# PROTECCIÓN INTEGRAL PARA REDES DE AREA METROPOLITANA PRIVADAS Y REDES DE ÁREA DE CAMPUS CONTRA ATAQUES DE MALWARE MODERNO

**Arteaga Delgado Grace Katherine**
**Atiaga Galeas Pablo Alberto**
**Romero Gallardo Carlos**

**kathy_art03@yahoo.com, pablo_ati_g@hotmail.com, cgrmero@espe.edu.ec**

**Universidad de las Fuerzas Armadas - ESPE**
**Sangolquí-Ecuador**

**Resumen**

El artículo describe la implementación de un sistema de seguridad integral simulado dentro de la red de e-GovSolutions S.A. aplicable a una red de área metropolitana o red de área de campus

Se analizó las diferentes tendencias de seguridad de la información empresarial, atacantes y códigos maliciosos avanzados para posteriormente realizar un estudio de las posibles vulnerabilidades que podían existir en los diferentes componentes de la red como son enlaces, servidores, dispositivos finales y factor humano.

Se combinaron recomendaciones, estándares, políticas y herramientas comerciales con herramientas de código abierto que permitirán proveer seguridad en diferentes niveles de la red de manera que no exista huecos de seguridad y permita una protección en tiempo real para ataques conocidos que aprovechan vulnerabilidades del sistema además de proteger contra ataques de malware sofisticados tales como ataques de día cero, malware polimórficos e ingeniería social.

Para probar el sistema de seguridad integral se realizarán varias pruebas incluyendo pruebas de penetración y propagación de diferentes tipos de códigos maliciosos con diferentes vectores de ataques.

## 1. INTRODUCCION

Dentro de la época actual, la información se ha convertido en el activo más importante tanto en el ámbito personal como empresarial y esta información cada vez se sigue almacenando en mayor cantidad en dispositivos informáticos.

La seguridad de redes hoy en día está siendo forzada a avanzar a niveles superiores; las técnicas tradicionales de protección como firewalls, sistemas de prevención de intrusos y antivirus son métodos necesarios pero ya no son suficientes para proteger a las empresas, ya que éstas solo han encontrado la manera de mantener inmunes a los ataques conocidos, de esta manera la industria de malware está creciendo a un ritmo alarmante superando de manera significativa a las defensas tradicionales. [1] (FireEye, Inc., 2013)

Los hackers han desarrollado de manera sigilosa, dinámica y persistente tipos de malware que pueden aprovechar vectores desconocidos. Además los ataques en la actualidad son personalizados, los cuales varían en función de los objetivos de los atacantes.

## 2. PROTECCIÓN DE LA RED

### 2.1 SOLUCIONES PARA SEGURIDAD DE LA RED

Para contrarrestar estos ataques, varias empresas de seguridad han empezado a crear herramientas de nueva generación como son firewalls de nueva generación, sistemas de prevención de intrusos de nueva generación y otros equipos que se especializan en detectar ataques avanzados.

Los primeros en innovar fueron los cortafuegos, Anteriormente parecía suficiente con controlar direcciones IP's y puertos pero ahora, debido a que las aplicaciones son evasivas, vulnerables y usadas para malware, los cortafuegos han

tenido que seguir evolucionando y empezar a detectar las mismas independiente de la dirección y puerto se comuniquen. También se ha visto la necesidad de inspeccionar dentro de estas aplicaciones para ver realmente si son legítimas o están llevando algún código no deseado dentro de ellas y finalmente se ha llegado a la conclusión que los computadores ya no necesariamente se encuentran asociadas a una persona por lo que la mayoría de empresas utilizan servidores de dominio que permiten al usuario autenticarse con du contraseña y es importante que el cortafuegos tome una decisión también con esta información. Las empresas líderes en este ámbito son Palo Alto Networks y Check Point, siendo la primera la que posee una gran ventaja en la visión de su tecnología (Fig. 1)

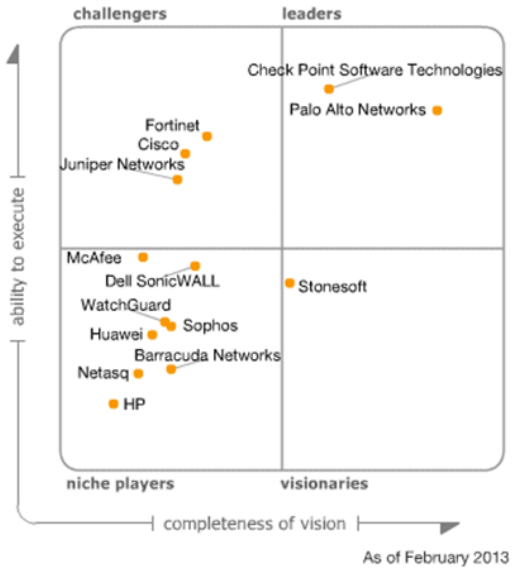


**Figura 1.** Cuadrante mágico de Gartner para firewalls empresariales [2] (Gartner Inc., 2013)

Los sistemas de prevención de intrusos también han ido aumentando sus características de detección y bloqueo. Estas herramientas además de tener sus sistemas basados en firmas han incorporado patrones de comportamiento para poder detectar ataques que no se encuentren en sus bases de datos. Además han incorporado la capacidad de crear "parches virtuales" que lo que buscan es patrones de comportamiento que intenten explotar una vulnerabilidad y en cuanto detectan este tipo de tráfico son capaces de desechar estos paquetes. Los líderes en este campo son Tipping Point de HP, McAfee, SourceFire e Imperva (Fig. 2).

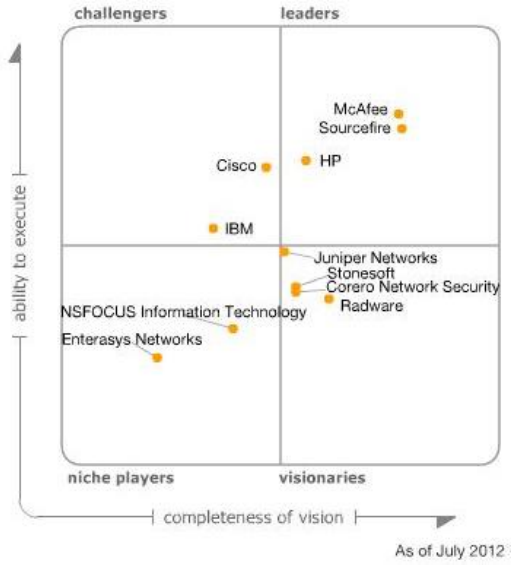


**Figura 2.** Cuadrante mágico de Gartner para sistemas de prevención de intrusos [3] (Gartner Inc., 2012)

Por otro lado existen las tecnologías de honeypot y honeynet que han demostrado ser una solución económica y efectiva de detectar ataques avanzados simulando ser servidores reales vulnerables para que el atacante trate de ingresar a la red o escalar privilegios a través de ellos. Estas tecnologías han dado paso a herramientas que basan su detección en sandbox, las mimas consisten en ejecutar los archivos en diferentes ambientes virtuales con diferentes técnicas de detección para definir su comportamiento benigno o malicioso. Las empresas líderes en esta área son FireEye y Palo Alto Networks.

### 2.2 MATERIALES Y MÉTODOS

Es necesario proteger todos los enlaces existentes con diferentes sistemas de seguridad, colocando protecciones adicionales en los enlaces que van hacia internet. Los dispositivos más importantes son el firewall y el sistema de prevención de intrusos y además en necesario investigar nuevas herramientas existentes que puedan complementar a los sistemas antes mencionados.

Absolutamente todos los enlaces deben estar protegidos por un firewall y un sistema de prevención de intrusos. Para esto se utilizará un firewall de siguiente generación (Palo Alto Networks), el cuál funciona perfectamente como los dos elementos y como tiene una gran versatilidad de ruteo, este reemplazará a los ruteadores que se encuentra dentro de la red de área de campus y de esta forma pueden estar protegidos todos los enlaces internos existentes.

Para el acceso a internet se proveerán soluciones complementarias ya que es el principal vector de donde provienen las amenazas hoy en día, primero hay que tomar en cuenta que el sistema de prevención de intrusos es basado en firmas, por lo que hay que proveer sistemas que sean capaces de bloquear ataques nuevos o desconocidos (FireEye y BotHunter).

Con el objetivo de no tomar ninguna acción, pero proveer mayor información en caso de una alerta se utilizará un sistema de detección de intrusos (Snort), además para tener un elemento con diferente arquitectura de forma que se pueda tener otro filtro de información.

Otro elemento que requiere protección adicional son los servidores WEB que suelen ser el punto de entrada de un atacante a la red interna, para esto se usará un firewall de aplicaciones WEB (ModSecurity).

Para proteger a los servidores de ataques internos, se va a colocar un honeypot (KFSensor) dentro de la DMZ a fin de detectar comportamiento anómalo en esa zona.

### 2.2.1 PALO ALTO NETWORKS

Los cortafuegos de Palo Alto Networks se caracterizan principalmente por funcionar con tres tecnologías principales: [4] (Palo Alto Networks, 2012)

- App-ID
- User-ID
- Content-ID

App-ID es el encargado de identificar las aplicaciones y lo hace mediante cuatro características principales:

- Firmas de aplicaciones
- Decodificación
- Descifrar
- Heurística

User-ID es el encargado de identificar los usuarios y lo hace mediante cuatro características principales:

- Monitoreo de logs
- Descubrimiento de roles
- Polling de estación final
- Portal cautivo

Content-ID es el encargado de inspeccionar el contenido transmitido dentro de las aplicaciones y lo hace en cuatro principales segmentos:

- Archivos
- Datos
- Amenazas
- Filtrado de URL's

Ventajas:

- Amigable
- Latencia muy baja
- Políticas unificadas
- Puede descifrar el tráfico SSL y SSH
- Puede crear firmas de ataques basados en su comportamiento
- Degradamiento de rendimiento muy bajo
- Es muy versátil en networking.
- Da protección completa a usuarios remotos

Desventajas:

- Es el firewall más costoso del mercado.
- El sistema de prevención de intrusos es basado en firmas

### 2.2.2 FIREEYE

FireEye correlaciona los eventos de los hosts detectando patrones sospechosos y además analiza y ejecuta los archivos que son transmitidos en ambientes virtualizados que simulan ser reales.

El sistema de protección de malware para tráfico web (Web MPS) se encarga de controlar el vector de amenazas web. Es un sistema cerrado capaz de controlar exploits web en tráfico de entrada y de salida y callbacks (llamados a servidores externos de comando y control) en diferentes protocolos.

El equipo se encarga de hacer una captura agresiva y analizarla con la ingeniería más sofisticada de virtualización de sistemas para detección de ataques de día cero llamada MVX (Multi-Vector Virtual Execution), la cual permite protección en tiempo real y la captura de callbacks dinámicos. [1] (FireEye, Inc., 2013)

Finalmente una vez que se ha detectado un ataque diferente, todos los equipos FireEye alrededor del mundo son notificados mediante el Malware Protection Cloud (MPC) el cuál es el servicio para descarga de actualizaciones, firmas, parches, versiones de máquinas virtuales y versiones de sistemas operativos.

Ventajas:

- Es capaz de detectar cualquier tipo de malware sofisticado.

- Es capaz de detener callbacks en caso de que ingrese un host infectado.
- Fácil instalación y configuración.
- Es capaz de enviar notificaciones vía correo electrónico o vía syslog hacia un sistema de correlación de eventos.
- No genera latencia.
- Recibe colaboraciones de todas las partes del mundo (MPC Network)

Desventajas:

- Es una herramienta costosa.
- No es capaz de descifrar tráfico.
- Debido a la cantidad de interfaces tiene limitaciones para colocar el equipo en sectores internos.
- El equipo más grande soporta 1Gbps de thoughput, lo que limita su funcionamiento en ambientes muy grandes.

### 2.2.3 SNORT

Snort al igual que todos los sistemas de detección de intrusos tradicionales funcionan a través de reglas que permiten configurar varios parámetros identificativos del tráfico de red de manera que se detecten determinados patrones de comunicación del software malicioso.

La secuencia de acción de Snort se da de la siguiente manera: [5] (Montoro, 2012)

- Captura del paquete.
- Decodifica con la información de protocolos conocidos.
- Se ejecutan preprocesadores predefinidos dependiendo del tipo de tráfico (FTP, SSH, HTTP, IMAP, POP, RPC, Skype, Stream5, entre otros).
- Se compara el resultado con las reglas pre definidas y activadas.
- En caso de que no empate con ninguna regla, el tráfico continúa.
- En caso de que empate con alguna regla, el tráfico continúa a los plugins de salida y toma la acción definida por la regla.

Ventajas:

- Es un software gratuito y de código abierto.
- Tiene gran cantidad de colaboradores alrededor del mundo.
- Es posible la creación de software adicional para mejorar la capacidad de detección de amenazas.
- Se pueden crear reglas propias.
- Proporciona bastante información para un análisis forense.

Desventajas:

- Genera gran cantidad de falsos positivos.
- Requiere bastante esfuerzo, tunning de reglas y análisis.
- No es capaz de detectar malware avanzado no basado en firmas.

### 2.2.4 BOTHUNTER

BotHunter se encarga de analizar los flujos de comunicación que son intercambiados entre el host interno y o más entidades externas, como son escaneo del destino, ejecución de un exploit, descarga de un binario de malware, comunicación con servidores de comando y control y escaneo de salida.

El correlador de BotHunter está basado en el sistema de detección de intrusos Snort del cual se han utilizado el conjunto de reglas enfocadas en malware, además se han aumentado dos plugins llamados SCADE (Analizador de escaneo de puertos tanto de entrada como de salida) y SLADE (Analizador de flujos de tráfico), que analizan el flujo de tráfico [6] (Phillip Porras, 2012)

Ventajas:

- Es un software gratuito.
- Está disponible para varias plataformas (Windows, Linux, FreeBSD, Mac OS) en sus diferentes distribuciones.
- Es un sistema que no se basa en firmas sino en comportamiento.
- Ayuda a detectar si los sistemas están formando parte de botnets.
- Genera pocos falsos negativos.
- Se pueden detectar las etapas de infección del malware.
- Su configuración es bastante sencilla e intuitiva para los usuarios.
- Toma ventaja en relación de los IDS ya que por medio del plugin SLADE se optimiza la utilización de recursos y el tiempo de ejecución es más corto.

Desventajas:

- Requiere realizar un análisis exhaustivo de los resultados para llegar a conclusiones finales
- Entrega gran cantidad de falsos positivos
- No se puede tomar acción sobre el malware que intenta ingresar al equipo víctima.

### 2.2.5 KFSENSOR

Un honeypot es un sistema que simula ser un servidor en la red vulnerable y se lo pone en la red de manera que pueda ser sondeado y atacado y así se pueda obtener información del atacante.

KFsensor es un honeypot de mediana interacción que se ejecuta bajo Windows y permite simular servicios vulnerables, escuchar el tráfico de red y además interactuar con servicios o aplicaciones instalados en el sistema operativo.

KFsensor es un honeypot híbrido, lo que quiere decir que puede implementar tanto servicios simulados (programados por KFSensor) como servicios nativos (instalados y configurados por el usuario), lo que permite dar un ambiente mucho más maduro y real [7] (Keyfocus Ltda., 2013).

El lugar óptimo es colocar el servidor KFSensor dentro de la DMZ o dentro de la zona de servidores internos.

Ventajas:

- Realiza la detección de intrusos basado en Honeypot.
- Detecciones en tiempo real.
- Puede detectar amenazas desconocidas.
- Es eficaz ante amenazas internas y externas.
- Es fácil de usar.
- Se puede configurar según los requerimientos del usuario.
- Emula eficazmente a un servidor.
- Realiza un registro detallado de todas las transacciones.
- Muy bajo número de falsos positivos.
- Se complementa con Snort para trabajar con sus reglas.

Desventajas:

- No sirve para eliminar o corregir fallas de inseguridad.
- Aunque genera patrones para un IDS no es capaz de reemplazarlo.
- Si la red posee vulnerabilidades, instalar un honeypot no ayudará a mitigar estas fallas.
- No evitará que un atacante intente ingresar a la red.

### 2.2.6 MODSECURITY

Es un firewall de aplicaciones web que encarga de prevenir ataques contra aplicaciones web, funciona de manera integrada con el servidor web.

Estas son sus principales características: [8] (Ristic, 2012)

- Las solicitudes entrantes son analizadas a medida que van llegando, y pueden ser filtradas antes que lleguen al servidor web.
- Se utilizan técnicas anti evasión, las rutas y parámetros se normalizan antes de que sean analizados.
- Tiene la capacidad de entender el protocolo HTTP, con lo que se puede realizar filtrado de manera granulada. Por lo que se puede llegar a ver los valores de cookies.
- Se puede interceptar los contenidos transmitidos por medio del método POST.
- Todos los detalles de las solicitudes realizadas se pueden registrar para un análisis forense posterior.
- Filtrado HTTPS; se puede tener acceso a los datos requeridos una vez que hayan sido descifrados.
- Filtrado de contenido comprimido; el motor de seguridad tendrá acceso una vez que se realice la descomprensión de los datos.

ModSecurity realiza un monitoreo en tiempo real las aplicaciones web. Sin embargo no tiene un conjunto de reglas fijas, por lo que depende de cada administrador elegir las funcionalidades que va a entregar a ModSecurity.

Ventajas:

- ModSecurity permite a los desarrolladores y administradores proteger sus servicios web sin necesidad de realizar modificaciones en el código fuente de las aplicaciones.
- Tiene la capacidad de inspeccionar el lenguaje SSL ya que puede desencriptarlo para su análisis.
- Fácil instalación.
- Realiza correlación de los datos y alertas, ya que las peticiones HTTP pasan por el servidor proxy.
- Filtrado simple
- Validación de codificación URL.
- Permite realizar auditorías.
- Prevención de ataques de byte nulo.
- Enmascara la identidad del servidor.

Desventajas:

- No puede detectar ataques de día cero.
- Se demora en obtener nuevas actualizaciones de firmas.
- Disminuye la capacidad de los servidores y aplicaciones.
- Es necesario tener una buena base de conocimiento para lograr entender los ataques que están intentando ingresar a la red, con el fin de poder crear reglas para mitigar estos riesgos.
- La configuración se la realiza de manera manual.

## 3. VULNERABILIDADES EN LOS ELEMENTOS DE LA RED

Las organizaciones deben realizar un análisis de vulnerabilidades constantemente a servidores, dispositivos finales, elementos de seguridad y aplicaciones de manera que se puedan identificar y remediar las brechas de seguridad encontradas de manera que se pueda evitar el ingreso de software malicioso a la red.

El análisis de vulnerabilidades se lo realiza siguiendo los siguientes pasos:

- Descubrimiento.- Identificación de los activos que forman parte de la red, localizando los activos, sistema operativo y todos los servicios que están activos en el sistema.
- Priorización.- Toda organización posee activos que son de mayor importancia que otros ya sea por la información que albergan o por cualesquiera que sean las funciones que este cumpla, por lo cual se debe priorizar cuáles serán los activos que necesitan ser analizados.
- Evaluación.- Es necesario determinar cuáles serán los niveles de riesgo en los cuales se va a enfocar la corrección de errores, esto se basa en la criticidad de los activos y la importancia de los mismos, y se determinará por el administrador de la red. Se debe realizar una evaluación de las vulnerabilidades de forma periódica y programada.
- Informe.- Se basa en medir los riesgos hallados durante el análisis y entregar un reporte con las vulnerabilidades encontradas, esto va a asociado con las políticas de seguridad de la empresa respecto a los activos.
- Remediación.- Reparar las vulnerabilidades encontradas, de acuerdo al riesgo que estas implican en la organización, la remediación se la realiza según como se priorice los activos.
- Verificación.- Se realiza una nueva auditoría para determinar que las vulnerabilidades han sido eliminadas.

### 3.1 QUALYS

Qualys es un escáner de vulnerabilidades, este realiza una gestión completa de las vulnerabilidades, empezando con el descubrimiento de la red para conocer todos los activos que están conectados a la misma, realiza un escaneo, reporta los datos encontrados, informa acerca de la remediación y finalmente se recomienda realizar un escaneo para verificar que las vulnerabilidades fueron mitigadas.

Para realizar la gestión de vulnerabilidades se utiliza el módulo VM (Vulnerability Management), con esta aplicación se automatiza el ciclo de vida de la auditoría de la red, para realizar dicha auditoría se deben cumplir cuatro pasos:

- Mapeo de la red
- Escaneo de vulnerabilidades
- Reporte de Vulnerabilidades
- Remediación

Por medio del módulo WAS (Web Application Scanner) se puede realizar:

- Escaneo de aplicaciones web en busca de vulnerabilidades.
- Identificar como se manejan los datos confidenciales.
- Crear listas blancas para evitar falsos positivos.
- Entregar reportes con prácticas a seguir, lista detallada de vulnerabilidades, etc.

Ventajas

- Interfaz de usuario amigable
- Reportes flexibles y totalmente personalizables en diferentes formatos.
- Realiza un análisis más profundo que herramientas open source.
- Se pueden usar filtros según las necesidades del usuario.
- Entrega un resumen detallado de las vulnerabilidades.
- Escaneos de aplicaciones web que contienen JavaScript y flash.

Desventajas

- Herramienta Costosa.
- Basada en web.

## 4. FACTOR HUMANO Y PROTECCIÓN DE DISPOSITIVOS FINALES

Todas las personas que forman parte de una empresa deben tener un conocimiento de las amenazas actuales y como las mismas pueden ser un riesgo para la empresa y su información.

Es necesario que toda empresa tenga políticas de seguridad de la información, el cual es un documento de alto nivel establecido por la gerencia y el departamento de seguridad de la información en el que se debe expresar el compromiso de la empresa acerca de la protección de su información y la de sus empleados.

Las empresas líderes para la protección de dispositivos finales son Kaspersky, Symantec, McAfee, Trend Micro y Sophos (Fig. 3).

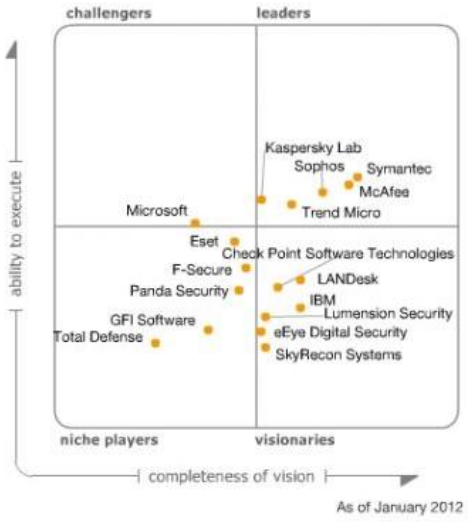


**Figura 3.** Cuadrante mágico de Gartner para seguridad de dispositivos finales. [9] (Gartner Inc., 2012)

### 4.1 KASPERSKY INTERNET SECURITY

Kaspersky Internet Security se especializa en la protección de los dispositivos finales y en todo el vector de ataque que puede venir asociado con el mismo. Las características principales son las siguientes: [10] (Kaspersky Lab., 2013)

- Protección contra virus y amenazas de Internet.
- Detecta amenazas nuevas y emergentes.
- Identifica sitios web sospechosos y sitios web de phishing.
- Brinda mayor seguridad para compras y actividades bancarias en línea.
- Protege la privacidad e identidad digital.
- Impide que el malware aproveche las vulnerabilidades de la estación de trabajo.

Ventajas:

- Se enfoca en archivos maliciosos a nivel de dispositivo final.
- Los laboratorios sofisticados y la ayuda en tiempo real de colaboradores y clientes proveen una respuesta ágil en caso de nuevas amenazas descubiertas.
- Costo muy bajo.
- Afectación mínima en el rendimiento de la estación de trabajo.
- Provee protecciones adicionales al momento de ingresar información confidencial por medio de tráfico web.

Desventajas:

- Es basado en firmas.
- Es incapaz de detectar un ataque sin una firma de por medio.
- No puede descifrar tráfico.

### 4.2 SECUNIA PSI

Secunia PSI (Secunia Personal Software Inspector) es un software gratuito que se encarga de verificar que los programas instalados en una estación de trabajo estén actualizados.

Ventajas:

- No se necesita actualizar manualmente los programas instalados en el equipo, pues Secunia PSI lo hace de manera automática.
- Tiene gran cantidad de programas en su base de datos para mantenerlos actualizados.
- Es gratuito

Desventajas:

- Consume recursos del sistema.
- Contiene algunos bugs al intentar la descarga de actualizaciones automáticas.

## 5. EVALUACIÓN PRÁCTICA

Las distintas metodologías para análisis de seguridad son las siguientes: (Fig. 4).

- Vulnerability Scanning: se refiere generalmente a los chequeos automatizados para encontrar vulnerabilidades conocidas en un sistema o los sistemas de una red.

- Security Scanning: se refiere generalmente a escaneos de vulnerabilidad que incluyen verificación manual de falsos positivos, identificación de debilidades en la red y análisis profesional personalizado.
- Penetration Testing: se refiere generalmente a un proyecto orientado a un objetivo en el cual el objetivo es el trofeo e incluye la obtención de acceso privilegiado a través de condiciones pre-establecidas.
- Risk Assesment: se refiere generalmente a un análisis de seguridad a través de entrevistas e investigación de mediano nivel, la cual incluye justificaciones del negocio, legales y justificaciones específicas a la industria.
- Security Auditing: se refiere generalmente a una inspección de seguridad privilegiada del sistema operativo y las aplicaciones de un sistema o de varios sistemas en varias redes.
- Ethical Hacking: se refiere generalmente a un test de penetración en el cual el objetivo es descubrir trofeos en la red dentro de un tiempo límite del proyecto.

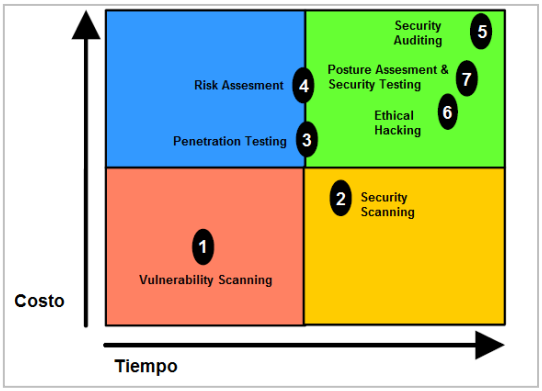


**Figura 4.** Tipos de metodologías de análisis de seguridad basados en tiempo y costo ([11] Herzog, 2010)

El sistema integral propuesto consiste en la protección de los enlaces de la red de área de campus (Palo Alto Networks), protección del enlace de internet (FireEye y Palo Alto Networks), sistema de detección de intrusos para el enlace de internet (Snort), sistema de detección de botnets por comportamiento (BotHunter), protección de la DMZ (Palo Alto Networks y KFSensor), protección de las aplicaciones web (Palo Alto Networks y ModSecurity) y protección de estaciones finales (Kaspersky y Secunia PSI). A partir de este momento se realizarán pruebas para analizar las respuestas de los diferentes equipos de seguridad.

Al utilizar una herramienta líder en el mercado como QualysGuard complementada con herramientas de código abierto BackTrack, se consigue un test de penetración más completo, automatizado y preciso logrando una reducción de falsos positivos y negativos significativa, lo que permite al cliente reducir el tiempo de interpretación y remediación de las vulnerabilidades, minimizando el riesgo de un posible ataque.

Dentro de las metodologías usadas se cuenta con: Mapeo, Enumeración, Descubrimiento y análisis de vulnerabilidades, etc.

Las pruebas ejecutadas fueron las siguientes:

- Identificación de Sistemas Operativos, se identifican los sistemas operativos y la versión de los mismos, en busca de información relevante para un atacante.
- Identificación de Servicios, se identifican los servicios y la versión de los mismos, en busca de información relevante para un atacante.
- Escaneo de Puertos, se realiza la identificación activa de los puertos visibles de forma pública, se identifican en ellos la versión de servicio, identificación del mismo, versión y vulnerabilidades.
- Análisis de Vulnerabilidades, se realizan baterías de pruebas tanto a la infraestructura pública de la organización como a las aplicaciones web publicadas. Para identificar claramente vulnerabilidades y problemas de configuración que puedan significar riesgos importantes en la organización.
- Identificación de Información, se identifica la información de valor para un atacante y que puede representar un riesgo para la organización.

Las pruebas a realizar fueron las siguientes:

- Test de penetración desde una de las sedes simuladas a la DMZ.- En la presente prueba se utilizaron servidores Windows y Linux en los cuales Palo Alto Networks logró bloquear incluso los intentos de visibilidad de más de 100 vulnerabilidades existentes además de bloquear los intentos de explotación de las vulnerabilidades encontradas. Por

otro lado KFSensor registró todas las peticiones y actividades que se realizaron contra el honeypot de manera que se pudo identificar al posible atacante.

- Test de penetración desde una de las sedes simuladas a una aplicación WEB.- En la presente prueba se realizaron varios intentos de ataques manuales en los cuáles ModSecurity demostró su acción de bloqueo inmediata. Posteriormente se realizó el test de penetración en el cuál Palo Alto Networks no logró bloquear la visibilidad de algunas vulnerabilidades encontradas, en cambio ModSecurity logró bloquear todos los intentos de visibilidad y explotación.
- Descarga de diferentes tipos de archivos maliciosos conocidos.- Para esta prueba se descargaron diferentes archivos maliciosos nuevos pero conocidos del sitio http://www.malwaredomainlist.com para comprobar el bloqueo inmediato de Palo Alto Networks al intentar la descarga de los mismos y además se los transfirieron a través de un dispositivo extraíble y se pudó demostrar el bloqueo y remediación inmediata por parte de Kaspersky Internet Security.
- Descarga de un archivo malicioso de día cero.- Para descargarse ataques de día cero hay como hacerlo de diferentes sitios web actualizados instantáneamente o crear uno con diferentes herramientas disponibles en el mercado. En este caso se procedió a investigar en la web un archivo malicioso que no sea bloqueado en primera instancia por Palo Alto Networks ni por Kaspersky y que tampoco sea detectado por Snort. Posterior a la descarga se pudo visualizar que FireEye y Palo Alto Networks entregaron reportes demostrando el comportamiento malicioso que tuvo el archivo después de ser analizado en sus respectivos ambientes virtuales.
- Infección de un host para análisis de comportamiento con los sensores.- En la presente prueba ejecutaron variedades de códigos maliciosos dentro de una máquina vulnerable y se pudo visualizar que snort y bothunter pueden entregar información importante para realizar el análisis forense de un host infectado, en este caso se pudieron visualizar descarga de archivos maliciosos, software instalado dentro del host y comunicaciones con diferentes servidores de comando y control.

## 6. CONCLUSIONES

La tendencia en los siguientes años será que por lo menos un 50% de la información se encuentre en la nube, esto logrará que los atacantes se vuelvan más sofisticados y persistentes en busca de esa información.

No existe ninguna persona o empresa que esté utilice cualquier tipo de dispositivo informático que se encuentre excluyente a los ataques informáticos ya que todos tienen información que pueden interesar a diferentes tipos de atacantes.

La necesidad de conectividad de empresas grandes y el crecimiento tecnológico está haciendo que cada vez existan más redes de área metropolitana y redes de áreas de campus, y debido al alto valor que manejan las empresas en temas informativos, la necesidad de seguridades avanzadas está incrementando el capital presupuestado anual en herramientas de seguridades en redes.

Las redes de área metropolitana y redes de área de campus requieren mayores protecciones que una LAN debido a que tiene más puntos de falla y requiere proteger todos sus enlaces de manera que se pueda mitigar en ataque independientemente desde que enlace se genere el mismo.

No existe ninguna herramienta que sea capaz de detectar y bloquear la gran variedad de ataques que existen actualmente por lo que siempre se debe buscar un sistema integral de manera que las diferentes herramientas sean capaces de bloquear ataques que las otras no son capaces de hacerlo.

Además de la calidad de las herramientas, es necesario realizar configuraciones adecuadas a la funcionalidad de las mismas dependiendo de cada empresa, esto logrará tener un mayor control y visibilidad del entorno de red.

Es necesario evaluar cada entorno de red y detectar y corregir las vulnerabilidades que pueden existir en los enlaces y en los sistemas operativos, servicios y aplicaciones de servidores de elementos de red, herramientas de seguridad, servidores y dispositivos finales.

El factor humano es el eslabón más débil en la cadena de seguridad de una empresa por lo que para reducir el riesgo de infección es obligatorio tener un personal capacitado con políticas de seguridad de la información regulatorias trabajando en estaciones de trabajo seguras y actualizadas.

El sistema de seguridad propuesto ha demostrado ser seguro ante las diferentes pruebas realizadas con una gran diversidad de ataques y vectores de ataque, emulando las posibles situaciones que pueden aparecer en el entorno empresarial.

## 7. BIBLIOGRAFÍA


[1] FireEye, Inc. (2013). FireEye Corporate Presentation.

[2] Gartner Inc. (2013). Gartner Magic Quadrant for Enterprise Network Firewalls.

[3] Gartner Inc. (2012). Gartner Magic Quadrant for Network Intrusion Prevention systems.

[4] Palo Alto Networks. (2012). Customer Overview.

[5] Montoro, R. (2012). Snort Training. Guayaquil.

[6] Phillip Porras, M. F. (2012). Cyber-TA: BotHunter distribution page. Obtenido de http://www.cyber-ta.org/releases/botHunter/index.htm

[7] Keyfocus Ltda. (2013). KFSensor Overview. Obtenido de http://www.keyfocus.net

[8] Ristic, I. (2012). ModSecurity Handbook. Obtenido de http://www.modsecurity.org/documentation/modsecurity-

[9] Gartner Inc. (2012). Gartner Magic Quadrant for Endpoint Protection Platforms.

[10] Kaspersky Lab. (2013). Kaspersky - Internet Security. Obtenido de http://latam.kaspersky.com/productos/productos-para-el-hogar/internet-security

apache/1.9.3/modsecurity-manual.html

[11] Herzog, P. (2010). Open Source Security Testing Methodology Manual.


## 8. BIOGRAFÍA DE LOS AUTORES

*Grace Katherine Arteaga Delgado* nació el 10 de Marzo de 1986 en la ciudad de Manta. En el año 2004 obtiene el título de Bachiller especialidad Físico-Matemático en el Colegio Geovanni Farina. En el año 2011 egresa de la carrera de Ingeniería en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército. En la actualidad trabaja en SIMAA S.A. y aspira conseguir el título de tercer nivel en los estudios mencionados.

*Pablo Alberto Atiaga Galeas.* Nació el 11 de Diciembre de 1987 en la ciudad de Quito. En el año 2004 obtiene el título de Bachiller especialidad Ciencias en el Colegio Particular Experimental “Lev Vygotsky”. En el año 2011 egresa de la carrera de Ingeniería en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército. En la actualidad trabaja en e-GovSolutions S.A. y aspira conseguir el título de tercer nivel en los estudios mencionados.

*Carlos Gabriel Romero Gallardo.* Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército (2002) y Especialista en Proyectos de Investigación Científica y Tecnológica en la Universidad Complutense de Madrid (2006). Candidato a PhD Universidad Nacional de la Plata. Es profesor de la Escuela Politécnica del Ejército. Sus áreas de interés e investigación son Seguridad de la Información, Networking con TCP/IP e Implementación de servicios y aplicaciones con software libre