# Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala

**Daniel Santiago Garzón**
**Juan Carlos Ratkovich Gomes**
**Alejandro Vergara Torres**

**Director: Ing. Maria Isabel Serrano**

Pontificia Universidad Javeriana, Bogotá, Colombia

**RESUMEN:**

El siguiente artículo da una perspectiva global de un proceso de investigación sobre seguridad informática, específicamente en el aseguramiento de los recursos de la empresa, tomando como base cinco pilares fundamentales de la seguridad informática, Integridad, Confidencialidad, Disponibilidad, Auditabilidad y no Repudio, enfocándose en empresas de mediana y pequeña escala. El resultado de esta investigación fue una metodología la cual da a conocer una serie de pasos, que abarcan diferentes temas como lo son planeación, políticas de seguridad, aseguramiento de los recursos de la compañía entre otros. Cada uno de estos temas ayuda al mejoramiento de la seguridad de la información, haciendo que un sistema permanezca cubierto y preparado ante eventualidades que puedan interrumpir el desarrollo normal de las actividades de una organización. De este modo se comienza por la planeación, la cual se encarga de valorar, analizar y proyectar los diferentes riesgos que se encuentren presentes en el ambiente empresarial, así como clasificar la información dependiendo del grado de importancia y sensibilidad de la misma. De acuerdo con este plan, se deben implementar políticas de seguridad, identificando las amenazas internas y externas, teniendo en cuenta la infraestructura tecnológica que se posee; asimismo, tanto el plan como las políticas deben estar de acuerdo con las necesidades y los recursos con que cuente la organización. Luego se debe implementar la parte práctica, eligiendo y estableciendo una arquitectura de red soportada por el plan, en la cual se monten todos los servicios que presta la organización, asegurando, tanto física como lógicamente los recursos, solucionando así las vulnerabilidades de cada uno de éstos. Por ultimo se recomienda llevar a cabo una auditoria de este proceso, la cual debe seguir realizándose periódicamente con el fin de verificar que los procedimientos y planes se estén cumpliendo.

**ABSTRACT:**

The following article describes a global perspective on a research process about information security, focused in securing resources of any enterprise. The research is based on five fundamentals in information security: Integrity, Confidentiality, Availability, Auditing and No reply; for implementation in medium size and small size enterprises. The result of this research is a methodology that gives a series of steps which help to improve the company's security; obtaining a hardened and prepared system before eventualities that can interrupt the normal development of the activities by an organization. It includes different topics such as: planning, security policies and securing the resources in the enterprise among others. The process begins with planning; which deals with quantifying, analyzing and detecting the different risks that are presents in the enterprise's atmosphere; as well as classifying the information according to its importance and sensitivity. Because of this, security policies have to be implemented by identifying internal and external threats, considering the technological infrastructure of each company. These plans and the policies must be developed according to the necessities and resources with which the organization counts. The next step relates to the implementation, choosing and establishing network architecture supported by the plan; in which all that the organization serves, securing, as much physical as logically the resources will be mounted; therefore solving the vulnerabilities of the platform. At last it is recommended to carry out an audit of this process, which must continue periodically as to verify that the securing system is being fulfilled.

En la actualidad la información manejada por una organización es fundamental e indispensable, pues ésta es sinónimo de poder; poder para controlar los proyectos, los negocios, las tácticas y el mercado de sus productos y es por tanto lo que más preocupa a las organizaciones hoy en día.

La viabilidad de los proyectos y negocios sustentados en sistemas de información no está determinada por las bondades de la tecnología que se usa, puesto que también el desarrollo de éstas ofrece un nuevo campo de acción a conductas antisociales y delictivas, otorgando la facilidad de cometer delitos tradicionales en formas no tradicionales, atentando contra la confidencialidad, disponibilidad, seguridad de la infraestructura y los datos. En consecuencia, esto ocasiona un aumento en el grado de vulnerabilidad e incertidumbre sobre la eficacia de los sistemas que guardan y protegen la información, lo cual ha convertido a la seguridad en una preocupación prioritaria para cualquier empresa.

Por tal motivo que se creo el área de Seguridad Informática, área que se encarga de brindar protección en los diferentes sectores de la empresa. Ésta se fundamenta en cinco principios básicos: confidencialidad, disponibilidad, integridad, auditabilidad y no repudio, pero debe tenerse en cuenta que no solo con estos principios se garantiza una seguridad efectiva, ya que la forma en que estos principios tengan efectos en pro de la organización es mediante la implantación de controles o mecanismos de seguridad, basados en las políticas generales de la empresa, particularmente en las políticas y procedimientos de seguridad, con lo que se busca minimizar las vulnerabilidades expuestas y aumentar la seguridad de la información.

Con el fin incrementar tal seguridad, se hace necesario realizar un análisis de vulnerabilidades, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad. De este modo, el estudio de estas vulnerabilidades debe abarcar varios frentes de seguridad, reduciendo al mínimo la efectividad de los ataques que pueden aprovechar las mismas. Estos frentes son Seguridad Lógica, donde se aplican barreras y se elaboran procedimientos que ayuden a proteger la información; Seguridad Física, la cual aplica defensas físicas y procedimientos de control; Políticas y Estándares, que son los documentos que utiliza una organización para administrar y proteger la información; y finalmente Auditoría de Sistemas, que es la revisión y la evaluación de los controles, sistemas y procedimientos de informática.

Asimismo, se deben identificar y mitigar los riesgos a los que se encuentra expuesta la empresa, de tal modo que cada uno de estos frentes identifique, administre y mitigue cada uno de los mismos, basados en las necesidades y requerimientos de la empresa.

Sin embargo, a pesar de la identificación de los riesgos y las vulnerabilidades, es recomendable que una empresa este preparada para superar cualquier eventualidad que interrumpa las actividades habituales, mediante procedimientos tales como la sincronización y fijación del tiempo de equipos y dispositivos, así como el registro de las actividades en los mismos; este tipo de procedimientos hacen parte de lo que se conoce como computación forense, área que se encarga de detectar crímenes informáticos aplicando técnicas de recolección, análisis y validación de pruebas digitales.

Teniendo en cuenta los diferentes aspectos anteriormente mencionados, solo las empresas con suficiente capital podrían implementar una solución de seguridad que contemple todos los temas necesarios; por tal motivo se ha hecho necesaria la elaboración de una metodología de seguridad apropiada para las empresas que no poseen estos recursos.

La metodología creada busca satisfacer esta necesidad, con el fin de brindar y mejorar los ambientes de seguridad a un bajo costo, dándole, de esta manera, un enfoque social; cabe aclarar que las personas que hagan uso de esta metodología, tales como administradores de red, profesionales de seguridad informática, etc. deben tener conocimientos básicos de arquitecturas de redes, configuración de sistemas operativos y dispositivos de red, con el fin de no crear malos entendidos respecto a las recomendaciones y los pasos a seguir.

## 1. Metodología De Análisis De Vulnerabilidades Para Empresas De Media Y Pequeña Escala

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, controlando todas estas áreas mediante la auditoria de los sistemas de información.

La metodología esta enfocada a la seguridad informática, específicamente al análisis de vulnerabilidades en empresas de mediana y pequeña escala, con el fin de aumentar la seguridad en este tipo de organizaciones, así como también para asegurar aquellos recursos que estén dispuestos para un posible ataque por parte de personas internas o externas a la entidad. Asimismo la metodología en general, debe ser un proceso iterativo y reiterado en el tiempo, debido a que la tecnología nunca deja de evolucionar y cada vez más se generan nuevos riesgos para las organizaciones.

Esta metodología ha sido estructurada en 6 fases[1]; Planeación, Políticas de Seguridad, Aseguramiento Físico, Arquitecturas de Seguridad, Aseguramiento de Servicios y Auditoria de Sistemas, las cuales se han vislumbrado como las fases necesarias para la implementación y monitoreo de un ambiente de seguridad apropiado no solo en las empresas a las que se ha enfocado la metodología, si no para cualquier empresa en general.

Una vez se haya finalizado el proceso de implantación de la metodología, la organización debería poseer las condiciones básicas de aseguramiento de sus recursos informáticos, de esta manera encontrarse preparada para reaccionar ante cualquier eventualidad, y lista para tomar medidas procedimentales o disciplinarias ante alguna irregularidad.

[1] Ver Figura 1

Figura 1. Diagrama de flujo de la Metodología de Análisis de Vulnerabilidades

### 1.1. Fase 1: Planeación

Como en todos los aspectos de la gerencia, una buena parte del éxito del manejo de una empresa se empieza a desarrollar en la planeación, pues es allí donde se establecen los conceptos básicos y las prioridades a las cuales se les darán respuesta, para que ésta produzca máximo beneficio a la organización. Por esta misma razón las directivas deben estar involucradas con el fin de generar un compromiso cumplir con el objetivo principal de este proceso “La seguridad de la organización”.

Con el fin de crear un plan de aseguramiento de la compañía, inicialmente se debe estudiar el cometido de la misma para conocer su misión y visión, y de esta manera generar una solución de

seguridad de acuerdo a sus necesidades y requerimientos. Posteriormente se ha de realizar un análisis de los datos y la información de la compañía, en donde se establecerán los recursos que se van proteger, priorizándolos de manera tal que se cuantifique el impacto en el caso de suspensión del servicio de las aplicaciones, definiendo medidas y procedimientos de seguridad; asimismo en esta etapa se debe hacer un análisis de los posibles riesgos que puede tener la compañía, en donde se identifiquen las amenazas y las vulnerabilidades tanto físicas como lógicas, proporcionándoles un valor de impacto y la probabilidad de que se materialicen.

Una vez se tengan concluidas estas etapas, se ha de definir el plan de aseguramiento de la organización, el cual se debe organizar de manera estructurada según las prioridades definidas en las etapas anteriores, con el fin de continuar con la siguiente fase de la metodología "Políticas de Seguridad".

### 1.2. Fase 2: Políticas De Seguridad

En esta fase se pretende implantar una serie de métodos, controles y directrices para el correcto uso de los recursos informáticos en general, para que de esta manera se pueda respaldar el plan de seguridad.

Al realizar esta labor, la organización debe ser conciente del nivel de responsabilidad que debe asumir, puesto que éstas se elaboran a la medida de cada organización y de acuerdo con su infraestructura tecnológica de información, así como de su cometido. Desafortunadamente ésta no es una tarea sencilla ni rápida, ya que la elaboración de las políticas debe ser de tal manera que éstas sean breves y de fácil entendimiento, así como también de una implementación sencilla. Además ha de tenerse en cuenta que las políticas deben apoyarse en estándares internacionales de seguridad tales como el BS-7799[2] y la ISO 17799[3], sin contradecir las diferentes regulaciones gubernamentales particulares para cada país. Una vez creadas las políticas, la implementación de las mimas se hace a través de procedimientos detallados, los cuales describirán los pasos a seguir, con el fin de cumplir el objetivo de la política de seguridad.

Sin embargo el proceso de documentación de procedimientos es extenso, ya que se requieren una serie de actividades con el fin de lograr el cumplimiento del estándar. La implantación de estas políticas, hará que el valor de la organización aumente así como su credibilidad y reputación, y por que no, conseguir el aval de una entidad certificadora, con el fin obtener una mayor competitividad, consiguiendo el mejoramiento de los procesos.

Una vez concluida la creación y/o modificación de las políticas, y procedimiento de seguridad se da inicio a las fases prácticas del ciclo de vida de la metodología.

### 1.3. Fase 3: Aseguramiento Físico

La seguridad física es una de las vías fundamentales para minimizar los riesgos al interior de la empresa. Para la metodología creada, la fase de aseguramiento físico se enfoco en 4 temas principales:

Ubicación física y disposición del centro de cómputo: Este es uno de los puntos de mayor cuidado y atención, puesto que aquí se encuentra la infraestructura central de la información y de comunicaciones de las cuales depende la compañía para sus labores diarias; control de acceso físico: Esta etapa refuerza la anterior, debido a que en ésta se dan parámetros para controlar el acceso de personas ajenas o no autorizadas a la organización; seguridad administrativa: Busca la capacitación de los empleados de la organización en cuanto al manejo y aseguramiento de los recursos en general. Por ultimo la realización de Planes de Contingencia: Se ocupa del los procedimientos de recuperación del negocio, en caso de algún incidente de seguridad.

Una vez terminada con esta fase, se procede con el aseguramiento lógico del negocio a partir de las arquitecturas de red.

[2] Norma Británica de Seguridad Publicada en 1995.
[3] Estándar Internacional De Seguridad de Información publicada en el año 2000

### 1.4. Fase 4: Arquitecturas De Red

Las arquitecturas de red se crearon para dividir las redes empresariales de las redes públicas, con el fin de mantener la información confidencial fuera del alcance de terceros. Para la metodología de análisis de vulnerabilidades se trabajó con diferentes tipos de arquitecturas de red, con el fin proporcionar a las compañías opciones de acuerdo al plan de seguridad.

Dentro de los diferentes tipos de arquitecturas propuestas, existen las llamadas zonas desmilitarizadas o DMZ (demilitarized zone), las cuales protegen la red privada de la red pública, separando el tráfico de red interna en dos grupos, con el fin de asegurar el control de acceso a los servidores públicos desde la red pública y privada. Las arquitecturas propuestas son[4]:

- *Arquitecturas sin DMZ*
  a. Red básica con un solo Firewall.
  b. Red básica con un solo Firewall y un host bastión

- *Arquitecturas con DMZ*
  c. Firewall básico con una DMZ
  d. Firewall dual con una DMZ

- *Arquitectura de Red con IDS*

- *Arquitectura de Red Inalámbrica (WLAN)*

Una vez establecida la arquitectura, teniendo en cuenta sus ventajas y desventajas[5], se procede con la implementación física de la misma, configurando y actualizando cada uno de los dispositivos que hacen parte de la arquitectura elegida, de tal manera que en su mayoría desaparezca las vulnerabilidades presentes en éstas, ya que solo con el montaje de la arquitectura no se obtiene un nivel suficiente de seguridad.

### 1.5. Fase 5: Aseguramiento Y Configuración De Sistemas Operativos Servicios, Herramientas Y Dispositivos

Gran parte del éxito de la metodología radica en el aseguramiento y buena configuración de los servicios que presta la organización, de las herramientas o aplicaciones que tiene la empresa para su protección, así como de los dispositivos que hacen parte de su arquitectura de red.

Dentro de las herramientas que se utilizan a diario en una organización se encuentra el sistema operativo, el cual controla el acceso y uso de los recursos de una máquina, siendo uno de los elementos más apetecibles para intentar explotar cualquier vulnerabilidad, por lo tanto, en un sistema operativo se debe contemplar:

- Identificación y autentificación de los usuarios.
- Control de acceso a los recursos del sistema.
- Monitorear las acciones realizadas por los usuarios.
- Auditoría de los eventos de posible riesgo.
- Garantía de integridad de los datos almacenados.
- Garantía de la disponibilidad de los recursos.

Además es necesario asegurar los recursos, y controlar su acceso y uso a través de sujetos remotos, tal como es el caso de los archivos compartidos; esta seguridad se debe implementar a través de políticas de seguridad en el sistema por parte de los administradores, con el fin de brindar la protección a los diferentes elementos del sistema.

De la misma manera el aseguramiento de los servicios que presta una organización es una tarea que debe ser realizada con sumo cuidado configurándolos de manera correcta y llevando un seguimiento periódico a los archivos de registro que son creados en cada uno de éstos.

La mayoría de los problemas de seguridad comienzan por una mala configuración de los servicios, los cuales son dispuestos con sus configuraciones por defecto[6] [7], lo cual hace que, para un atacante, sea mucho más sencillo el tener

[4] Documento Metodología de Análisis de vulnerabilidades, Fase 5, página 66

[5] Documento Metodología de Análisis de vulnerabilidades, Fase 5 página 70.

[6] Documento Metodología de Análisis de vulnerabilidades, configuración de dispositivos, páginas 83 a 94.

[7] Ejemplos prácticos: Anexo 5 Manual de la Metodología para configurar los servicios (win2000, Linux, Apache, IIS, Exchange, etc.)

control de éstos. En consecuencia dentro de la metodología se elaboraron una serie de recomendaciones y listas de chequeo[8], con las cuales la organización se puede ayudar para la eliminación de las vulnerabilidades que se encuentran presentes en los dispositivos tales como Firewalls e IDS principalmente, los cuales ayudan a la protección de las redes organizacionales, pero que por si solos no constituyen la solución final a todos los problemas de seguridad; sistemas operativos, servidores y demás, que hacen parte de la arquitectura de red de la compañía. De la misma manera se encuentran las herramientas de apoyo, como lo son los escaneadores de puertos y sniffers, brindan un gran soporte para la comprobación de las configuraciones previamente establecidas.

### 1.6. Fase 6: Auditoria De Sistemas

Una vez implementada la metodología y aseguradas todas las áreas que se tuvieron en cuenta en el plan de seguridad, se procede con la auditoría de sistemas, con el fin de verificar del éxito de la implementación y el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y contengan un buen nivel de seguridad. En la auditoria de sistemas se determina si los sistemas de información salvaguardan los activos, mantiene la integridad de los datos y utiliza eficientemente los recursos.

Dentro de las principales áreas que hacen parte de la auditoría de sistemas, se encuentran:

#### *1.6.1. Auditoría Física*

La auditoría es el medio que va a proporcionar la evidencia de la seguridad física en el ámbito en el que se va a desarrollar la labor profesional, por lo tanto se debe asumir que ésta no se limita a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y seguridad, así como también el correcto uso de las políticas y procedimientos de seguridad.

#### *1.6.2. Auditoría de Bases de Datos*

La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utilizan esta tecnología.

#### *1.6.3. Auditoría de Redes*

En este punto ha de auditarse hasta qué punto las instalaciones físicas ofrecen garantías suficientes para la seguridad de los datos. De la misma manera es necesario monitorear la red, revisar los errores o situaciones anómalas que se producen y además tener establecidos los procedimientos para detectar y aislar equipos posiblemente infectados o comprometidos.

#### *1.6.4. Auditoría de Aplicaciones*

El objetivo de este punto consiste en ayudar a planificar, preparar y llevar a cabo auditorías de aplicaciones en funcionamiento, en cuanto al grado de cumplimiento de los objetivos para los que éstas fueron creadas.

#### *1.6.5. Auditoría de la Seguridad*

En este tipo de auditoría se debe evaluar si los modelos de seguridad están en concordancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones.

### 1.7. Computación Forense

Finalmente la rama de la computación forense apoya la metodología de análisis de vulnerabilidades, con el fin de preparar los equipos y dispositivos[9] con los que cuente una empresa para llegar a realizar un estudio adecuado de los sistemas de información y/o maquinas de trabajo ante la posibilidad o sospecha de una violación de seguridad, llegando a ser ésta evidencia valida en el caso de incurrir en un acto legal[10].

## 2. Pruebas y Resultados

Gracias a que la metodología creada tiene la flexibilidad de adecuarse a cada empresa, brindando la posibilidad de establecer su propio plan de seguridad, evaluación de riesgos y clasificación de la información de acuerdo a su misión y visión, recursos informáticos y económicos según las necesidades y/o recursos

[8] Documento Metodología de Análisis de vulnerabilidades, Anexo 2: Listas de Chequeo

[9] Refiérase a la página 106 del documento Metodología de Análisis de vulnerabilidades.

[10] Refiérase al Anexo 4 del documento Metodología de Análisis de vulnerabilidades.

de la misma, la elaboración y posterior verificación de las cuatro fases iniciales (Planeación, políticas de seguridad, aseguramiento físico y arquitectura de red), están sujetas a los objetivos, políticas y fundamentalmente la apreciación de la organización en cada fase, por lo tanto, las pruebas y los resultados hacen referencia a la fase 5 de la metodología, donde se hacen recomendaciones sobre las distintas configuraciones herramientas escogidas[11] para este fin.

Para la realización de las pruebas se diseñó e implementó un ambiente simulado[12] con el fin de comprobar la fiabilidad y confiabilidad de detección, bloqueo y/o remoción de acciones maliciosas de cada una de las herramientas y servicios configurados de acuerdo con la guía metodológica. El fin de estas pruebas y resultados es el de brindarle a las empresas la facilidad de elegir entre las distintas herramientas en el momento del aseguramiento de la misma.

Figura 2. Ambiente de pruebas con IDS y Firewalls

De esta manera en los resultados obtenidos durante el proceso de pruebas de las distintas arquitecturas de red y las herramientas de protección que se utilizaron en la metodología, se pudo observar variadas similitudes y diferencias entre las herramientas usadas, los dispositivos y los sistemas operativos.

Figura 3. Pruebas de los diferentes ataques en Windows

[11] Refiérase a criterios de Selección de herramientas, documento Metodología de Análisis de vulnerabilidades página 113

[12] Ver Figura 2

Con el fin de garantizar los resultados obtenidos sobre los servicios contra la metodología, se pudo observar que una buena configuración de estas aplicaciones es altamente efectiva para la mayoría de los ataques probados, sin embargo existen algunos casos aislados en los cuales un servicio determinado es vulnerable a cierto tipo de ataques, tal como el caso de MySQL, en donde el 60% de los expolits probados tuvieron efecto, de la misma manera esta situación se dio en el caso de IIS, en el cual el 50% de los ataques de Heap Overflow fueron efectivos.

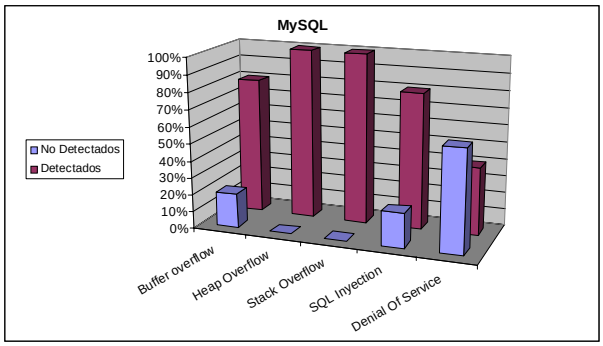


Figura 4. Pruebas sobre MySQL

Por otro lado se encontró, en repetidas ocasiones, que un ataque no era bloqueado o detectado por alguna de estas herramientas o dispositivos de red, sin embargo al configurar el servicio, la vulnerabilidad desaparecía totalmente; de igual forma, si al configurar un servicio alguna vulnerabilidad sigue existiendo, las herramientas de protección pueden llegar a detectar y bloquear un ataque, por tal motivo se confirma que al unir alguna arquitectura con una combinación eficiente de herramientas y además una buena configuración de los servicios y las herramientas, el nivel de seguridad aumenta sustancialmente.

Así, los antivirus de marcas distinguidas de libre distribución o de bajo costo (Antivir, AVG, Bitdefender, Kaspersky) tienden a reconocer de una manera más óptima los archivos sospechosos, los archivos con cuerpo de virus y los virus como tal, en comparación con su similar menos reconocido, trabajando con el mismo tipo de archivos, concluyendo que los antivirus de marcas distinguidas son recomendables para su uso dentro de la aplicación de la presente metodología.

Asimismo, en los resultados de las pruebas hechas con herramientas de protección, como lo son los Firewalls, se encontró que los diferentes tipos de ataques son significativamente más efectivos en Windows que en Linux[13]. Del mismo modo, para el caso de detección de ataques con los IDS, el comportamiento fue similar; sin embargo para algunos casos particulares en donde era necesario descifrar la especificación de los patrones de los ataques, no se logró hacer un análisis de su comportamiento, puesto que se requería una investigación más profunda, la cual no se encontraba dentro del alcance del proyecto de investigación. En consecuencia no se logró hacer una configuración adecuada, la cual ayudara a hacer una más profunda verificación de efectividad de la herramienta ante ataques de SQL Inyección, Manipulation path e Inyección de comandos, ya que se debía aplicar expresiones regulares o una configuración definida para abarcar un mayor numero de patrones con los cuales el IDS soportara su función de verificación.

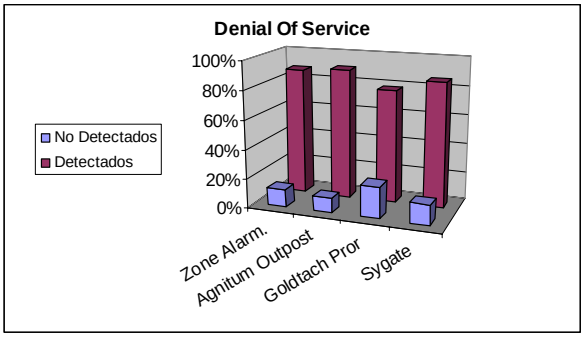


Figura 5. Pruebas sobre Firewalls en Windows

Dentro de los ejemplos para estos casos, se tiene que en Windows el 40% de los ataques de Denial of Service no fueron detectados, sin embargo al probar los mismos contra el Firewall IpTables y el IDS Snort la vulnerabilidad fue cubierta; en otro caso el IDS Snort no detecto el 30% de los ataques de Manipulation path, pero al realizar la configuración del servicio de Internet Information Service, este ataque no tuvo efectividad ya que la vulnerabilidad desapareció.

[13] Ver Figura 4.2 “Pruebas en Linux” página 139 Documento original

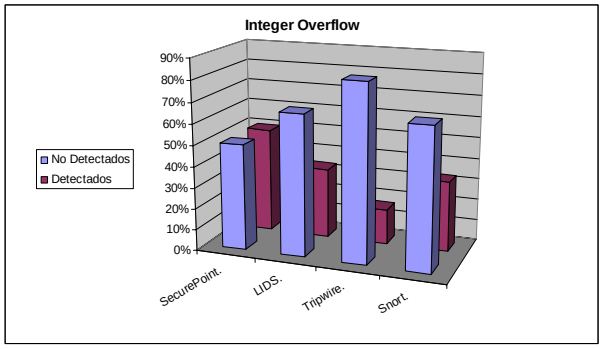


Figura 6. Pruebas sobre IDS en Linux

Como observación final los ataques de Integer Overflow son difícilmente detectables puesto que no siguen un patrón definido, pues éstos se consideran errores de programación de cada proveedor.

## 3. Conclusiones

- Los resultados del análisis de riesgo proveen información sobre las debilidades y vulnerabilidades que posee una organización, siendo éste el punto de partida para la toma de decisiones en relación a la seguridad informática, con el fin de garantizar un aseguramiento exitoso de los sistemas de información.
- Al implementar un plan de seguridad, éste debe adaptarse a la empresa, no la empresa al plan de seguridad; por lo tanto, en el momento de la planeación, la entidad debe escoger los modelos de seguridad adecuados dependiendo de sus necesidades y requerimientos con el fin de minimizar los riesgos.

- El proceso de aseguramiento de los sistemas de información de la empresa debe ser iterativo y controlado en cada una de sus etapas, puesto que debe realizarse una verificación cada una de éstas y llevar un registro de los eventos sucedidos durante cada fase.

- Es necesario involucrar todas las áreas de la empresa para que trabajen con el departamento de tecnología, conocer su infraestructura tecnológica y adaptar las soluciones de seguridad a sus requerimientos y necesidades con el fin de lograr una sinergia total referente al aseguramiento de la compañía.

- El aseguramiento de los recursos informáticos es un proceso, una especificación, no un producto. De tal modo que un adecuado aseguramiento y configuración de éstos no protegerán permanentemente a la empresa, por lo tanto se deben hacer actualizaciones y controles periódicos, donde se pruebe el nivel de seguridad de los dispositivos, servicios y aplicaciones, ya sea para proteger la información o los equipos de la organización.
- En el momento del aseguramiento de los recursos de la organización, una adecuada configuración de los diferentes dispositivos, servicios y aplicaciones le permite a la empresa solucionar en gran proporción las brechas de seguridad que éstos presentan, disminuyendo así la probabilidad de un posible ataque por parte de terceros que aprovechen tal vulnerabilidad.

- Las políticas, estándares y procedimientos de seguridad conforman el conjunto de lineamientos que una organización debe seguir para asegurar sus sistemas, sin embargo éstas por sí solas no constituyen una garantía para la seguridad, por lo tanto deben responder a intereses y necesidades organizacionales basadas en el cometido de la empresa, las cuales lleven a un esfuerzo conjunto para la protección y restauración de los sistemas, así como para administrar sus recursos. En razón a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

- En lo posible se debe probar y comprobar periódicamente el nivel de seguridad de la empresa, tanto la protección de las maquinas de escritorio como las que administran y/o mantienen la información, con el fin de garantizar el aseguramiento físico de los recursos de la organización, puesto que la restricción de su acceso es tan importante como el aseguramiento de la parte lógica.

- La principal barrera que impide el crecimiento de la seguridad informática dentro de la sociedad es el analfabetismo digital que actualmente tiene la mayoría de las personas que conforman la sociedad actual.

- La auditoria de sistemas debe considerarse como un método que ayuda a incrementar y mejorar los procesos de seguridad al interior de la organización.

- Es recomendable que una empresa este preparada para superar cualquier eventualidad que interrumpa las actividades habituales, mediante procedimientos tales como la sincronización y fijación del tiempo de equipos y el registro de actividades.

- La metodología es una buena opción para la aplicación de una infraestructura de seguridad a nivel lógico y físico, pues ésta sirve de guía para empresas que en la actualidad no poseen un área de tecnología de información o no cuenten con los recursos necesarios y adecuados para realizar este tipo de tareas.

## 4. Bibliografía


- [1] CERT, Information Security Statistics (online) http://www.cert.org,
- [2] M. Bishop. Documento electrónico: “A Survey of Vulnerabilities”. Departament of Computer Science, University of California, 2002
- [3] Security Focus. Vulnerabilities. http://www.securityfocus.com
- [4] FBI. http://www.fbi.gov
- [5] CVE. International Organization On Computer Evidence. http://www.ioce.org/ioceprinc.shtml
- [6] Asobancaria, Políticas De Seguridad Informática Del Sector Financiero Colombiano, 2001.
- [7] D. Schweitzer. “Incident Response: Computer Forensics Toolkit”. Wiley Publishing, Inc. 2003
- [8] Network Security Tools, http://www.insecure.org
- [9] T. Pitsenbarger. “Guide to the secure Configuration and Administration of Microsoft Exchange”, NSA “National Security Agency of EE.UU”, 2002

- [10] Seifried. “Linux Administrator’s Security Guide”. 2000

- [11] Common Vulnerabilities and Exposures. http://cve.mitre.org