

**SISTEMA PARA EL CONTROL DE TRAZAS DE UN SERVIDOR PROXY
(SCTRAZAS)**
**SYSTEM FOR THE CONTROL OF TRACES OF A PROXY SERVER
(SCTRAZAS)**

Autores: Ing. Yoel Benedico Aguilera
MSc. Yankier Crespo González

Institución: Universidad de Ciego de Ávila Máximo Gómez Báez

Correo electrónico: ybaquilera@unica.cu

RESUMEN

En la presente investigación se realizó una revisión acerca de como gestionar y visualizar las trazas generadas por el acceso a los servicios de redes, de manera que permita detectar el acceso no autorizado a alguno de los servicios o el uso indebido de las tecnologías por parte de los usuarios de la Universidad de Ciego de Ávila Máximo Gómez Báez (UNICA), además de una valoración de la situación de las herramientas informáticas utilizadas hasta ese momento para el control de dicho proceso, permitiendo demostrar las limitaciones existentes. Por esta razón, se plantea como objetivo desarrollar un sistema informático que permita visualizar las trazas de navegación a través del proxy de la UNICA, generar informes sobre el uso de este servicio, además de alertar a los administradores y responsables de seguridad informática al detectar irregularidades en el uso de este servicio, a través de una aplicación Web implementada en el entorno de desarrollo NetBeans y el Framework Play, utilizando Java como lenguaje de programación, MySQL como servidor para la base de datos, y RUP (Proceso Unificado de Rational) como metodología de desarrollo de software.

Palabras clave: Trazas, Proxy, Control, Software.

ABSTRACT

In the present investigation, a review was carried out on the management and visualization of the traces generated by the access to the network services, so as to detect unauthorized access to some of the services or the improper use of

the technologies by the Users of the University of Ciego de Ávila Máximo Gómez Báez (UNICA), as well as an assessment of the situation of the computer tools used up to that moment to control this process, allowing to demonstrate the existing limitations. For this reason, it aims to develop a computer system that allows visualizing the navigation traces through the UNICA proxy, generating reports on the use of this service, as well as alerting administrators and IT security officers when detecting irregularities In the use of this service, through a Web application implemented in the NetBeans development environment and the Framework Play, using Java as programming language, MySQL as server for the database, and Rational Unified Process (RUP) as Software development methodology.

Keywords: Proxy, Control, Traces, Software.

INTRODUCCIÓN

En la actualidad, con el avance de las Tecnologías de la Información y las Comunicaciones (TIC), es común que en la mayoría de los centros de trabajo educacionales existan al menos una conexión a la Red de Redes, porque se ha convertido en uno de los mayores exponentes de la comunicación a nivel mundial. A través de esta, los usuarios pueden acceder a toda la información ofrecida por una gran cantidad de servidores distribuidos por todo el mundo. La información se encuentra distribuida en una amplia variedad de contenidos que abarcan desde un simple texto hasta gráficos y multimedia. Además, ha propiciado el surgimiento de nuevos estilos de trabajo al acortar las distancias entre los involucrados.

En Cuba, este último año ha sido el de mayores avances en este sentido, logrando que gran parte de la sociedad tenga la posibilidad de acceder a internet desde una cantidad en ascenso de puntos WIFI. En los centros Universitarios adscritos al MES y en particular en la Universidad de Ciego de Ávila Máximo Gómez Báez también es palpable este avance, logrando un incremento de ancho de banda de un 70 % aproximadamente, pero su uso irracional e inadecuado puede hacer que no sea suficiente e impedir que los usuarios puedan desarrollar sus trabajos científicos a plenitud. Por este motivo resulta necesario controlar el acceso a la red, para lograr un uso adecuado del

ancho de banda, uno de los métodos para lograrlo es implementando la navegación a través de un servidor proxy.

El proxy permite establecer gran cantidad de reglas que restringen el uso de este servicio a conveniencia de los centros y posibilita el almacenamiento de los registros de la navegación.

Entre los mayores generadores de registros se encuentran algunos servicios, tales como: servidor HTTP, correo electrónico, DNS y FTP, almacenando estos registros en archivos conocidos como logs.

En nuestras universidades el acceso a los servicios de redes es normalizado por resoluciones y normativas, tanto ministeriales como rectorales. Cada persona tiene un nivel de acceso o privilegios según estas normas y solo puede acceder a los servicios que le son aprobados. Es de vital importancia la necesidad de gestionar y visualizar las trazas generadas por los mismos, de manera que permita detectar el acceso no autorizado a alguno de los servicios, o el uso indebido de este servicio por parte de los usuarios.

Antecedentes históricos del proceso de control de trazas

Existen muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP o *Simple Mail Transfer Protocol*), la transmisión de archivos (FTP y P2P o *peer-to-peer*), las conversaciones en línea (IRC o *Internet Relay Chat*), la mensajería instantánea, la transmisión de contenido y comunicación multimedia telefonía (VoIP o *Voice Over Internet Protocol*), televisión (IPTV o *Internet Protocol Television*), los boletines electrónicos (NNTP o *Network News Transport Protocol*), el acceso remoto a otros dispositivos (SSH o *Secure Shell* y Telnet *TELEcommunication NETwork*) o los juegos en línea. (Castells, 1999).

Inicialmente la red de redes tenía un objetivo claro. Se navegaba para algo muy concreto: búsquedas de información. Ahora quizás también, pero sin duda es más probable perderse en la red debido al inmenso abanico de posibilidades que esta brinda. Este exceso de posibilidades puede convertirse en un problema para las empresas u organizaciones que no cuentan con un ancho de banda acorde a la cantidad de usuarios que hacen uso de este servicio. Además de los centros que establecen políticas de navegación para restringir

el acceso solo a las informaciones de interés para mantener el ambiente corporativo.

Es así que se usan las distintas herramientas que restringen estos accesos y otras que permiten gestionar la información que brindan las trazas o *logs* de navegación de cada uno de los usuarios para luego analizarlos y descubrir las posibles violaciones a las políticas establecidas.

Se considera que el proceso de gestión de la información es el cumulo de actividades en una organización donde la información como recurso se debe recopilar, controlar, manipular y arrojar algún resultado final para dicha actividad y además, contribuya a cumplir con los objetivos generales de la misma.

El control es un elemento fundamental dentro de la gestión, su concepto puede ser muy general y puede ser utilizado en el contexto organizacional para evaluar el desempeño general frente a un plan estratégico.

Mario Gutiérrez utiliza los siguientes conceptos dados por autores estudiosos del tema:

Según Stephen Robbin el control puede definirse como el proceso de regular actividades que aseguren que se están cumpliendo como fueron planificadas y corrigiendo cualquier desviación significativa.

Sin embargo, James Stoner lo define de la siguiente manera: el control administrativo es el proceso que permite garantizar que las actividades reales se ajusten a las actividades proyectadas. Mientras que, para Henry Fayol, citado por Ramón Melinkoff, el control consiste en verificar si todo se realiza conforme al programa adoptado, a las órdenes impartidas y a los principios administrativos. Tiene la finalidad de señalar las faltas y los errores a fin de que se puedan reparar y evitar su repetición. (Gutiérrez, 2007).

Al analizar todas las definiciones se nota que el control posee ciertos elementos que son básicos o esenciales por lo que se puede concluir diciendo que es la función que permite la supervisión y comparación de los resultados obtenidos contra los resultados esperados originalmente, asegurando además que la acción dirigida se esté llevando a cabo de acuerdo con los planes de la organización y dentro de los límites de la estructura organizacional.

En cuanto a los tipos de control, Stephen Franklin y George Terry afirman que «existen 3 tipos de control que son: el control preliminar, el concurrente y el de retroalimentación».

El control debe llevarse en cualquier nivel del sistema, garantizando de esta forma que en la misma se cumplan los objetivos. Pero hay que aclarar que este no solo debe hacerse al final del proceso, sino que, por el contrario, debe ser realizado conjuntamente al llevarse a cabo las tareas para que de esta forma se solucionen de manera más eficaz y en el menor tiempo posible todos los errores o problemas que se presenten. (Terry, 1999).

Un sistema de control está definido como un conjunto de componentes que pueden regular su propia conducta o la de otro sistema con el fin de lograr un funcionamiento predeterminado, de modo que se reduzcan las probabilidades de fallos y se obtengan los resultados buscados. Aplicando técnicas como estudios de tiempos y movimientos, inspecciones, programación lineal, análisis estadísticos y gráficas.

Un sistema de control del tráfico de trazas es una herramienta utilizada para el control, planeamiento y monitoreo de las trazas que alojan los servicios. Está orientado a facilitar y automatizar varias de las tareas de control sobre los datos que fluyen. Una herramienta de este tipo permite analizar trazas, emitir estadísticas sobre el uso de servicios específicos, cantidad de tráfico y gestión de reportes. (Quiñones, 2011).

Los autores consideran que el proceso de control de trazas son las actividades que se llevan a cabo para identificar los datos necesarios, procesarlos, manipularlos y mostrarlos de forma organizada y eficiente, necesaria para el conocimiento y toma de decisiones del personal que realiza estas actividades. Todo esto permite lograr un mejor uso de la red, contribuyendo a cumplir con los objetivos generales de las instituciones.

Sistemas de análisis de registro de servidores proxy a nivel mundial

En la actualidad existen muchos sistemas que permiten analizar los registros de servidores proxy con variadas funcionalidades. Algunos de ellos permiten mostrar los datos estadísticos en forma de tabla o gráfico, lo que hace que sea

más sencillo y elegante observar las estadísticas del servidor proxy, entre estos sistemas se encuentran:

1. WebSpy Analyzer Giga: Es una herramienta de análisis para monitorear el uso de Internet. Esta herramienta permite una organización lógica de los datos usando alias y perfiles configurables. Importa las bitácoras generadas por los servidores de Proxy o firewalls de las empresas. Incluye tareas pre-programadas para «establecer y olvidar» análisis de datos. Utiliza los recursos de red existentes tal como Windows NT® User Groups. Además analiza de manera eficientemente gran cúmulo de datos. También genera una variedad de informes personalizables en formatos comunes.
2. Webalizer: Es una herramienta gratuita de análisis de archivos de registro que genera resúmenes de utilización muy detallados acerca de servidores Web y FTP en formato gráfico y tabular de fácil comprensión. Los registros son un resumen estadístico del tráfico de usuarios en su servidor. Los informes de Webalizer se generan en horarios programados de acuerdo con las opciones de configuración que usted estableció para el sitio al momento de crearlo. (Webalizer, s.f.).
3. AWStats (Advanced Web Statistics o Estadística Web Avanzada): Es una herramienta de análisis open source escrita en Perl, que permite parsear *logs* de un servidor web, ftp o de correo y generar estadísticas en forma de reportes HTML. Puede ejecutarse desde un navegador web o desde la línea de comandos y funciona sobre diversos sistemas operativos.

Un análisis del registro completo permite mostrarles la siguiente información: el número de visitas y de visitantes únicos y la duración de las visitas, los usuarios autenticados y últimas visitas autenticadas, las páginas más vistas, los navegadores utilizados (páginas, hits, kb para cada navegador), OS utilizado (páginas, hits, KB para cada sistema operativo), los motores de búsqueda, frases y palabras clave utilizadas para encontrar su sitio y los errores HTTP (Página no encontrada con el último árbitro, etc.). (Sawstats, s.f.).

4. Squid Analysis Report Generator (Sarg): Es una herramienta que permite conocer, toda la actividad de los usuarios y/o equipos incluidos en la red, registrada en los *logs* del proxy. Fue desarrollada con el lenguaje de programación C y es distribuida bajo la licencia GPL v2. Provee mucha información sobre las actividades de los usuarios de Squid: tiempo, bytes, sitios y otros. Este analizador brinda una variedad de información como: listados de sitios más visitados, reportes diarios, semanales y mensuales, gráficos semanales y mensuales del consumo por usuario/host, detalles de todos los sitios a los que entró un usuario/host y descargas.
5. WebTrends Log Analyzer: Programa que permite a los administradores de páginas Web optimizar una o varias páginas Web sabiendo la máxima información posible sobre los gustos de los usuarios. (Webtrends Log Analyzer, s.f.).

Sistemas de análisis de registro de servidores proxy a nivel nacional.

En Cuba no hay muchos sistemas dedicados al análisis de registros de servidores proxy, las que existen se desarrollaron por la necesidad de algunas instituciones de controlar la navegación por Internet ya que los *softwares* existentes en el mercado internacional no resolvían sus necesidades y vieron en sí la capacidad de elaborar sus propios analizadores de log. Aquí se muestran algunos de esos sistemas desarrollados por algunas instituciones del país:

1. AiresProxy es un indagador de ficheros de *logs* que brinda a los usuarios la información referente a sus registros de navegación en forma de reportes. Posee un motor de segmentación de registros, otro de mantenimiento a la base de datos y por último un módulo de análisis y presentación de datos. Además, posibilita actualizar la cuota de navegación de los usuarios en caso de que la institución establezca cuotas para acceder a redes externas. Posee un programa de mantenimiento auxiliar encargado de eliminar de la base de datos los registros que no son de interés del usuario o los administradores de red.

Es una herramienta muy versátil gracias al elevado poder de configuración mediante ficheros XML.

Dentro de la información que brinda se puede encontrar: reporte por dominios, reporte de dominio por dirección IP9, reporte de dominio por fecha, reporte por dirección IP, reporte por fecha y reporte por URL. (Chavez, 2011).

2. ISAWeb: es un producto realizado en el Instituto Central de Investigación Digital (ICID), el cual le permite a un usuario autenticado poder filtrar información relevante sobre el acceso de Internet. Además, genera una variedad de reportes y posee filtros para la búsqueda de información. La aplicación valida las credenciales entradas por el usuario contra el servidor Active Directory del dominio, mediante el protocolo LDAP. La información de tráfico de Internet se extrae del servidor de Internet Isa Server, transformando los ficheros donde se almacenan las trazas de la navegación, a una base de datos en SQL Server. (Palenzuela, ISAWEB. Monitoreo de Tráfico en Internet, 2006).
3. AAInternet: Aplicación realizada por Segurmática, la cual permite extraer información de los ficheros *log* de los servidores proxy, generar reportes gráficos de análisis de la navegación de los usuarios, donde pueden observarse la fecha y hora de visita al sitio, los dominios o sitios Web visitados y la transferencia por usuarios, entre otros datos. Funciona sobre el sistema operativo *Windows*. Utiliza una base de datos creada a partir del procesamiento de archivos *log* del servidor proxy, para ello es necesario copiar manualmente hacia la estación donde está instalada esta herramienta los archivos *log* que se deseen parsear o a una estación dentro de la red donde sean accesibles estos archivos desde la estación donde se encuentra instalado AAInternet.
4. SRNI: El Sistema de Reportes de la Navegación por Internet (SRNI) es una aplicación web realizada en UCI, desarrollada bajo la tecnología Java y que utiliza como gestor de base de datos *PostgreSQL*. Debido a que es una aplicación web puede consultarse desde cualquier lugar de la UCI. El *software* brinda a los usuarios reportes dinámicos de su navegación, los cuales son creados a partir de las trazas del servidor

proxy. La información de acceso que se puede consultar es por URL, dirección IP, días y horas. (Martín Álvarez & García Martínez, 2007).

Luego de analizar cada una de las herramientas y soluciones existentes, ninguna satisface las necesidades que plantea la institución por las siguientes condiciones: las herramientas que son propietarias (*WebTrends Log Analyzer*) o funcionan sobre el sistema operativo *windows* (*WebSpy Analyzer Giga*, *AAInternet*) no se tendrán en cuenta para darle solución al problema por ser herramientas privativas o funcionar sobre un OS (*Operative System*) propietario, y la institución está enfrascada en el desarrollo y uso de *software* libre. Las que son libre (*AWStats*, *Squid Analysis Report Generator* y *Webalizer*) no son sistemas web y no están orientado a usuarios. Estos sistemas son adecuados para llevar estadísticas generales para empresas e instituciones, para llevar el monitoreo de sitios en específicos, sin embargo, no es funcional para mostrar informaciones de los usuarios durante su navegación. Las herramientas nacionales AiresProxy, ISAWeb y SRNI no permiten generar informes personalizados ni realizar estadísticas y se enfocan solamente en los usuarios. Debido a lo antes expuesto no se utilizará ninguna aplicación existente, pero si se tendrán en cuenta algunas de sus funcionalidades y se procede a la creación de un nuevo sistema para analizar los *logs* del proxy Squid.

Universidad de Ciego de Ávila Máximo Gómez Báez (UNICA)

La UNICA, ubicada en la provincia de Ciego de Ávila tiene como misión consagrar sus esfuerzos en formar profesionales integrales desde las dimensiones académica, científica, medio ambiental y humanista que preserva, desarrolla y promueve la cultura con plena integración al entorno económico, político y social avileño, contribuyendo a la elevación de la eficiencia económica organizacional y el desarrollo social y local, con prioridad en la producción de alimentos, el desarrollo del turismo, el uso racional de la energía, el agua, las construcciones, la educación, las ciencias sociales y la informatización de la sociedad, a través de la formación de pregrado, el posgrado, las investigaciones y la extensión universitaria, con profesores,

investigadores y trabajadores comprometidos y preparados, en correspondencia con la política trazada por el Partido Comunista de Cuba y el Gobierno.

La misma está constituida por un conjunto de departamentos y facultades, donde resalta la labor desempeñada por el Departamento de Redes e Informatización, en el cual se brindan un conjunto de servicios informáticos, tales como servicios especializados del nodo, generales de la red UNICA y del DGIC: Dentro de los especializados del nodo está el acceso a Internet, controlar este acceso es de suma importancia, debido a la amplia documentación dañina que existe en la red, para ello cada usuario tiene una cuenta con un privilegio de acceso, según su categoría docente, año que cursa o si pertenece a un grupo de científico. Cada vez que un usuario utiliza este servicio se genera una traza, que posee la fecha, sitio al que accedió, de donde realizó el acceso y el tamaño. Analizar esta traza resulta eficiente para la universidad para tomar decisiones en cuanto al uso de la navegación internacional, pero también es importante para los usuarios poder controlar su navegación sin tener que solicitar al Especialista de Seguridad Informática el listado de sus accesos a la navegación nacional o internacional.

Para realizar el control de las trazas del proxy en la universidad se usa la herramienta Sawmill. Esta herramienta es fácil de usar, tiene una documentación completa, genera reportes y gráficos en vivo y utiliza diversos gestores de base de datos. Pero es una herramienta privativa, solo se puede utilizar en una pc, se demora demasiado tiempo en el análisis de ficheros grandes y muchas veces solo analiza un por ciento del total de la información, presenta problemas con los filtrados de las trazas una vez analizadas.

Para el usuario poder llevar un control de su navegación, debe acercarse al Especialista de la Seguridad Informática y hacerle una solicitud de sus trazas. Luego el especialista le entregara un listado con todas las direcciones a las que accedió la semana pasada o las anteriores a estas. Si el usuario sospecha que existe algún uso descontrolado de su cuota o piensa que existe un robo de su contraseña debe informárselo al especialista, entonces el procederá a investigar el incidente.

A partir de ese momento surge una nueva propuesta que le facilitará el trabajo al especialista, permitiéndole obtener con un día de diferencia cada una de las trazas que se conciban y generar cada uno de los reportes de forma automática y mostrar las estadísticas de forma web. Además de que los usuarios podrán ver donde acceden, la hora y la fecha que se realizó dicha vista, por lo que podrán controlar su cuota y si ocurriera algún uso no autorizado de su cuota poder indicárselo al especialista y él tomará las medidas pertinentes.

Estas han sido sugerencias por parte de los usuarios, corroboradas a través de entrevistas. Tales entrevistas se realizaron con el objetivo de conocer sobre el nivel de automatización de la entidad, además de investigar acerca de los procedimientos en caso de violaciones a la seguridad informática.

Los entrevistados manifestaron que la precisión y rapidez en el manejo de la información han sido factores que han atentado contra la toma de decisiones y que la información necesaria no se encuentra disponible. La solución para estos problemas sería un software automatizado de dirección, con el auxilio de las nuevas tecnologías, que cumpliera con las exigencias demandadas por trabajadores y dirigentes de la institución y supla las limitaciones de los sistemas existentes.

Herramientas utilizadas para el desarrollo del sistema

1. RUP: El Proceso Racional Unificado es un proceso de desarrollo de *software* y junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

La metodología posee ciertas ventajas y desventajas. Algunas de las ventajas son que es el proceso de desarrollo más general de los existentes actualmente y es una forma disciplinada de asignar tareas y responsabilidades en una empresa de desarrollo (quién hace qué, cuándo y cómo). Entre sus desventajas se encuentran que es un método pesado, por el grado de complejidad puede ser no muy adecuado y en proyectos pequeños, es posible que no se puedan cubrir los costos de dedicación del equipo de profesionales necesarios.

2. Java: Es un lenguaje de programación de propósito general, su sintaxis deriva mucho de C y C++, pero tiene menos facilidades de bajo nivel que cualquiera de ellos. Es un lenguaje orientado a objeto, de una plataforma independiente. La programación en Java, permite el desarrollo de aplicaciones bajo el esquema de Cliente Servidor, como de aplicaciones distribuidas, lo que lo hace capaz de conectar dos o más computadoras u ordenadores, ejecutando tareas simultáneamente y de esta forma logra distribuir el trabajo a realizar.

Java se creó como una herramienta de programación para ser usada en un proyecto de *set-top-box* en una pequeña operación denominada *The Green Project* en *Sun Microsystems* en el año 1991. El equipo (*Green Team*), compuesto por trece personas y dirigido por James Gosling, trabajó durante 18 meses en *Sand Hill Road* en *Menlo Park* en su desarrollo. (Lenguajes de programación, s.f.)

3. NetBeans: Es un sistema modular, basado en estándares entorno de desarrollo integrado (IDE), escrito en el lenguaje de programación Java. El proyecto NetBeans consiste en un IDE de código abierto con todas las funciones escritas en el lenguaje de programación Java.

Permite el uso de un amplio rango de tecnologías de desarrollo tanto para escritorio, como aplicaciones Web, o para dispositivos móviles. Da soporte a las siguientes tecnologías, entre otras: *Java, PHP, Groovy, C/C++, HTML5...* Además puede instalarse en varios sistemas operativos: Windows, Linux, Mac OS. Diseño de *GUIs Swing* intuitiva de arrastrar y soltar los componentes de interfaz gráfica de usuario de una paleta en un lienzo, luego haga clic en *JLabels, JButtons, JTextFields* y editar el texto directamente en el lugar. Usted puede incluso utilizar el constructor de interfaz gráfica de usuario para crear prototipos de interfaces gráficas de usuario justo en frente de los clientes. El IDE NetBeans viene con soporte incorporado para la localización de interfaz gráfica de usuario y la accesibilidad. (Download3k, s.f.)

4. MySQL: Es un sistema de gestión de base de datos relacional de código abierto, basado en lenguaje de consulta estructurado (SQL). (MySQL, s.f.)

Posee varias ventajas como velocidad al realizar las operaciones, lo que le hace uno de los gestores con mejor rendimiento, bajo costo en requerimientos para la elaboración de bases de datos, ya que debido a su bajo consumo puede ser ejecutado en una máquina con escasos recursos sin ningún problema, facilidad de configuración e instalación, soporta gran variedad de Sistemas Operativos, baja probabilidad de corromper datos, incluso si los errores no se producen en el propio gestor, sino en el sistema en el que está, su conectividad, velocidad, y seguridad hacen de MySQL altamente apropiado para acceder bases de datos en Internet y el *software* MySQL usa la licencia GPL.

5. *Play framework*: Es una alternativa simple a la sobrecargada plataforma para desarrollo de aplicaciones empresariales de Java. Se concentra en la productividad del desarrollar y apunta a arquitecturas de aplicaciones *RESTful*. El objetivo del framework Play es facilitar el desarrollo de aplicaciones web sin renunciar al uso de Java y está basado en la arquitectura MVC (Modelo, Vista, Controlador).

Play utiliza *sbt* como sistema de *builds*. Tiene una serie de *scripts* predefinidos que nos ayudan a comenzar con nuestra aplicación (*play new, run* o *start*), además de un fichero con *script* pre configurado que será suficiente para la mayor parte de los desarrollos, pero que permite una modificación fácil de los *scripts* de *build, deployed, etc.* A diferencia de otros Framework de desarrollo, Play no utiliza *Servlets* para el manejo de peticiones, esto implica que no existe una sesión para cada una de las peticiones. Para tener una funcionalidad similar a las sesiones tendremos que utilizar el almacenamiento en el navegador a través de *cookies* o *localStorage*. Esto permite una mejor escalabilidad horizontal de las aplicaciones. Cuando llega una petición a la aplicación el balanceador podrá enviarla a cualquier nodo, sin importarnos en cual se ha servido la petición anterior. No se necesita replicar el estado. (Saez, s.f.)

Entre las ventajas de Play se encuentran: que es un *framework* orientado a pruebas, productividad, fácil detectar los errores. Integración con Netbeans y Eclipse, proporciona un esqueleto para la aplicación. Una de las desventajas es que no cumple con la especificación de Java EE, lo cual no es un problema en sí, pero algo a tener en cuenta, implica que no hay sesiones por conexión.

Se obtiene un sistema Web que al acceder requiere de autenticación, este cuenta con roles para los usuarios y para los responsables de seguridad informática, en dependencia de estos y atendiendo a sus privilegios, serán las operaciones que aparecerán en las pantallas siguientes.

A su vez el sistema está dividido en 3 módulos.

Módulo 1 Obtención e inserción de trazas: El sistema debe obtener las trazas del proxy. Posteriormente debe parsear esos registros y guardarlos en la base de datos.

Módulo 2 Control de trazas para usuarios: Los usuarios podrán visualizar las trazas de navegación a través del proxy de la UNICA, permitiéndole analizar los horarios, los IP y los sitios.

Módulo 3 Soporte a la toma de decisiones: El sistema permitirá generar informes sobre el uso de los servicios de proxy, además de generar alertas al detectar irregularidades en el uso de estos servicios por parte de los usuarios.

CONCLUSIONES

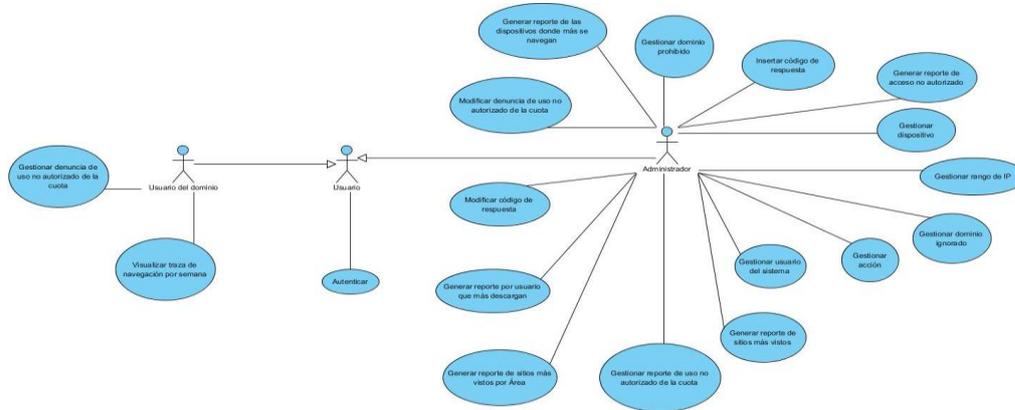
El presente trabajo se centró en la implementación de un sistema capaz de controlar las trazas generadas por el servidor proxy Squid. Los estudios realizados permitieron corroborar la necesidad de implementar un sistema de control de trazas del servidor proxy para la Universidad de Ciego de Ávila Máximo Gómez Báez. Este sistema obtenido permitirá a los usuarios poder visualizar sus trazas de navegación para llevar un control de las mismas, y servirá de apoyo a los directivos de la universidad en la toma de decisiones.

BIBLIOGRAFÍA CONSULTADA

- CASTELLS, M.: *La galaxia Internet – Reflexiones sobre Internet, empresa y sociedad*, Barcelona, España, 1999.
- CHAVEZ, M.: *Sistema de análisis de registros de servidores proxy para usuarios*, Universidad de las Ciencias Informáticas, La Habana, 2011.
- DOWNLOAD3K: Disponible en <http://www.download3k.es/DesarrolloSoftware/Otros/DownloadNetBeansIDE.html>. Visitado el 20 de enero de 2016.
- GUTIÉRREZ, M.: *Administrar para la calidad. Conceptos administrativos del control total de calidad*, México Limusa (Noriega Editores México), 2007.
- Lenguajes de programación*. Disponible en <http://www.lenguajes-de-programacion.com/programacion-java.shtml>. Visitado el 20 de enero de 2016.
- MARTÍN ÁLVAREZ, L.O. Y GARCÍA MARTÍNEZ, Y.: *Sistema de reportes de la navegación por Internet*, (Pregrado en Ingeniería en Ciencias Informáticas), Habana, Cuba, Universidad de las Ciencias, 2007.
- MySQL. Disponible en <http://searchdatacenter.techtarget.com/es/definicion/MySQL>. Visitado el 29 de marzo de 2016.
- PALENZUELA, O.B.: *ISAWEB. Monitoreo de Tráfico en Internet*, Ciudad Habana, 2006.
- QUIÑONES, D.: *Sistema informático para el Control del Tráfico de Red en la Universidad Máximo Gómez Báez de Ciego de Ávila*, 2011.
- SAEZ, A.: *Codecriticon.*, de <http://codecriticon.com/play-framework/>
- Sawstats. Disponible en <http://kevells spanish.readthedocs.org/es/latest/sawstats.html>. Visitado el 12 de enero de 2016.
- TERRY, G.F.: *Principios de administración*, México, Ed. Continental, 1999.
- Webalizer*. Disponible en <http://www.webalizer.org/>. Visitado el 15 de febrero de 2016.
- Webtrends Log Analyzer*. R. Disponible en <http://webtrends-log-analyzer.softonic.com/>. Visitado el 12 de enero de 2016

ANEXOS

Anexo 1- Diagrama de Casos de Uso. RUP



Anexo 2- Portada del módulo control de trazas para usuarios.



Anexo 3- Portada del módulo soporte a la toma de decisiones.

