Implementación de una herramienta para administrar el uso de los navegadores[1] mediante un proxy, para los usuarios de una red.

Estrella Flórez, Sandra Patricia Bohórquez, Martha Doreila Cabrera
Estrellaflorez@hotmail.com, engineers.exe0@gmail.com, marthadoreila2013@outlook.es
Asesores: Ingeniero Peter Alejandro Agudelo, Ingeniero Carlos Ignacio Torres
Universidad Cooperativa de Colombia
Villavicencio (Meta), Colombia
2016

***Resumen*—** *Hoy en día, las personas viven en un mundo donde todo está controlado por la tecnología, las ventajas que trae consigo han revolucionado miles de vidas, pero al mismo tiempo la seguridad e integridad de la información está constantemente expuesta al peligro. Para minimizar los riesgos a los que las personas están expuestas a diario, existen diversas herramientas en el mercado, en este documento se detallará una de esas alternativas que funciona en un ambiente Microsoft que ayuda, en un entorno empresarial, para combatir la inseguridad que pueda afectar a las redes de las empresas, para proteger los ordenadores de software malicioso, para ajustar los horarios y limitar el consumo de ancho de banda, de esa manera tratar de ofrecer un ambiente seguro y optimizar el rendimiento de los empleados.*

Palabras Claves*—Seguridad; Información; Web; Proxy; Virtualización*

***Abstract*—** *Nowadays, people live in a world where everything is controlled by technology, the advantages that brings with it have revolutionized thousand of lives but at the same time the security and integrity of information is constantly exposed to danger. To minimize the risks that everybody fights daily unconsciously when they surf the net, this document contains detailed information about some Microsoft tools that helps, in a business environment, to battle the insecurity that might affect business networks, to protect computers from malicious software, to set schedules and limit the bandwidth consumption, that way trying to offer a safe environment and optimize employee performance.*

Keywords*—Security; Information; Web; Proxy; Virtualization.*

I. INTRODUCCIÓN

Hoy por hoy, la seguridad informática se ha convertido en una necesidad apremiante dado el gran avance tecnológico que trae consigo cambios constantes y nuevas plataformas de computación disponibles, siendo posible traspasar las fronteras de las organizaciones gracias a la interconexión de las redes. Con los avances tecnológicos también llegan las amenazas en los sistemas computarizados, entonces surgen las políticas de seguridad informática (PSI), como herramienta organizacional para concientizar a los miembros de las organizaciones que trabajan con computadoras conectadas a una red. Las organizaciones deben tener normativas para el uso adecuado de los recursos y de los contenidos, es decir el buen uso de la información, la importancia y la sensibilidad de la misma.

Existen varias herramientas de conexión a Internet que hacen de intermediario entre los PCs de la red y el router de conexión a Internet. La herramienta que se uso para este proyecto fue GFI WebMonitor, la cual se ejecuta a través de una página web, y permite administrar la actividad del ingreso y las descargas realizadas al sitio web por parte de los usuarios que están conectados a una red de una compañía; esta herramienta analiza el tráfico de redes en la internet a tiempo real, es decir, que da una estadística donde permite ver que usuario ingreso, a qué hora, el tiempo de duró en la web, cuánto ancho de banda consumió, a qué páginas ingresó, entre otros, según la política que se haya configurado y lo que se viene produciendo desde el inicio del GFI WebMonitor, esta herramienta permite el bloqueo de redes sociales y descargas, aumentando significativamente la productividad de la empresa entre otros. [1]

II. JUSTIFICACIÓN

La era tecnológica actual está rodeada de peligros informáticos y las organizaciones están más vulnerables que nunca, debido al desconocimiento o a la incredulidad de las amenazas cibernéticas, un gran número de empresas han sido víctimas de ataques, que al final resultan en pérdidas millonarias más elevadas de lo que pudo costar la implementación de herramientas de protección.

Para aseverar esta información, empresas dedicadas a la seguridad informática han revelado estadísticas sobre el país que dejan una gran preocupación respecto al tema.

> "El 49 % de las empresas colombianas sufrió infección por malware durante el 2015. Esto significa que la mitad de las compañías nacionales perdieron información. Y lo más

[1] Los navegadores en los que la herramienta se utilizó son: IE, Mozilla Firefox, Safari, Opera y Google Chrome.

paradójico es que la ocurrencia de estos eventos son casi que diarios.

La firma de seguridad Cisco reveló que en lo corrido del 2015 "el país sufrió pérdidas por alrededor de un billón de pesos debido a ataques cibernéticos de diversa índole, robo de información y fraudes informáticos […]

La empresa Kaspersky Lab, hizo un sondeo que reveló estadísticas dicientes sobre los usuarios finales. Según el estudio realizado, el 28 % de la gente comparte datos confidenciales por accidente, mientras que un 16 % revela secretos acerca de si mismos, de manera voluntaria. De igual forma, se concluyó que el 13 % de las personas no toma aún ninguna precaución para mantener sus actividades en línea." (Revista Semana, 2016).

Estos datos demuestran la fragilidad de las organizaciones colombianas frente a esta problemática de la que no se quiere hacer frente principalmente por cuestiones económicas.

Este proyecto presenta una solución para evitar pérdidas como las mencionadas por medio de la administración de un controlador de dominio y la implementación de una herramienta para entorno Microsoft; ofrece a un ambiente empresarial el control del contenido web que visitan sus empleados mediante políticas de seguridad a perfiles de usuario y un escaneo de descargas para evitar infecciones que puedan perjudicar toda la red.

III. OBJETIVOS

OBJETIVO GENERAL

Administrar una herramienta proxy para controlar el tráfico del HTTP y HTTPS a través de un controlador de dominio en un entorno Microsoft.

OBJETIVOS ESPECÍFICOS

- Crear un controlador de dominio en el servidor para la creación de usuarios y aplicación de GPO's.
- Aplicar mediante GPO's la configuración del servidor proxy en computadores clientes del dominio.
- Instalar la herramienta GFI WebMonitor para administrar el uso de los navegadores Opera, Google Chrome, Mozilla Firefox, Safari e Internet Explorer.
- Ingresar las políticas de seguridad en la herramienta GFI WebMonitor, establecidas por la alta dirección, para la administración de los navegadores.

IV. DESARROLLO

A. ESTADO DEL ARTE

Actualmente existen diferentes herramientas que se encargan de proxy web más usadas en el mercado, tales como:

MCAFEE WEB GATEWAY: McAfee Web Gateway ofrece seguridad integral para todos los aspectos del tráfico de la Web, con independencia de la ubicación o el dispositivo. Para las solicitudes web iniciadas por el usuario, McAfee Web Gateway implementa en primer lugar la directiva de uso de Internet de la empresa.

A continuación, para todo el tráfico permitido, utiliza técnicas locales y globales para analizar la naturaleza y la intención de todo el contenido y el código activo que entran en la red a través de las páginas web solicitadas, con el fin de proporcionar protección inmediata frente al malware y otras amenazas ocultas. Y, a diferencia de las técnicas básicas de inspección de paquetes, McAfee Web Gateway puede examinar el tráfico SSL con el fin de ofrecer protección exhaustiva contra código malicioso o aplicaciones inadecuadas que se han "disfrazado" mediante técnicas de cifrado

La protección del tráfico entrante reduce también el riesgo para las organizaciones que albergan sitios web que aceptan cargas de datos o de documentos de fuentes externas. McAfee Web Gateway en modo proxy inverso analiza todo el contenido antes de que se cargue, protegiendo de esta forma tanto el servidor como el contenido.

Para proteger el tráfico saliente, McAfee Web Gateway utiliza nuestra tecnología líder de prevención de fugas de datos (DLP) para analizar el contenido generado por los usuarios en todos los protocolos principales de la Web, incluidos HTTP, HTTPS y FTP, y proteger frente a la pérdida de información confidencial o sometida a normativas, a través de sitios de redes sociales, blogs, wikis o herramientas de productividad online, como las de correo web, los organizadores y las agendas. McAfee Web Gateway también evita que los datos no autorizados salgan de la organización a través de equipos infectados por bots que intentan enviar información al atacante o transmitir datos confidenciales.

Licencias para disponer de la mayor flexibilidad de despliegue y proteger su inversión para el futuro, McAfee ofrece todas las funciones de McAfee Web Gateway y del servicio McAfee SaaS Web Protection en una única suite: McAfee Web Protection. Hay disponibles opciones de despliegue in situ, en la nube, o ambos para una mayor flexibilidad y la mayor disponibilidad. Usted elige. Todas las opciones le permitirán disfrutar de la galardonada protección antimalware y filtrado web completo de McAfee. El hardware de McAfee Web Gateway se vende por separado. (Corporativo Intel Security, 2016)

SYMANTEC WEB GATEWAY: Protege a las organizaciones contra varios tipos de software malicioso provenientes de la Web y brinda a las organizaciones la flexibilidad de implementar este producto como appliance virtual o en hardware físico. Con el respaldo de Insight, la innovadora tecnología de filtrado de software malicioso basado en reputación de Symantec, Web Gateway se basa en una red global de más de 210 millones de usuarios para identificar

nuevas amenazas antes de que provoquen interrupciones en las organizaciones.

La tecnología de Symantec Insight brinda protección proactiva contra las amenazas mutantes, dirigidas y nuevas

- Detecta amenazas a medida que se crean
- Utiliza el contexto para reducir los falsos positivos y la sobrecarga administrativa
- Con el respaldo de los conocimientos colectivos de más de 210 millones de sistemas

La integración con Network Prevent for Web de Symantec Data Loss Prevention facilita una sólida solución de prevención contra la pérdida de datos y Web de un solo distribuidor

- Evita que los datos confidenciales salgan de la red corporativa por medio de la Web
- Disminuye el riesgo de pérdida de datos mediante la aplicación automática de las políticas de seguridad de la organización
- Cambia el comportamiento de los usuarios mediante la educación en tiempo real sobre las políticas con notificaciones sobre las infracciones de las políticas

Opción de implementación de appliance virtual

- Los clientes ahora pueden implementar Web Gateway como appliance físico, virtual o una combinación de ambos

La capacidad de almacenamiento en memoria caché y proxy satisface las necesidades de los clientes que:

- Requieren un proxy en la topología de red
- Requieren memoria caché HTTP para conservar el ancho de banda
- Desean descifrar SSL y/o integrarlo con Symantec Data Loss Prevention.

Funciones clave

- Con el respaldo de la red Symantec Global Intelligence Network
- Con el respaldo de la tecnología de Symantec Insight
- El software de filtrado web se integra perfectamente con Symantec Data Loss Prevention
- Capacidades de control de aplicaciones
- Filtrado de URL de Symantec RuleSpace con configuración flexible de políticas
- Opción de implementación del appliance físico o virtual
- Capacidades de descifrado de SSL
- Varias capas de protección de software malicioso
- Se integra con el galardonado motor de Symantec AntiVirus

Beneficios clave

Protección

- El software de filtrado de contenido web cuenta con el respaldo de la red Symantec Global Intelligence Network, con actualizaciones en tiempo real para reforzar la protección
- Integra el galardonado motor de Symantec AntiVirus
- La tecnología de Symantec Insight brinda protección proactiva contra las amenazas mutantes, dirigidas y nuevas.

Control

- La integración con Network Prevent for Web de Symantec Data Loss Prevention facilita una sólida solución de prevención contra la pérdida de datos y Web de un solo distribuidor
- La lista de filtrado de URL de Symantec RuleSpace brinda a los administradores la posibilidad de supervisar, bloquear o permitir el acceso a millones de direcciones URL que representan a mil millones de páginas web organizadas en aproximadamente 100 categorías diferentes
- La lista de filtrado de URL ofrece a los administradores la capacidad de supervisar, bloquear o permitir el acceso a más de 100 millones de sitios web organizados en 62 categorías diferentes. (Symantec Corporation US, 2016)

DANSGUARDIAN: Es un galardonado filtro de contenido web de código abierto, que actualmente se ejecuta en Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX y Solaris. Se filtra el contenido real de las páginas basadas en muchos métodos, incluyendo la concordancia de frase, el filtrado PICS y filtrado de URL. Es puramente no filtrado basado en una lista de sustancias prohibidas de sitios como filtros menor totalmente comerciales.

DansGuardian está diseñado para ser completamente flexible y le permite adaptar la filtración a sus necesidades exactas. Puede ser tan draconiano o como un obstructive como desee. Los ajustes predeterminados están orientados hacia lo que una escuela primaria, pero puede ser que desee DansGuardian te pone en control de lo que quiere bloquear.

Con DansGuardian puede utilizar lo que cada vez proxy que desea, siendo la más común calamar y Privoxy. Abajo son dos formas de instalar DansGuardian con el calamar o Privoxy.

Calamar: Squid es un demonio del servidor proxy y caché web. Cuenta con una amplia variedad de usos, desde acelerar un servidor web mediante el almacenamiento en caché peticiones repetidas; para el almacenamiento en caché de web, DNS y otras búsquedas de la red de ordenadores para un grupo de personas que comparten los recursos de red; para ayudar a la seguridad filtrando el tráfico. Aunque se utiliza principalmente para HTTP y FTP, calamar incluye un soporte limitado para varios otros protocolos, incluyendo TLS, SSL, Internet Gopher y HTTPS.

Privoxy: Es un proxy web no almacenamiento en caché con capacidades de filtrado para mejorar la privacidad, la manipulación de las galletas y la modificación de los datos de las páginas web y las cabeceras HTTP antes de que la página se

representa por el navegador. Privoxy es un anuncio "potenciadoras de la privacidad de proxy", el filtrado de páginas Web y la eliminación. Privoxy puede ser personalizado por los usuarios, tanto para los sistemas autónomos y redes multi-usuario. Privoxy puede ser encadenado a otros servidores proxy y se utiliza con frecuencia en combinación con el calamar y se puede utilizar para eludir la censura en Internet. También se incluye con Tor para aumentar la privacidad. (Community Ubuntu, 2016)

B. MARCO TEORICO

- **SEGURIDAD:** La seguridad puede entenderse como aquellas reglas destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño. (Centro Criptológico Nacional, 2015)
- **SEGURIDAD INFORMATICA:** Disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, así como su transmisión.

  Técnicamente resulta muy difícil desarrollar un sistema informático que garantice la completa seguridad de la información, sin embargo, el avance de la tecnología ha posibilitado la disposición de mejores medidas de seguridad para evitar daños y problemas que puedan ser aprovechados por los intrusos. Dentro de la seguridad informática se pueden mencionar dos tipos: seguridad lógica y seguridad física. (Centro Criptológico Nacional, 2015)
- **ARQUITECTURA DE SEGURIDAD:** Un planteamiento y un plan que cubre: (a) los servicios de seguridad que se le exigen a un sistema, (b) los componentes necesarios para proporcionar dichos servicios y (c) las características que se requieren de dichos componentes para enfrentarse eficazmente a las amenazas previsibles. (Centro Criptológico Nacional, 2015)
- **VIRTUALIZACIÒN:** Un es una tecnología probada de software que permite ejecutar múltiples sistemas operativos y aplicaciones simultáneamente en un mismo servidor. Está transformando el panorama de TI y modificando totalmente la manera en que las personas utilizan la tecnología. (Centro Criptológico Nacional, 2015)
- **ENTORNO VIRTUAL:** Es un espacio alojado en la web, conformado por un conjunto de herramientas informáticas o sistema de software que posibilitan la interacción didáctica. (Centro Criptológico Nacional, 2015)
- **VIMWARE:** Es una filial de EMC Corporation (propiedad a su vez de Dell Inc) que proporciona software de virtualización disponible para ordenadores compatiblesX86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Servery VMware Player. El software de VMware puede funcionar en Windows, Linux, y en la plataforma Mac OS X que corre en procesadores Intel, bajo el nombre de VMware Fusion. El nombre corporativo de la compañía es un juego de palabras usando la interpretación tradicional de las siglas «VM» en los ambientes de computación, como máquinas virtuales (Virtual Machines). (VMware, Inc, 2016)
- **CONTROLADOR:** Programa que comanda los periféricos conectados a la computadora. (Centro Criptológico Nacional, 2015)
- **DOMINIO:** Conjunto de caracteres que identifica la dirección de un sitio web. (Centro Criptológico Nacional, 2015)
- **DIRECCIONAMIENTO IP:** Usado para identificar únicamente un dispositivo en una red del IP. El direccionamiento se compone de 32 bits binarios, que pueden ser divisibles en una porción de la red y recibir la porción con la ayuda de una máscara de subred. Los 32 bits binarios se dividen en cuatro octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa con un punto. Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor en cada octeto posee un rango decimal de 0 a 255 o binario de 00000000 a 11111111. (Centro Criptológico Nacional, 2015)
- **RED DE DATOS:** Un aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la Transmisión de información mediante el intercambio de datos. Las redes de datos se diseñan y construyen en Arquitecturas que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la Comunicación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física. (Centro Criptológico Nacional, 2015)
- **HOST:** Es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red. (Centro Criptológico Nacional, 2015)
- **SPAM:** Se denomina ’spam’ a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El ’spam’ generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias. (Centro Criptológico Nacional, 2015)
- **PHISHING:** simulación, algunas veces perfecta, de una página Web de un banco solicitando el ingreso de claves secretas, con la excusa de la aplicación de nuevas políticas de seguridad de la entidad. Dentro del enlace a la noticia de Hispasec, se recomienda la visualización de los vídeos explicativos en flash con los altavoces del PC encendidos. (Centro Criptológico Nacional, 2015)
- **PROXY:** Es un programa o software que permite que varios computadores accedan a Internet a través de una única conexión (distribuida por un computador Servidor). El Proxy actúa como intermediario entre el Servidor y los computadores para controlar las páginas Web visitadas, monitorear el tráfico de las conexiones, proteger el correo

electrónico, entre otras cosas. (Centro Criptológico Nacional, 2015)

- **AUTENTICACIÒN:** Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se lo puede utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. (Centro Criptológico Nacional, 2015)
- **HTTP:** Hypertext Transfer Protocol. Protocolo de transferencia de hipertextos. Es un protocolo que permite transferir información en archivos de texto, gráficos, de video, de audio y otros recursos multimedia. (Centro Criptológico Nacional, 2015)
- **DNS:** Domain Name System. Sistema de Nombres de Dominio. Método de identificación de una dirección de Internet. Según este método, cada computadora de la red se identifica con una dirección unívoca, la URL (Uniform Resource Locator), compuesta de grupos de letras separados por puntos. Esa dirección se obtiene subdividiendo todas las computadoras en grupos grandísimos llamados TLD (Top Level Domain) que son afines entre sí por alguna razón. Por ejemplo están los TLD basados en la identificación geográfica (donde.ar es Argentina,.uy es Uruguay, .cl es Chile) y los grupos basados en el tipo dominante de actividad (.com para actividades comerciales; .edu para fines educativos). (Centro Criptológico Nacional, 2015)
- **SERVIDOR:** Una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos. almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML. (Centro Criptológico Nacional, 2015)
- **DHCP:** Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red. Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host. (Centro Criptológico Nacional, 2015)
- **CONEXIÒN REMOTA:** Conectarse a un equipo que ejecute Windows desde otro equipo que ejecute Windows y que esté conectado a la misma red o a Internet. Por ejemplo, puede usar todos los programas, archivos y recursos de red desde su equipo doméstico y estar como si estuviese sentado frente a su equipo del trabajo. (Centro Criptológico Nacional, 2015)
- **FIREWALL:** Elemento de red cuya finalidad es asegurar que solamente las comunicaciones autorizadas son las permitidas a pasar entre redes. Bloquear las comunicaciones no autorizadas y registrarlas. (Centro Criptológico Nacional, 2015)
- **NAVEGADOR:** Programa para recorrer la World Wide Web. Algunos de los más conocidos son Netscape Navigator, Microsoft Explorer, Opera, Neoplanet, entre otros. (Centro Criptológico Nacional, 2015)
- **GOOGLE CHROME:** Es un navegador web desarrollado por Google y compilado con base en varios componentes e infraestructuras de desarrollo de aplicaciones(frameworks) de código abierto, como el motor de renderizado Blink (bifurcación o fork de WebKit). Está disponible gratuitamente bajo condiciones específicas del software privativo o cerrado. El nombre del navegador deriva del término en inglés usado para el marco de la interfaz gráfica de usuario. (Google, 2016)
- **MOZILLA FIREFOX:** Es un navegador web libre y de código abierto8desarrollado para Microsoft Windows, Android, OS X y GNU/Linux coordinado por la Corporación Mozilla y la Fundación Mozilla. Usa el motor Geckopara renderizar páginas web, el cual implementa actuales y futuros estándares web. (Mozilla Foundation US, 2016)
- **OPERA:** Es un navegador web creado por la empresa noruega Opera Software. Usa el motor de renderizado Blink. Tiene versiones para computadoras de escritorio, teléfonos móviles y tabletas. (Opera, 2016)
- **INTERNET EXPLORER:** Microsoft Internet Explorer. Navegador de la empresa Microsoft que, a partir de Windows98, viene integrado al sistema operativo. (Microsoft, 2016)
- **GPO:** Objetos de Directiva de grupo es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. en parte, controla lo que los usuarios pueden y no pueden hacer en un sistema informático. (Centro Criptológico Nacional, 2015)
- **PSI:** Política de Seguridad Informática requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas. (Centro Criptológico Nacional, 2015)
- **LDAP:** Lightweight Directory Access Protocol (en español Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. (Centro Criptológico Nacional, 2015)
- **GFI WEBMONITOR:** Es una solución completa de supervisión del uso de Internet. Se le permite monitorizar y navegación web de filtro y las descargas de archivos en tiempo real. También le permite optimizar el ancho de banda mediante la limitación de acceso a medios de transmisión y otras actividades que consumen ancho de banda, al tiempo que mejora la seguridad de la red con herramientas integradas que escanean el tráfico en busca de virus, troyanos, spyware y material de phishing.

Es la solución ideal para ejercer de forma transparente y sin problemas el control sobre los hábitos de navegación y descarga. Al mismo tiempo, le permite asegurar la responsabilidad legal, iniciativas de mejores prácticas sin alienar a los usuarios de la red. (GFI WebMonitor, 2016)

- **FIREBIRD**: Es un sistema de administración de base de datos relacional (o RDBMS) (Lenguaje consultas: SQL) de código abierto, basado en la versión 6 de Interbase, cuyo código fue liberado por Borland en 2000. Su código fue reescrito de C a C++. (GFI WebMonitor, 2016)

- **WPAD:** (Web Proxy Auto-Discovery protocol) es un método utilizado por los clientes de servidores Proxy para localizar el URI de un archivo de configuración, valiéndose de métodos de descubrimiento a través de DHCP y DNS. (GFI WebMonitor, 2016)

- **SMTP:** Es la sigla que corresponde a la expresión de la lengua inglesa Simple Mail Transfer Protocol. En nuestro idioma, dicho concepto puede traducirse como Protocolo para la Transferencia Simple de Correo. El SMTP es un protocolo de red que se emplea para enviar y recibir correos electrónicos (emails). (GFI WebMonitor, 2016)

- **SSL:** "Secure Sockets Layer". SSL Definición, Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás. (GFI WebMonitor, 2016)

C. MARCO JURIDICO

Con la expedición de la Ley 1273 de 2009, Colombia entró a formar parte de los países que se han reparado con herramientas eficaces para contrarrestar la problemática de los delitos informáticos en todas sus modalidades.

CAPITULO PRIMERO - De las atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- **Artículo 269A:** ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B:** OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C:** INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D:** DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E:** USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269G:** SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. . El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- **Artículo 269H:** CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA. : las penas imponible de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

  1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO SEGUNDO - De los atentados informáticos y otras infracciones.

- **Artículo 269I:** HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

- **Artículo 269J:** TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. la misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

  Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

V. ANÁLISIS Y DISCUSIÓN

A. *PROCEDIMIENTO **"Diagrama de Red Lógico"***

Descripción detallada: topología en estrella, medio de transmisión cableada, UTP Cat6, direccionamiento IP descrito en el mapa, ámbito de la red, cantidad de HOST, servidor DNS, descripción del servidor y las maquinas físicas y virtuales a utilizar en el procedimiento como se muestra en [ilustración 1].

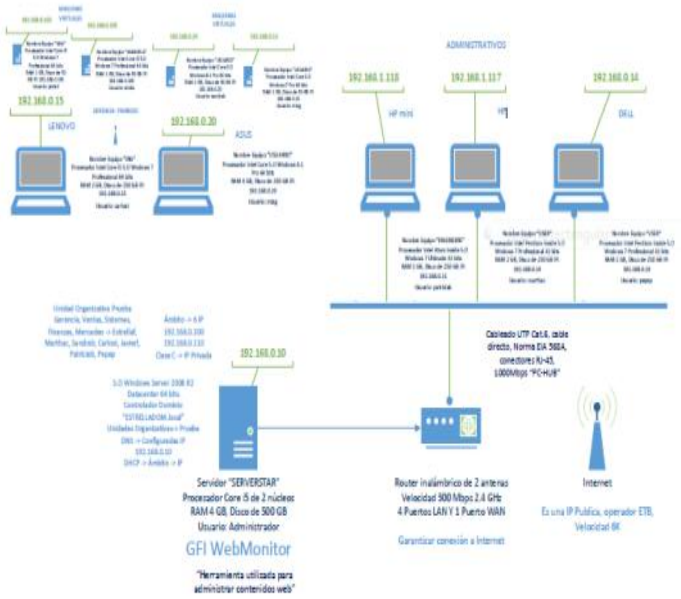

Ilustración 1 Diagrama de Red Lógico

B. *HARDWARE Y SOFTWARE*

Una vez analizados los componentes físicos necesarios a utilizar para este proyecto, se configuraron las máquinas a utilizar: servidor, máquinas físicas y máquinas virtuales.

Se contó con 6 máquinas físicas y 4 máquinas virtuales con las siguientes características:

EQUIPO 01 MAC BOOCK
Servidor: SERVERSTAR
Procesador Intel Core i5 de 2 núcleos 64 bits
RAM 4 GB
Disco 500GB
IP: Dinámica
Se instaló herramienta GFI WebMonitor
S.O. Windows Server 2008 R2 Datacenter
Controlador de Dominio: ESTRELLADOM.local
Unidades organizativas: Prueba
Usuarios creados: 10 Users
DNS: Configuradas IP
DHCP: Ámbito – IP
Usuario: Administrador

EQUIPO 02 HP
Procesador: Intel Pentium Inside 32 bits
RAM 2 GB,
Disco: 250GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Doreila1
Sistema Operativo Windows 7 Professional
Usuario: Marthac

EQUIPO 03 DELL
Procesador: Intel Pentium Inside 32 bits
RAM 2 GB
Disco: 250GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: User
Sistema Operativo Windows 7 Professional
Usuario: Sandrab

EQUIPO 04 HP MINI
Procesador: Intel Atom Inside 32 bits
RAM 1 GB
Disco: 250GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Engineers
Sistema Operativo Windows 7 Ultimate
Usuario: Patriciab

EQUIPO 05 LENOVO
Procesador: Intel Core i5 de 2 núcleos 64 bits
RAM 8 GB
Disco: 500GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Ing
Sistema Operativo Windows 7 Professional
Usuario: Carlost

EQUIPO 06 ASUS
Procesador: Intel Core 64 bits
RAM 4 GB
Disco: 250GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Usuario
Sistema Operativo Windows 8.1 Pro
Usuario: Miag

EQUIPO 07 LENOVO MAQUINA VIRTUAL 1
Procesador: Intel Core i5 de 2 núcleos 64 bits
RAM 1 GB
Disco: 50GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Manuela
Sistema Operativo Windows 7 Professional
Usuario: Javierl

EQUIPO 08 LENOVO MAQUINA VIRTUAL 2
Procesador: Intel Core i5 de 2 núcleos 64 bits
RAM 1 GB
Disco: 50GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Mia
Sistema Operativo Windows 8.1 Pro
Usuario: Ericks

EQUIPO 09 ASUS MAQUINA VIRTUAL 1
Procesador: Intel Core 64 bits
RAM 1 GB
Disco: 50GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Usuario
Sistema Operativo Windows 8.1 Pro
Usuario: Sandrab

EQUIPO 10 ASUS MAQUINA VIRTUAL 2
Procesador: Intel Core 64 bits
RAM 1 GB
Disco: 50GB
IP: Dinámica
Dominio: ESTRELLADOM.local
Nombre del equipo: Usuario
Sistema Operativo Windows 7 Professional
Usuario: Miag

*C. PROCEDIMIENTO **"Creación del dominio"***

Se requiere un sistema operativo Windows Server para el proceso de instalación del controlador del dominio por lo que se instala el Windows Server 2008 r2. Para mayor seguridad se recomienda establecer una contraseña compleja pero que se pueda recordar. [5,6].

Sistema operativo Windows Server 2008 r2 instalado por completo como se muestra en [ilustración 2].

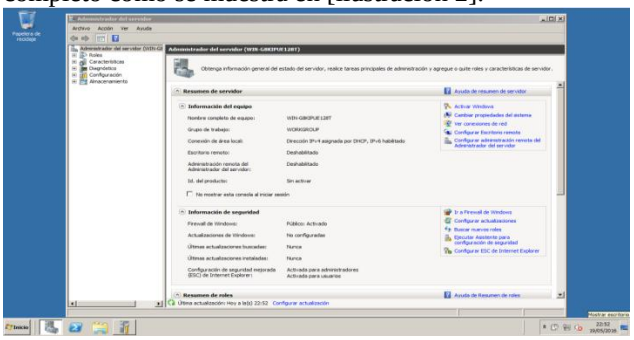

Ilustración 2 S.O. Windows Server 2008 R2

Se asegura que la hora y fecha sea la correcta; se le cambia el nombre al equipo y se reinicia para aplicar cambios como se muestra en [ilustración 3].

Ilustración 3 Configuración de fecha y hora.

Se le asigna un nombre de equipo; se le cambia la opción grupo de trabajo por dominio como se muestra en [ilustración 4].

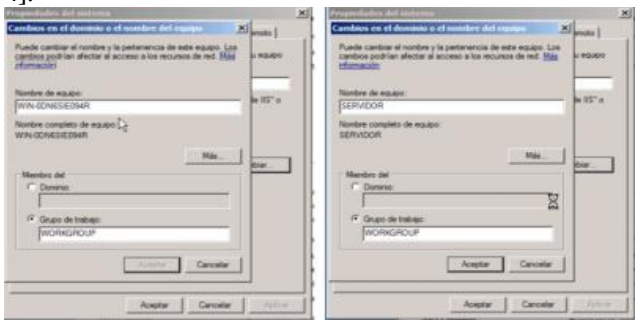

Ilustración 4 Asignación nombre de equipo

Antes de iniciar el proceso de la creación del controlador del dominio se debe configurar la red, para eso se debe ingresar, manualmente, una dirección IP fija y agregar el DNS como se muestra en [ilustración 5].

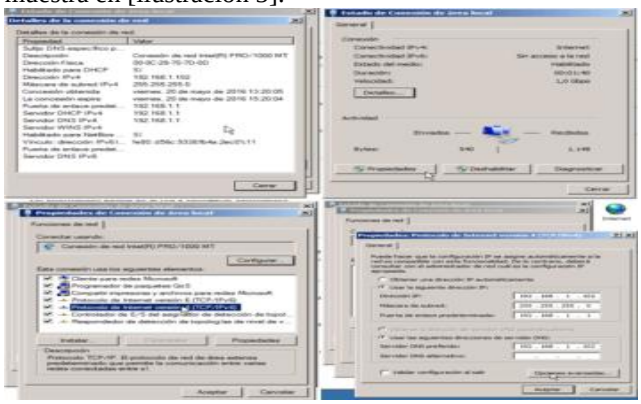

Ilustración 5 Configuración de la Red

Con la hora, fecha y la configuración de una dirección IP estática se procede a la instalación del Controlador de Dominio ejecutando el comando "dcpromo", mediante un asistente de instalación se añadirá el Rol de Servicios de dominio de Active Directory donde se creó un nuevo dominio en un bosque nuevo, también se nombró el dominio y se agregó el Rol Servidor DNS. Se reinicia para aplicar cambios como se muestra en [ilustración 6].

Ilustración 6 Instalación Controlador de Dominio

Ya teniendo instalado el controlador del dominio, se accede al dominio como administrador y se creó usuarios mediante la Herramienta administrativa: Usuarios y Equipos de Active Directory; y para mantener un orden se crean las Unidades Organizativas como se muestra en [ilustración 7].

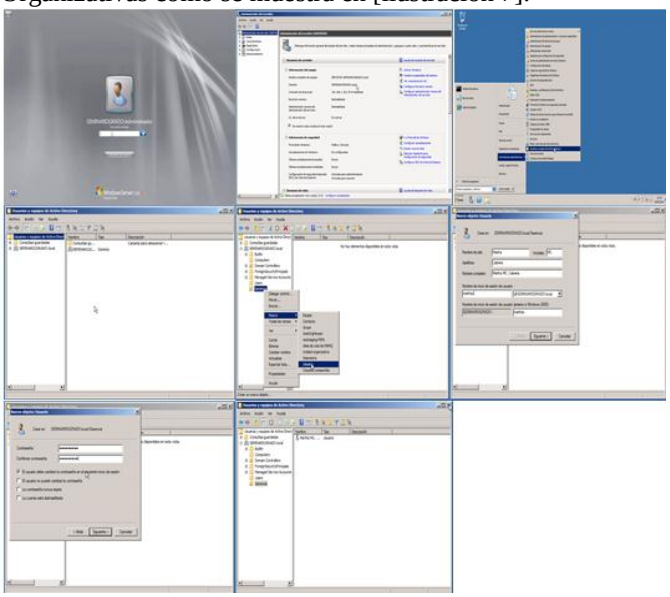

Ilustración 7 Creación de Unidades Organizativas

*D. PROCEDIMIENTO **"Instalación GFI WebMonitor"***

Para la implementación de la herramienta GFI WebMonitor se descarga la versión de prueba de 30 días y se procede con la instalación. La herramienta se encarga de la instalación de los componentes requeridos. [6,7]

Prerrequisitos de instalación de la herramienta GFI WebMonitor, como se muestra en [ilustración 8].

Ilustración 8 Requisitos de Instalación de la herramienta

Como todo software, existen unos términos legales establecidos por aceptar como se muestra en [ilustración 9].

Ilustración 9 Términos legales

Después de aceptados los términos se debe indicar quién podrá acceder a la interfaz del software, quién lo va administrar, para eso se debe ingresar la dirección IP del computador al que se le concederá el permiso. Esto también se puede hacer de la forma DOMINIO/usuario. La dirección IP actual del computador donde se está ejecutando la instalación ya está ingresada como se muestra en [ilustración 10].

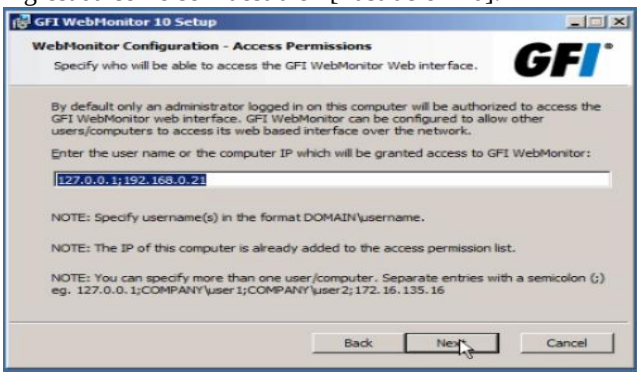

Ilustración 10 Configuración de administración

Se establecen las rutas donde se instalará el programa y se espera a la finalización de la instalación como se muestra en [ilustración 11].

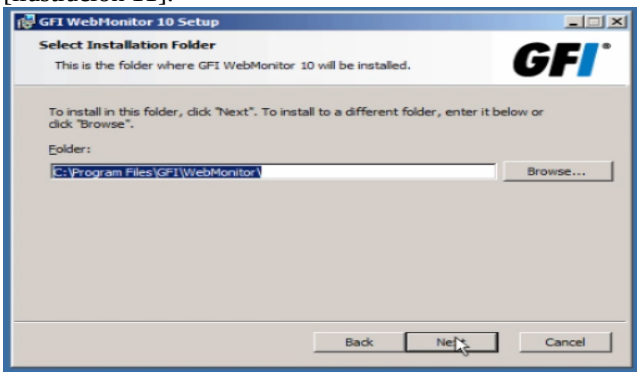

Ilustración 11 Ruta de instalación de la herramienta

Finaliza el proceso de instalación de la herramienta GFI WebMonitor como se muestra en [ilustración 12].

Ilustración 12 Finalización de la instalación

Se ejecutó el programa y su interfaz se inicia en el navegador que se tenga predeterminado mediante la dirección loopback 127.0.0.1 por el puerto 1007 como se muestra en [ilustración 13].

Ilustración 13 Inicialización de la herramienta

Cuando se inicia por primera vez, el GFI WebMonitor asistirá en la configuración mediante una interfaz amigable que permite una mejor interacción entre la herramienta y el usuario que lleva a cabo la instalación como se muestra en [ilustración 14].

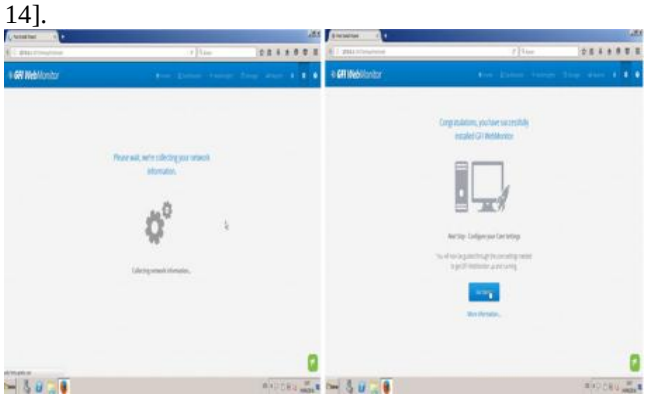

Ilustración 14 Configuración inicial de la herramienta

El primer paso para la configuración es seleccionar el modo en el que la herramienta va a operar: Modo Proxy Simple y Modo Gateway; para la realización de este proyecto se utiliza el Modo Proxy Simple ya que el Modo Gateway requiere de dos tarjetas de red como se muestra en [ilustración 15].

Ilustración 15 Configuración Modo Proxy Simple

Para la autenticación Proxy se tienen dos opciones, la Autenticación básica y la autenticación integrada, la primera permite ingresar las credenciales del usuario final cada vez que quiera utilizar un navegador, la segunda es utilizar las credenciales otorgadas al inicio de sesión. Se recomienda la segunda opción para evitar dar credenciales por la red. Para el proyecto se utiliza la primera opción para ejecutar pruebas en los distintos navegadores. También se encuentra la opción de ingresar determinada dirección IP o un rango de IP para evitar esta autenticación como se muestra en [ilustración 16].

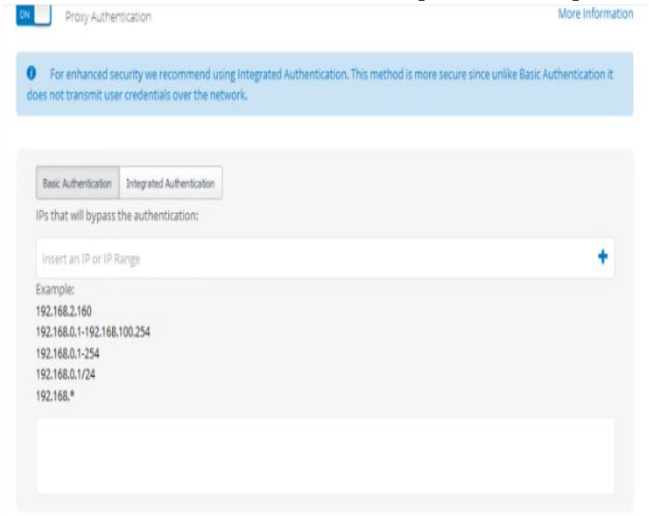

Ilustración 16 Configuración de Autenticación básica

El siguiente paso dentro de la configuración de la herramienta es habilitar el Proxy Transparente, el cual sólo se encuentra disponible si en el paso anterior el Modo Gateway fue seleccionado como se muestra en [ilustración 17]

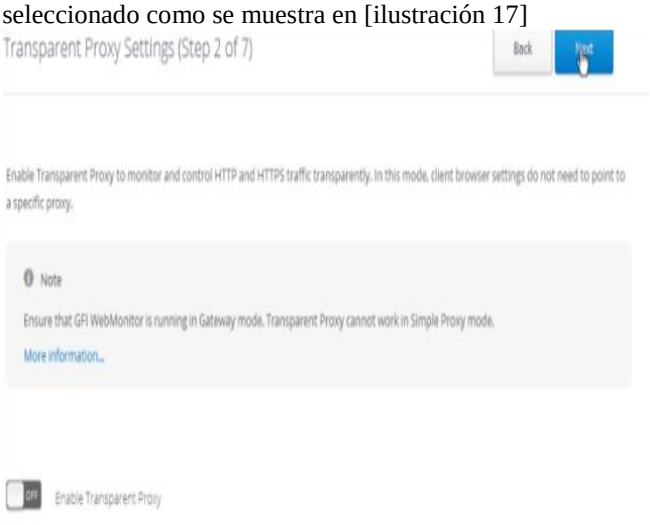

Ilustración 17 Habilitar Proxy Transparente

Siendo una versión de Prueba, la empresa otorga una licencia de 30 días al momento de descargar el instalador, si se tiene una licencia paga se ingresa en este paso, de lo contrario aparecerá la dada para versión trial como se muestra en [ilustración 18].

Ilustración 18 Licencia 30 días, versión de prueba

Para el escaneo del protocolo HTTPS se encuentra opción se importar certificados ya que la herramienta no lee o muestra contenidos encriptados como se muestra en [ilustración 19].

Ilustración 19 Escaneo del protocolo HTTPS

Uno de los requerimientos de la herramienta es SQL Server para controlar las bases de datos. Para la versión de prueba, GFI WebMonitor cuenta con un sistema de administración de base de datos integrado llamado Firebird que se recomienda cambiar una vez comprada la licencia como se muestra en [ilustración 20].

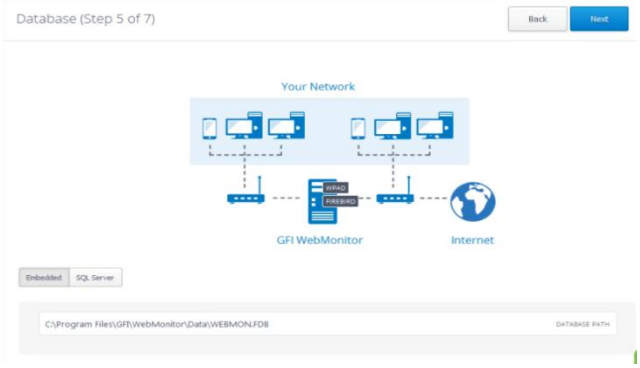

Ilustración 20 Base de Datos del programa "Firebird"

Se ingresa las credenciales del administrador del servidor que controlará la herramienta como se muestra en [ilustración 21].

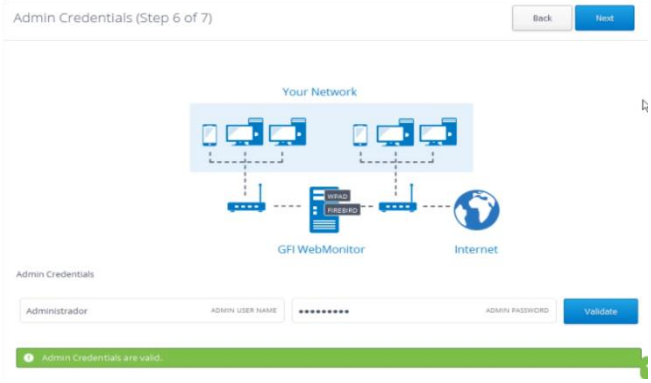

Ilustración 21 Ingreso credenciales administrador

Para finalizar se debe configurar los detalles del servidor de correo electrónico que se utilizará para las notificaciones que surjan durante el uso del programa como se muestra en [ilustración 22].

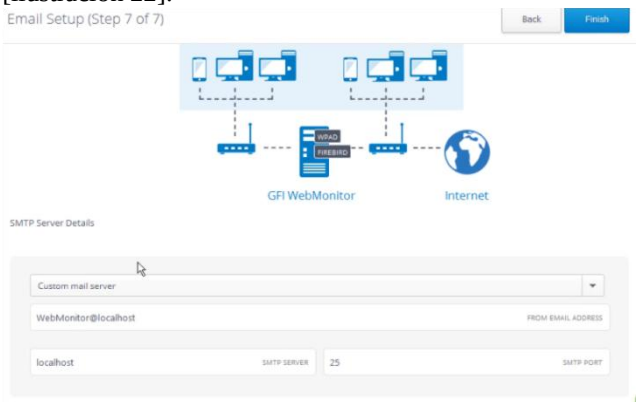

Ilustración 22 Configuración servidor de e-mail

Finalizada la configuración el GFI WebMonitor está listo para utilizarse mostrando su pantalla de Inicio donde hay un resumen del uso del contenido web de los empleados, el acceso a sitios con malware y el consumo de ancho de banda como se muestra en [ilustración 23].

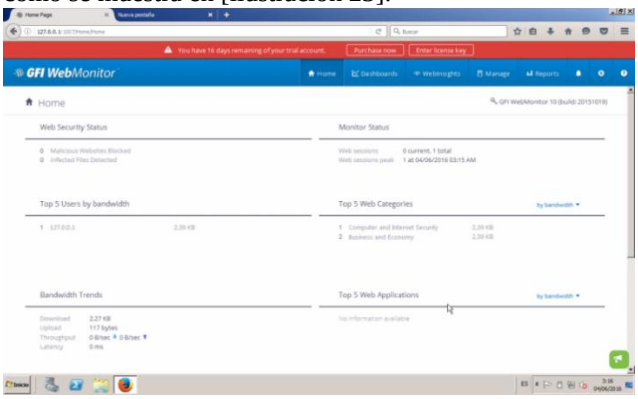

Ilustración 23 Vista inicial de la herramienta

VI. CONCLUSIONES

Por medio de los reportes generados en la herramienta GFI WebMonitor no sólo se puede recopilar información del contenido web visitado en un periodo de tiempo establecido, ya sea diario o mensual, sino que se recogen estadísticas de las infecciones evitadas y de los malware bloqueados; permitiendo así demostrar que los peligros cibernéticos a los que se enfrenta una empresa son reales y que está expuesta a cualquier ataque por medio de sus empleados que involuntariamente permiten estos riesgos penetrar la seguridad de dicha empresa.

Con la instalación de la herramienta GFI WebMonitor, se crearon y se aplicaron las políticas de seguridad establecidas por la alta dirección, administrando el uso de contenido web para los navegadores Opera, Google Chrome, Mozilla Firefox, Safari e Internet Explorer.

Gracias al GFI WebMonitor se logró limitar el consumo de ancho de banda de una red empresarial para mejorar el desempeño de los empleados. De igual forma se logró establecer periodos recreativos en los que el empleado puede revisar sus redes sociales y aun permitiendo al administrador de red controlar la seguridad dentro del contenido web y las descargas realizadas.

Para evitar problemas legales, se estableció la política de prohibir las descargas de instaladores para controlar la distribución de software pirata; así mismo se bloquean los sitios web de pornografía ya que no forma parte de las labores de la empresa y puede infringir alguna ley si es pornografía infantil.

VII. REFERENCIAS

[1] Una de cada dos empresas colombianas fue hackeada en el 2015 (Revista Semana, 2016).
http://www.semana.com/tecnologia/articulo/cibercrimen-en-colombia-una-de-cada-dos-empresas-fue-hackeada/474110

[2] Corporation Intel Security McAfee Web Gateway (Corporativo Intel Security, 2016)
http://www.mcafee.com/es/products/web-gateway.aspx#overview

[3] Symantec Corporation US Symantec Web Gateway (Symantec Corporation US, 2016)
https://www.symantec.com/es/mx/web-gateway/

[4] Ubuntu Documentation (Community Ubuntu, 2016)
https://help.ubuntu.com/community/DansGuardian

[5] Delta asesores de servicios e información (DELTA Asesores, 2015)
http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

[6] Guía de instalación GFI WebMonitor (GFI WebMonitor, 2016)
http://www.gfi.com/webmon/webmon_installation_guide_es.pdf

[7] VMware (VMware, Inc, 2016)
http://www.vmware.com/co

[8] Google (Google, 2016)
https://www.google.es/chrome/browser/desktop/

[9] Mozilla Firefox (Mozilla Foundation US, 2016)
https://www.mozilla.org/es-ES/firefox/products/

[10] Opera (Opera, 2016)
http://www.opera.com/es-419

[11] Microsoft (Microsoft, 2016)
http://windows.microsoft.com/es-es/internet-explorer/download-ie

[12] Youtube (Youtube, 2013)
https://www.youtube.com/watch?v=xz12tcTdk_4

[13] Prezi (Prezi, 2016)
http://prezi.com/3xa4a7d2mzoj/?utm_campaign=share&utm_medium=copy&rc=ex0share

[14] Aprende Informatica Conmigo (Oscar Abad Folgueira y Dinapyme, 2016)
aprendeinformaticaconmigo.com

[15] GFI WebMonitor (GFI WebMonitor, 2015)
http://www.gfihispana.com/pages/gfiwebmonitor2015-how-modify-the-whitelist-and-the-blacklist.asp?adv=29089&loc=104&wemail=nejihina@hotmail.com&utm_medium=email&utm_campaign=webmon_in-trial_no-call-home_es&utm_source=marketing-automation&utm_content=sl_transact_html_01&utm_term=body_how-to-modify-the-whitelist-and-the-blacklist

[16] GFI WebMonitor (GFI WebMonitor, 2015)
http://www.gfihispana.com/pages/gfiwebmonitor2015-how-to-enable-authentication-and-reporting.asp?adv=29089&loc=105&wemail=nejihina@hotmail.com&utm_medium=email&utm_campaign=webmon_in-trial_no-call-home_es&utm_source=marketing-automation&utm_content=sl_transact_html_01&utm_term=body_how-to-enable-authentication-and-reporting

[17] Youtube (Youtube, 2015)
https://www.youtube.com/watch?v=rMLa3rx1SFQ

[18] GFI WebMonitor (GFI WebMonitor, 2015)
http://www.gfi.com/webmon/webmon_installation_guide_es.pdf#page=13&zoom=auto,51,305.64

[19] SquidGuard (SquidGuard, 2007)
http://www.squidguard.org

[20] Google Drive (Google Drive, 2015)

https://drive.google.com/folderview?id=0B1elNDlnGsHyQnBRUW56SEl2NnM&usp=sharing_eid&ts=57571257

[21] CCM Servidores Proxy (CCM, 2016) http://es.ccm.net/contents/297-servidores-proxy-y-servidores-de-proxy-inversos

[22] Johnson, A. D., Handsaker, R. E., Pulit, S. L., Nizzari, M. M., O'Donnell, C. J., & De Bakker, P. I. (2008). SNAP: a web-based tool for identification and annotation of proxy SNPs using HapMap. Bioinformatics, 24(24), 2938-2939. http://scholar.google.com.co/scholar_url?url=https%3A%2F%2Fbioinformatics.oxfordjournals.org%2Fcontent%2F24%2F24%2F2938.full&hl=es&sa=T&oi=ggp&ct=res&cd=0&ei=1L1XV8v7B8aUmAHz_7WwBA&scisig=AAGBfm3axMQhlsVkk8cgpzAPNYOXkPK09g&nossl=1&ws=849x592

[23] Wu, K. L., & Philip, S. Y. (2003). Replication for load balancing and hot-spot relief on proxy web caches with hash routing. Distributed and Parallel Databases, 13(2), 203-220. http://link.springer.com/article/10.1023/A:1021519509203#page-1

[24] Wu, K. L., & Yu, P. S. (1999, November). Local replication for proxy web caches with hash routing. In Proceedings of the eighth international conference on Information and knowledge management (pp. 69-76). ACM. http://dl.acm.org/citation.cfm?id=319959

[25] ACM Digital Library (ACM Digital Library, 2016) http://dl.acm.org/citation.cfm?id=319959