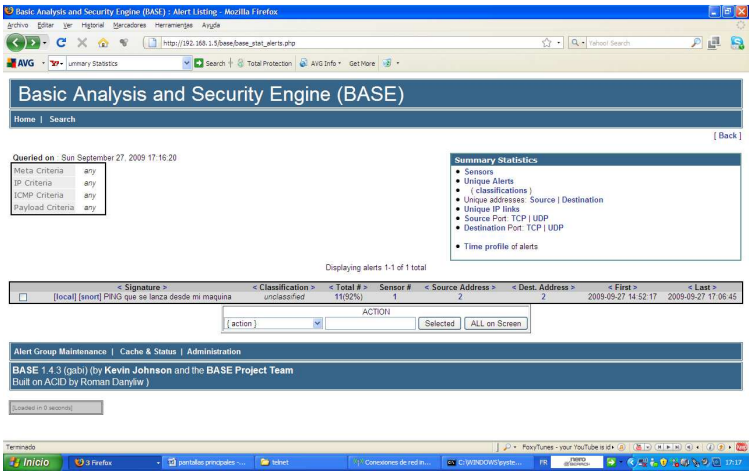


Figura V.30. Visualización de alertas que cruzaron por un sensor especifico.

✓ Búsqueda de Alertas

La búsqueda de las alertas las podemos realizar por detalles es decir por el sensor que las generó, fecha en la que se generó la alerta, grupo al que pertenece, es decir para la búsqueda especifica según lo amerite el caso.

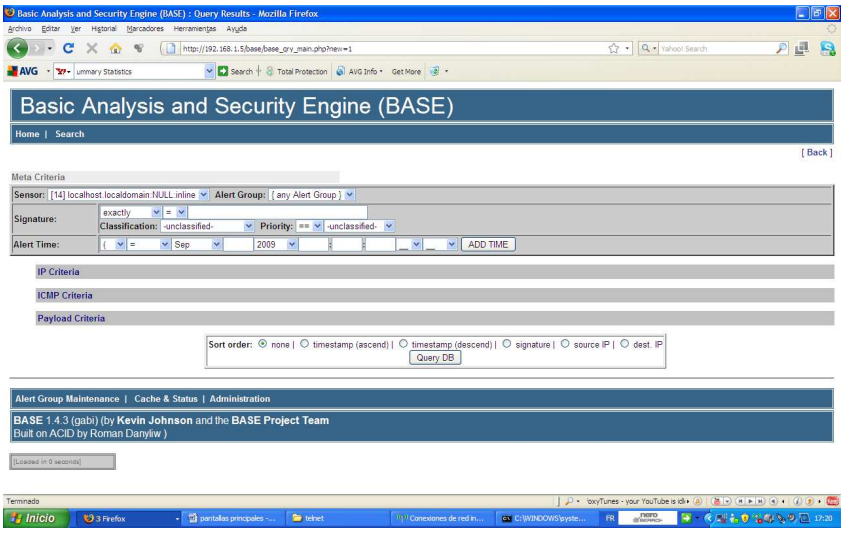


Figura V.31. Búsqueda de alertas.

Representación Gráfica

Todas las alertas también se pueden representar de forma grafica según los parámetros que se configuró, es decir:

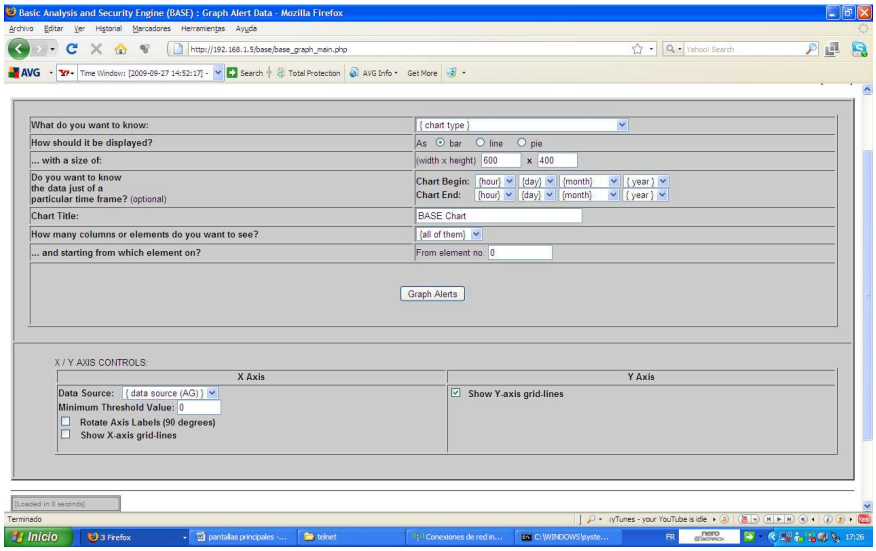


Figura V.32. Representación gráfica de BASE.

En la primera opción se puede escoger la forma en que se visualice las alertas como:

Tiempo(hora) vs Numero de alertas

Tiempo(día) vs Numero de alertas

Puerto TCP origen vs Numero de alertas

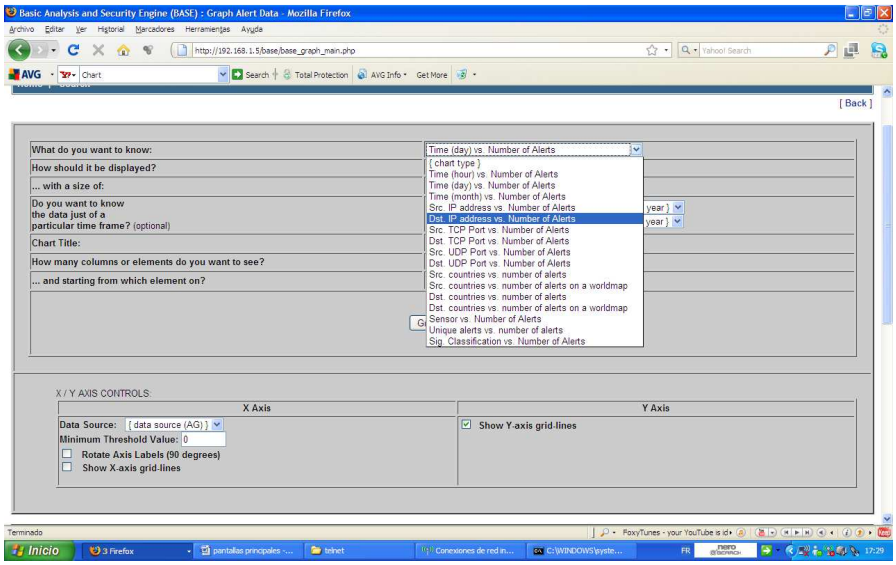


Figura V.33. Opciones de visualización de alertas.

L a grafica de representación se la puede visualizar en barras, líneas o pastel respectivamente.

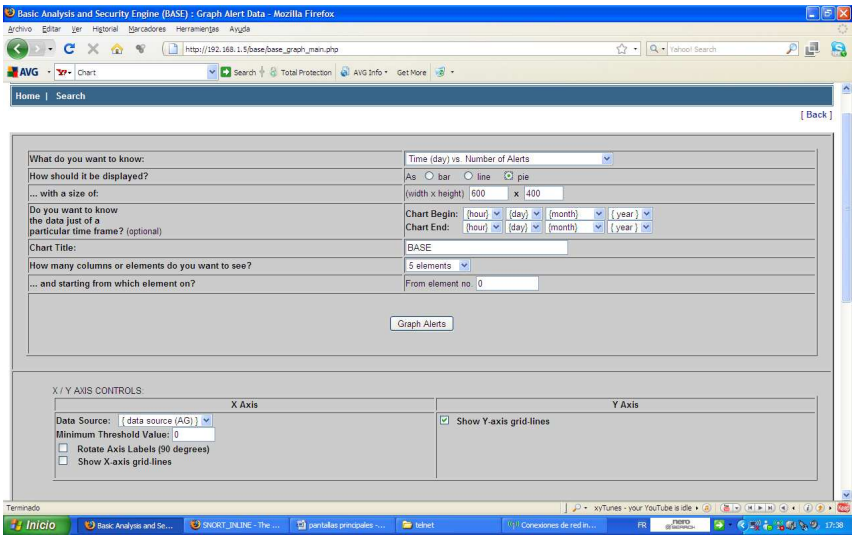


Figura V.34. Opciones de visualización de alertas

El siguiente campo que se debe incluir son las fechas de inicio y fin de las alertas.

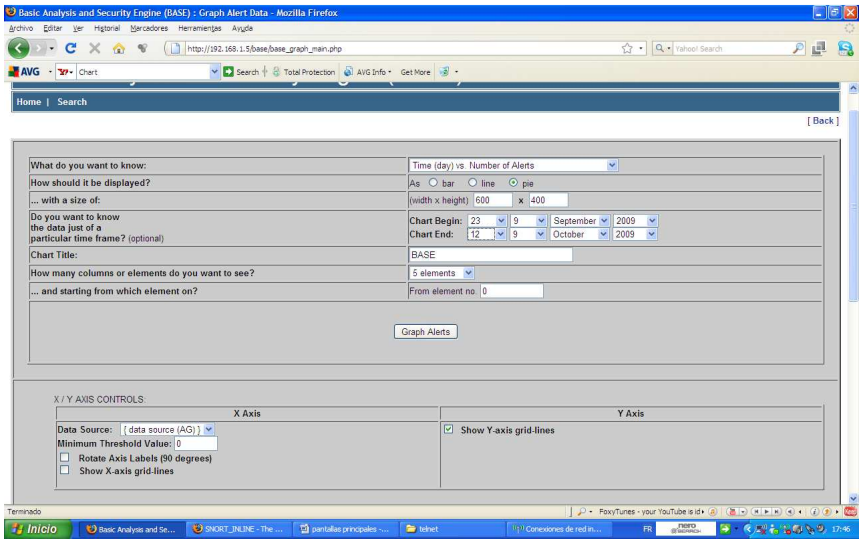


Figura V.35. Opciones de visualización de alertas.

Graficas representadas según los parámetros ingresados.

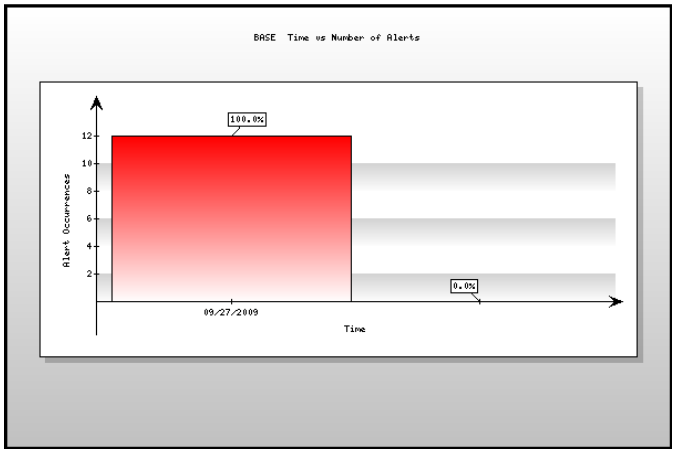


Figura V.36.Visualización de alertas en forma gráfica.

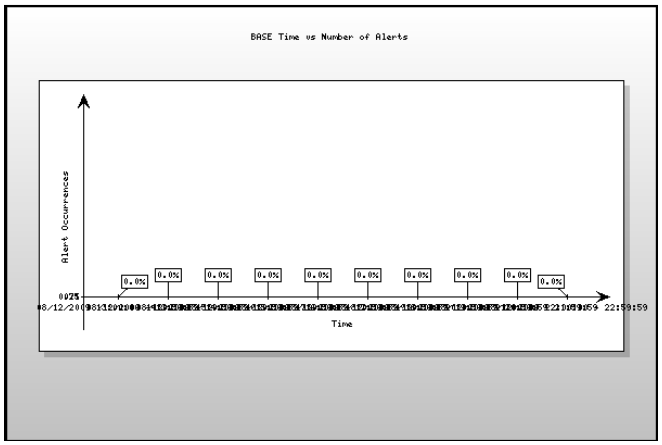


Figura V.37. Visualización de alertas en forma gráfica.

GRAFICA EXPONENCIAL

INVENTARIO TIPOS DE RECURSOS DE INFORMACION. METODOLOGIA MAGERIT

En este anexo se detallan los tipos de recursos de información incluidos en el inventario base de la metodología de análisis de riesgos. [MAGE06]

Procesos y servicios
- o Procesos
- o Servicios internos
- o Servicios externos

Personas
- o Directivos
- o Usuarios internos
- o Usuarios contratas
- o Administradores de sistemas
- o Clientes
- o Proveedores
- o Accionistas
- o Reguladores/supervisores

Aplicaciones informáticas

· Software de sistemas
- o Sistemas operativos
- o Bases de datos

· Dispositivos de hardware
- o Servidores
- o Puestos de trabajo
- o Ordenadores portátiles
- o Agendas electrónicas
- o Teléfonos inteligentes
- o Impresoras
- o Scanners
- o Modems
- o Hubs
- o Switches
- o Routers

· Redes de comunicaciones
- o Redes locales
- o Enlaces de telecomunicaciones
- o Redes inalámbricas

· Soportes de información
- o Papel
- o Cintas
- o Discos magnéticos
- o CD/DVD
- o Memorias flash
- o Tarjetas de memoria
- o Tarjetas inteligentes
- o Memorias internas dispositivos hardware

· Equipamiento auxiliar
- o Sistemas de alimentación eléctrica
- o Sistemas de aire acondicionado
- o Sistemas de detección/extinción de incendios
- o Sistemas de alarma
- o Sistemas de videovigilancia
- o Sistemas de control de acceso
- · Sistemas Ubicaciones físicas
- o Centros de Proceso de Datos
- o Salas de equipamiento auxiliar

    - Salas de comunicaciones
    - Centros de control
    - Salas de operadores
    - Salas de usuarios
- Dispositivos de seguridad
    - IDS/IPS
    - Firewall
    - Antivirus

INVENTARIO DE AMENAZAS

METODOLOGIA MAGERIT

En este anexo se detallan las amenazas incluidas en el inventario base de la metodología de análisis de riesgos. [MAGE06]

- Desastres naturales
  - Fuego
  - Agua
  - Otros desastres naturales
- De origen industrial
  - Fuego
  - Agua
  - Contaminación mecánica
  - Contaminación electromagnética
  - Avería de origen físico o lógico
  - Corte del suministro eléctrico
  - Condiciones inadecuadas de temperatura y/o humedad
  - Fallo de servicios de comunicaciones
  - Interrupción de otros servicios y suministros esenciales
  - Degradación de los soportes de almacenamiento de la información
  - Emanaciones electromagnéticas
  - Otros desastres industriales
- De origen regulatorio
  - Incumplimiento legal
  - Incumplimiento contractual
  - Incumplimiento normativa interna
- Errores y fallos no intencionados
  - Errores de los usuarios
  - Errores del administrador
  - Errores de monitorización (log)
  - Errores de configuración
  - Deficiencias en la organización
  - Difusión de software dañino
  - Errores de [re-]encaminamiento
  - Errores de secuencia
  - Escapes de información
  - Alteración de la información
  - Introducción de información incorrecta
  - Degradación de la información
  - Destrucción de información
  - Divulgación de información
  - Vulnerabilidades de los programas (software)
  - Errores de mantenimiento / actualización de programas (software)
  - Errores de mantenimiento / actualización de equipos (hardware)
  - Caída del sistema por agotamiento de recursos
  - Indisponibilidad del personal
- Errores y fallos intencionados
  - Manipulación de la configuración
  - Suplantación de la identidad del usuario
  - Abuso de privilegios de acceso
  - Uso no previsto
  - Difusión de software dañino
  - [Re-]encaminamiento de mensajes
  - Alteración de secuencia
  - Acceso no autorizado
  - Análisis de tráfico
  - Repudio

o Interceptación de información (escucha)
o Modificación de la información
o Introducción de falsa información
o Corrupción de la información
o Destrucción la información
o Divulgación de información
o Manipulación de programas
o Denegación de servicio
o Robo
o Ataque destructivo
o Ocupación enemiga
o Indisponibilidad del personal
o Extorsión
o Ingeniería social

INVENTARIO DE POLITICAS

NORMA ISO 27002:2005

En este anexo se detallan las salvaguardas incluidas en el inventario base de la metodología de análisis de riesgos. [ISO27002.05]

- 5 – Políticas, normas y procedimientos
    - 5.1.1 - Política de seguridad de la información
    - 5.1.2 - Revisión de la política de seguridad de la información
- 6 – Organización y estructura
    - 6.1.1 - Compromiso de la dirección con la seguridad de la información
    - 6.1.2 - Coordinación de la seguridad de la información
    - 6.1.3 - Asignación de las responsabilidades de la seguridad de la información
    - 6.1.4 - Proceso de la autorización para las instalaciones de tratamiento de la información
    - 6.1.5 - Acuerdos de confidencialidad
    - 6.1.6 - Contacto con autoridades
    - 6.1.7 - Contacto con los grupos de interés especial
    - 6.1.8 - Revisión independiente de la seguridad de la información
    - 6.2.1 - Identificación de los riesgos relacionados con externos
    - 6.2.2 - Abordando la seguridad al tratar con clientes
    - 6.2.3 - Abordando la seguridad en acuerdos con terceros
- 7 – Control de activos
    - 7.1.1 - Inventario de activos
    - 7.1.2 - Propiedad de los activos
    - 7.1.3 - Uso aceptable de los activos
    - 7.2.1 - Guías de clasificación
    - 7.2.2 - Etiquetado y tratamiento de la información
- 8 – Control de empleados
    - 8.1.1 - Roles y responsabilidades
    - 8.1.2 – Investigación
    - 8.1.3 - Términos y condiciones de la ocupación
    - 8.2.1 - Responsabilidades de la dirección
    - 8.2.2 - Conocimiento, educación, y entrenamiento en la seguridad de la información
    - 8.2.3 - Proceso disciplinario
    - 8.3.1 - Responsabilidades de la terminación
    - 8.3.2 - Devolución de activos
    - 8.3.3 - Retirada de los derechos de acceso
- 9 – Control de la seguridad física
    - 9.1.1 - Perímetro de seguridad física
    - 9.1.2 - Controles de entrada física
    - 9.1.3 - Asegurar oficinas, salas, e instalaciones
    - 9.1.4 - Protección contra amenazas externas y ambientales
    - 9.1.5 - Trabajo en áreas seguras
    - 9.1.6 - Acceso público, entrega, y áreas de carga
    - 9.2.1 - Localización y protección de equipos
    - 9.2.2 - Mantenimiento de suministros
    - 9.2.3 - Seguridad del cableado
    - 9.2.4 - Mantenimiento de los equipos
    - 9.2.5 - Seguridad de equipos fuera de los locales de la organización
    - 9.2.6 - Eliminación y re-utilización segura de equipos
    - 9.2.7 - Extracción de propiedades
- 10 – Control de las operaciones de los sistemas de información
    - 10.1.1 - Procedimientos operacionales documentados
    - 10.1.2 - Gestión del cambio
    - 10.1.3 - Segregación de tareas
    - 10.1.4 - Separación de los entornos de desarrollo, pruebas, e instalaciones operacionales

- 10.2.1 - Entrega de servicio
- 10.2.2 - Supervisión y revisión de los servicios de terceros
- 10.2.3 - Gestión de cambios en servicios de terceros
- 10.3.1 - Gestión de capacidades
- 10.3.2 - Aceptación de sistemas
- 10.4.1 - Controles contra código malicioso
- 10.4.2 - Controles contra código móvil
- 10.5.1 - Copia de seguridad de la información
- 10.7.1 - Gestión de soportes extraíbles
- 10.7.2 - Eliminación de soportes
- 10.7.3 - Procedimientos de utilización de la información
- 10.7.4 - Seguridad de la documentación de sistemas
- 10.8.1 - Procedimientos y políticas de intercambio de información
- 10.8.2 - Acuerdos de intercambio
- 10.8.3 - Soportes físicos en tránsito
- 10.8.4 - Mensajería electrónica (Correo Electrónico, EDI, etc.)
- 10.8.5 - Sistemas de información de negocio
- 10.9.1 - Comercio electrónico
- 10.9.2 - Transacciones On-line
- 10.9.3 - Información pública disponible
- 10.10.1 - Registros de auditoría
- 10.10.2 - Monitorización de uso de sistemas
- 10.10.3 - Protección de información de registros
- 10.10.4 - Registros de administrador y operadores
- 10.10.5 - Registro de fallos
- 10.10.6 - Sincronización de relojes

· 11 – Control de acceso lógico
- 11.1.1 - Política de control de acceso
- 11.2.1 - Registro de usuario
- 11.2.2 - Gestión de privilegios
- 11.2.3 - Gestión de contraseñas de usuarios
- 11.2.4 - Revisión de los derechos de usuario
- 11.3.1 - Uso de contraseñas
- 11.3.2 - Equipo informático de usuario desatendido
- 11.3.3 - Política de puesto de trabajo vacío
- 11.5.1 - Procedimientos de inicio de sesión segura
- 11.5.2 - Identificación y autenticación del usuario
- 11.5.3 - Sistema de gestión de contraseñas
- 11.5.4 - Uso de las utilidades del sistema
- 11.5.5 - Sesiones inactivas
- 11.5.6 - Limitación del tiempo de conexión
- 11.6.1 - Restricción de acceso a la información
- 11.6.2 - Aislamiento de sistemas sensibles
- 11.7.1 - Informática móvil
- 11.7.2 – Teletrabajo

· 10-11 – Control de las comunicaciones
- 10.6.1 - Controles de red
- 10.6.2 - Seguridad de servicios de red
- 11.4.1 - Política de uso de servicios de red
- 11.4.2 - Autenticación de usuarios por conexiones externas
- 11.4.3 - Identificación de equipos en red
- 11.4.4 - Protección de los puertos de diagnostico remoto
- 11.4.5 - Segregación de redes
- 11.4.6 - Control de conexión a redes
- 11.4.7 - Control de encaminamiento de la red

- 12 – Control de la adquisición, desarrollo y mantenimiento de aplicaciones
    - 12.1.1 - Análisis y especificación de requerimientos de seguridad
    - 12.2.1 - Validación de los datos de entrada
    - 12.2.2 - Control del proceso interno
    - 12.2.3 - Integridad de mensajes
    - 12.2.4 - Validación de los datos de salida
    - 12.3.1. - Política de uso de los controles criptográficos
    - 12.3.2 - Gestión de claves
    - 12.4.1 - Control del software en producción
    - 12.4.2 - Protección de los datos de prueba de sistema
    - 12.4.3 - Control de acceso al código de fuente del programa
    - 12.5.1 - Procedimientos de control de cambios
    - 12.5.2 - Revisión técnica de las aplicaciones tras cambios en el sistema operativo
    - 12.5.3 - Restricciones en cambios de paquetes de software
    - 12.5.4 - Fuga de información
    - 12.5.5 - Desarrollo externalizado del software
    - 12.6.1 - Control de vulnerabilidades técnicas
- 13 – Gestión de los incidentes de seguridad
    - 13.1.1 - Comunicación de eventos de seguridad de la información
    - 13.1.2 - Comunicación de vulnerabilidades
    - 13.2.1 - Responsabilidades y procedimientos
    - 13.2.2 - Aprendiendo de las incidencias de seguridad de la información
    - 13.2.3 - Recogida de pruebas
- 14 – Gestión de la continuidad
    - 14.1.1 - Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio
    - 14.1.2 - Continuidad del negocio y valoración del riesgo
    - 14.1.3 - Desarrollo e implementación de planes de continuidad incluyendo la Seguridad de la información
    - 14.1.4 - Marco de planificación para la continuidad del negocio
    - 14.1.5 - Prueba, mantenimiento y reevaluación de los planes de continuidad
- 15 – Cumplimiento regulatorio
    - 15.1.1 - Identificación de la legislación aplicable
    - 15.1.2 - Derechos de propiedad intelectual (IPR)
    - 15.1.3 - Salvaguarda de los registros de la Organización
    - 15.1.4 - Protección de datos de carácter personal y de la intimidad de las personas
    - 15.1.5 - Evitar el mal uso de los recursos de tratamiento de la información
    - 15.1.6 - Reglamentación de los controles de cifrado
    - 15.2.1 - Cumplimiento con políticas y estándares de seguridad
    - 15.2.2 - Comprobación del cumplimiento técnica
    - 15.3.1 - Controles de auditoría de sistemas de información
    - 15.3.2 - Protección de las herramientas de auditoría de sistemas

INFORME TECNICO

PNTE INEN-ISO/IEC 27002

INFORME TÉCNICO "NTE INEN-ISO/IEC 27 002"

1. **Título: Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información** – 119 páginas en español.

2. **Fecha aprobación Subcomité Técnico:** 2008-12-31
   Fecha entrega Directorio:

3. Objeto

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por una evaluación de riesgos.

Esta norma puede servir como guía práctica para el desarrollo de normas de la seguridad de una organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

4. **Justificación:**

La tecnología informática se debe hacer bajo esquemas normalizados para alcanzar la eficiencia que esta persigue. Los softwares por igual deben ser normalizados para la compatibilidad de los sistemas de ordenadores.

4.1 Este proyecto de norma hace referencia a los siguientes documentos normativos:

4.1.1 ISO/IEC Guide 2:1996 *Standardization and related activities – General vocabulary*

4.1.2 ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

4.1.3 ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

4.1.4 ISO/IEC TR 13335-3:1998, *Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security*

4.1.5 ISO/IEC 13888-1: 1997, *Information technology – Security techniques – Non-repudiation – Part 1: General*
4.1.6 ISO/IEC 11770-1:1996 *Information technology – Security techniques – Key management – Part 1: Framework*
4.1.7 ISO/IEC 9796-2:2002 *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms*
4.1.8 ISO/IEC 9796-3:2000 *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*
4.1.9 ISO/IEC 14888-1:1998 *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*
4.1.10 ISO/IEC 15408-1:1999 *Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model*
4.1.11 ISO/IEC 14516:2002 *Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services*
4.1.12 ISO 15489-1:2001 *Information and documentation – Records management – Part 1: General*
4.1.13 ISO 10007:2003 *Quality management systems – Guidelines for configuration management*
4.1.14 ISO/IEC 12207:1995 *Information technology – Software life cycle processes*
4.1.15 ISO 19011:2002 *Guidelines for quality and /or environmental management systems auditing OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002*
4.1.16 *OECD Guidelines for Cryptography Policy, 1997*
4.1.17 IEEE P1363-2000: *Standard Specifications for Public-Key Cryptography*
4.1.18 ISO/IEC 18028-4 *Information technology – Security techniques – IT Network security – Part 4: Securing remote access*
4.1.19 ISO/IEC TR 18044 *Information technology – Security techniques – Information security incident management*
4.1.20 ISO/IEC 27002:2005 *Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información*

5. **Impacto (sectores afectados):** Sector de la Informática.

6. **Número de partida de la ICS):**

7. **Áreas Comercio:** Todo el país.

8. **Producción nacional:** Si existe.

9. **Información adicional**
9.1 **Nombre Subcomité Técnico:** Comité Interno del INEN

9.2 Lista invitados
9.3 Lista Miembros Subcomité Técnico
9.4 Convocatorias
9.5 Actas reuniones
9.6 **Nombre Secretario Técnico:** Sr. Edgar Valenzuela
9.7 Texto PNTE INEN-ISO/IEC 27 002

BIBLIOGRAFÍA

1. AREITIO, J. Seguridad de la Información: redes informáticas y sistemas de información. Madrid: Paraninfo, 2008, 592 p.

2. ARGENTINA, SUBSECRETARIA DE TECNOLOGÍAS INFORMATICAS, Manual de Seguridad en Redes. Buenos Aires: Croquis, 2005, 99 p.

3. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Ginebra. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). ISO/IEC 27001:2005. Ginebra: ISO, 2005. 187 p.

4. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Ginebra. Tecnología de la Información. Técnicas de Seguridad. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información. ISO/IEC 27002:2005. Ginebra: ISO, 2005. 276 p.

5. SILES, R. Análisis de Seguridad de la Familia de Protocolos TCP/IP. Santiago: Catalonia, 2001, 143 p.

Recursos Web:

ARCHIVOS NECESARIOS PARA CARGAR SNORT.

http://snort.org/downloads
2009-05-10

DESCARGA DE Php

http://www.php.net/downloads.php
2010-05-20

DESCARGA DE REGLAS DE SNORT

https://www.snort.org/snort-rules/#rules
2010-04-5

DESCARGA DE SERVIDOR DE BASES DE DATOS MySQL

http://dev.mysql.com/downloads/
2010-04-15

DESCARGA Y MANUAL DE DISTRIBUCION DE LINUX CENTOS 5.3

http://www.centos.org/
2010-04-10

SEGURIDAD INFORMATICA.

http://www.inforc.ec/seguridadinfo.htm
http://www.segu-info.com.ar/fisica/seguridadfisica.htm
http://www.segu-info.com.ar/fisica/seguridadfisica.htm
2009-06-12

SISTEMAS DE PREVENCION DE INTRUSOS.

http://www.channelplanet.com/?idcategoria=13968
http://es.kioskea.net/contents/detection/ips.php3#
http://www.idg.es/iworld/articulo.asp?id=152376
2009-07-25