Sistema ATISA:
Analizador de Trazas de Internet

Raycos Brito Sarasa[1], Reinier González Gazapo[2]

[1] Ingeniero Informático, Máster en Ciencias en Informática Aplicada. rbrito@espac.avianet.cu
[2] Técnico Medio en Instrumentación y Control Automático. reinier.gonzalez@espac.avianet.cu

Dirección de Informática y Comunicaciones
Empresa de Seguridad y Protección de la Aviación Civil

RESUMEN

Sistema ATISA: Analizador de Trazas de Internet
La presente investigación muestra el desarrollo del Sistema ATISA (Analizador de Trazas de Internet), como propuesta para el control y monitoreo del uso de la infraestructura de redes, dentro de la estrategia de seguridad informática que se implementa de manera general en Cuba, y de forma particular por la Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.). Se exponen además, las principales actividades y funcionalidades implementadas, la importancia sobre el control del tráfico web, y los aportes económico-sociales que redundan para la entidad.

ABSTRACT

The present investigation shows the development of the ATISA System (Internet Trace Analyzer), as a proposal for the control and monitoring of the use of the network infrastructure, within the IT security strategy that is implemented in general in Cuba, and particular form by the Civil Aviation Security and Protection Company (ESPAC SA). The main activities and functionalities implemented, the importance of web traffic control, and the economic and social contributions that result in the entity are also exposed.

INTRODUCCIÓN

La mayoría de los servicios de Internet tienen la capacidad de registrar los accesos a sus contenidos mediante archivos de trazas o “logs”. Cada petición de una página web es almacenada como una línea de información en estos ficheros, y dependiendo del formato de la línea, incluye información como la página solicitada, su tamaño, qué navegador se utilizó, entre otros datos.

Estos ficheros de log contienen enormes cantidades de información, pero el formato es difícil de interpretar sin ayuda de las tecnologías. Se necesitan herramientas que realicen resúmenes de los datos para facilitar el análisis del contenido.

La Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.), cumple con las políticas establecidas por la Corporación de la Aviación Cubana (CACSA) en materia de seguridad informática, y emplea para el monitoreo del tráfico de Internet aplicaciones encargadas fundamentalmente de la gestión y el control del acceso a la red de redes, no así del análisis de trazas.

Esta investigación persigue como objetivo mostrar el desarrollo y las funcionalidades de la aplicación ATISA (Analizador de Trazas de Internet), como una nueva herramienta para la investigación de los accesos de los usuarios a la red de redes, a fin de aportar mayores elementos para la toma de decisiones en materia de seguridad informática. Se detallan además, la importancia del control sobre el tráfico en Internet, y una valoración económica que mide su factibilidad de uso dentro de la entidad.

DESARROLLO

Tráfico en Internet

El tráfico web es la cantidad de datos enviados y recibidos por los visitantes de un sitio web, y está determinado por el número de visitas y de páginas web consultadas. Es medido, además, para calcular la popularidad de sitios web y páginas individuales.

El tráfico web puede ser analizado empleando la estadística encontrada en el servidor de páginas web, que se genera automáticamente a partir de cada visita realizada al sitio. Algunos de los criterios de medición del tráfico en la red son:

- Número de visitantes.
- Promedio de páginas vistas por un usuario.
- Promedio de tiempo de un usuario en el sitio.
- Páginas más requeridas (más populares).

La cantidad de tráfico en un sitio web sirve para medir su popularidad. Analizando las estadísticas de visitantes es posible saber qué está bien y qué se debe mejorar. También es posible aumentar (o en algunos casos disminuir) la popularidad del sitio y la cantidad de gente que lo visita.

Cada servidor de Internet cuenta con un log o archivo que registra todas las visitas de los usuarios, a razón de una línea de texto por cada acceso al servidor. Estos archivos son utilizados con fines estadísticos, a fin de permitir el control del tráfico y minimizar la ocurrencia de delitos cibernéticos.

Control del Tráfico en Internet

El control de tráfico de Internet es el conjunto de herramientas que permiten a los administradores de red, tener un control de la actividad en la infraestructura de comunicaciones de una organización, con el objetivo de:

- Cumplir las políticas de seguridad de la organización.
- Alcanzar un rendimiento óptimo de la disponibilidad de la red.
- Lograr un uso adecuado de los recursos de la institución.

Las herramientas para el monitoreo de Internet permiten controlar el tráfico generado y recibido mediante el empleo de sistemas, que recolectan información en tiempo real de los elementos de la red, realizando también un análisis de los datos recogidos para detectar situaciones que están fuera de los parámetros normales de operación. Se realiza así un control sobre el uso del ancho de banda, los usuarios, el tipo de tráfico y del rendimiento en general.

Fundamentalmente, existen varios tipos de herramientas empleadas para el control y monitoreo del tráfico en Internet, entre ellas están:

- *Herramientas de gestión y control de ancho de banda*: destinadas a limitar y controlar el uso que se realiza del ancho de banda de la red, en base a políticas de seguridad y a las necesidades de la organización.
- *Herramientas de monitorización y reportes*: empleadas para analizar la disponibilidad de la red y generar informes que aportan información muy precisa de lo que está ocurriendo y de esta forma poder tomar decisiones para minimizar un determinado incidente.

El filtrado efectivo del tráfico de Internet ayuda en la educación y capacitación de los usuarios de una red a cumplir con las políticas y valores de la entidad, mientras sigue proporcionándoles a los individuos la información necesaria para realizar el trabajo.

La conservación y almacenamiento de los registros del tráfico de Internet en una organización permitirá realizar un correcto análisis de los mismos, contando además para ello con herramientas útiles que proporcionen un buen análisis de datos.

Herramientas empleadas

La Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.) utiliza fundamentalmente para la gestión y el control del tráfico en Internet herramientas propietarias, y su empleo está limitado al pago de una licencia de software.

Estas herramientas se utilizan fundamentalmente para la gestión y el control del ancho de banda de Internet, y sus funcionalidades potenciales están orientadas en este sentido, no así para el monitoreo y análisis de trazas, complicando el análisis oportuno de las informaciones relacionadas con tráfico en Internet, mediante la lectura de los “logs” o archivos de navegación de grandes períodos de tiempo.

ATISA: Analizador de Trazas de Internet

Para la ESPAC, el análisis de trazas de la navegación en Internet resulta fundamental, en pos de garantizar la seguridad informática de la entidad, y la disponibilidad del acceso a la red de redes.

En este sentido, por lo engorroso que resulta el estudio y monitoreo de grandes volúmenes de datos de la navegación de los usuarios en Internet, fue necesario la creación de una herramienta que se especializara en el análisis de trazas y la generación de informes oportunos y detallados, para apoyar la toma de decisiones en materia de seguridad informática.

Por su importancia para el desarrollo de este tipo de proceso, esta investigación propone la creación del Analizador de Trazas de Internet (ATISA), encargado de permitir a los especialistas de seguridad informática, el análisis oportuno de las trazas de Internet, con un mínimo de esfuerzos, y un apoyo visual y documental oportuno. La Figura 1 muestra la vista principal de la aplicación:

Es necesario señalar que la herramienta propuesta no sustituye el uso de otras aplicaciones ya establecidas en el mercado, sino que las complementa. Su función primordial es dotar a los especialistas y directivos de seguridad informática de un instrumento fácil de manipular, que permita establecer pronósticos a priori, relaciones o dependencias entre los datos, consolidar información y agruparla, además de graficar y exportar los datos pre-procesados.

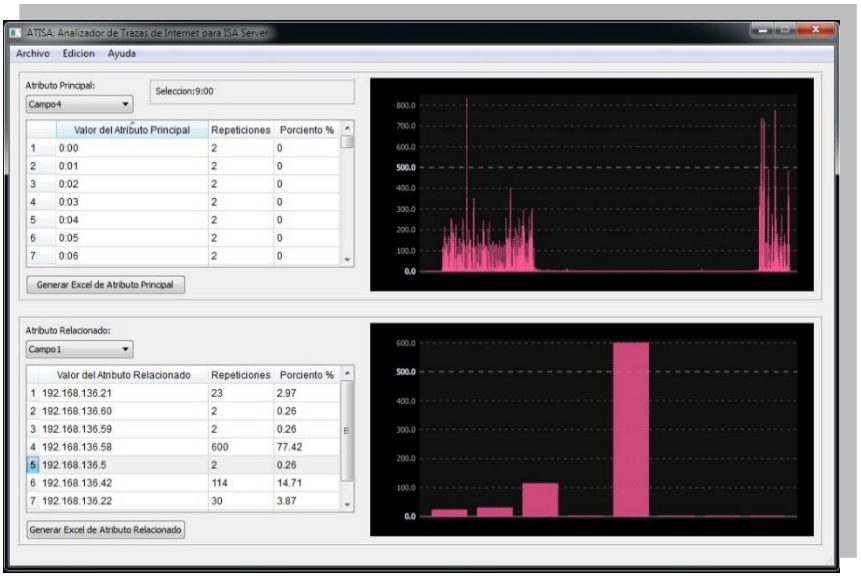


Figura 1. Algunas opciones del Analizador de Trazas de Internet (ATISA)

Funcionamiento

La herramienta ATISA permite a los especialistas de seguridad informática realizar análisis interactivos de los datos generados por su tráfico de Internet, tal como muestra la Figura 2.

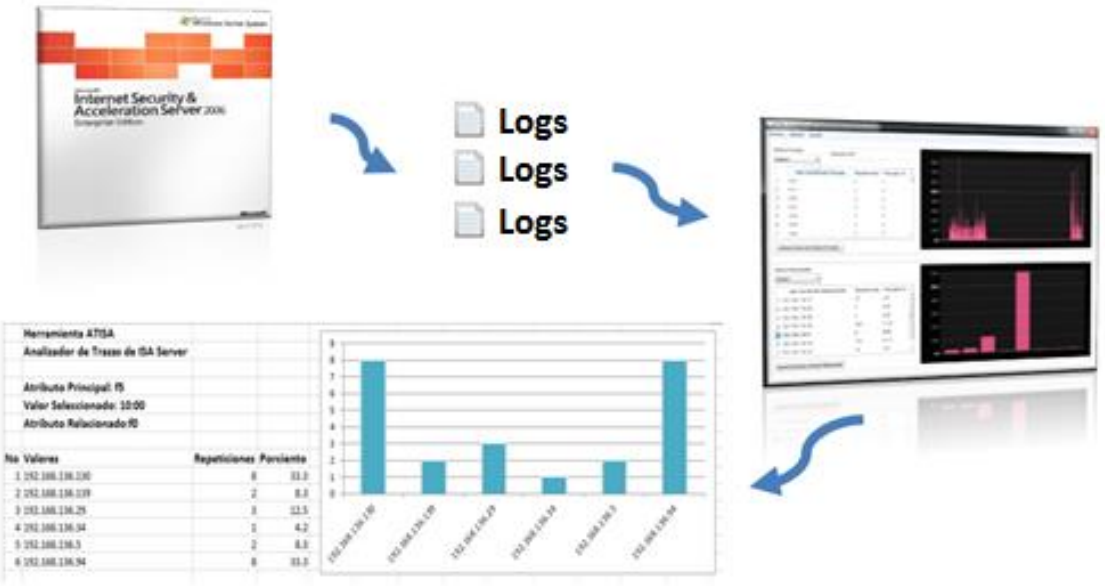


Figura 2. Flujo de trabajo con la herramienta ATISA

Desde la vista principal de la aplicación ATISA será posible abrir para el análisis de trazas, cualquier fichero generado por los proxy: ISA Server (*.iis), o Squid (*.log); y una vez cargada la información se mostrará la cantidad de datos analizados.

La herramienta está constituida por dos módulos de análisis de datos: uno para examinar el comportamiento de un Atributo Principal, y una vez seleccionado alguno de sus valores, otro para mostrar las dependencias de un Atributo Relacionado a este. Además, cada módulo permite:

- Ordenar y reagrupar valores de repeticiones y porcientos.
- Representación gráfica de comportamientos de los datos.
- Exportación a Excel de los datos y generación automática de gráficas.

Para desplegar la aplicación ATISA en cada computadora donde se necesite emplear, se ha desarrollado un programa de instalación muy intuitivo, que luego de varias preguntas simples al usuario, deja instalada la herramienta y suministra accesos directos a la misma desde el escritorio de trabajo.

Características

El Sistema ATISA contiene, como lo muestra la Figura 3, un ***Menú de Opciones*** que agrupa las principales tareas iniciales relacionadas con la carga de datos y la licencia de operación de la aplicación.

Figura 3. Características Generales del Sistema ATISA

Una vez cargados los datos, la herramienta mostrará dos módulos fundamentales, uno encima del otro; en el superior, bajo la etiqueta ***Atributo Principal***, la relación de todos los campos que fueron registrados por el proxy, y que pertenecen al log de navegación de Internet que se está analizando.

La etiqueta de ***Valores del Atributo Principal*** muestra los posibles valores, cantidad de repeticiones y por ciento, que puede tomar un atributo (campo) seleccionado como Atributo Principal.

La ***Gráfica de Valores del Atributo Principal*** muestra la distribución gráfica de los valores del atributo seleccionado.

El botón ***Generar Excel de Atributo Relacionado*** permite realizar una exportación a Excel, tanto de la tabla de valores como de la gráfica, del comportamiento del atributo seleccionado.

El segundo módulo, con funcionalidades similares al primero, permite seleccionar un ***Atributo Relacionado*** a un valor particular del Atributo Principal, de manera tal que se facilite obtener relaciones o dependencias entre el valor de un primer atributo, con los valores de un segundo. Todas las características de este segundo módulo son iguales a las del primero, por lo que una vez seleccionado

el Atributo relacionado, se podrán observar sus valores, repeticiones y porcientos, y una representación gráfica, de su comportamiento.

La Figura 4 muestra a continuación para el Menú de Opciones relacionado con Edición, la posibilidad de editar los campos que se importarán del log de navegación de internet que se desea analizar; en este sentido permite seleccionar para que se muestre o no un determinado Campo, así como la posibilidad de asignarle un nombre más representativo que identifique su contenido, muy útil para el análisis.

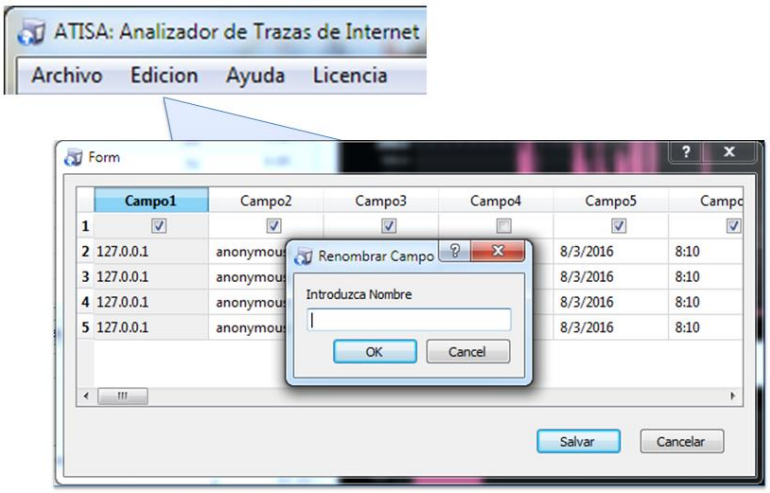


Figura 4. Menú Edición de la Herramienta ATISA

El Sistema ATISA se distribuye gratuitamente bajo una versión de prueba válida por un período de 30 días, luego del cual será necesaria una licencia de uso, que liberará completamente la herramienta por el tiempo pactado en la licencia, tal como muestra a continuación la Figura 5.

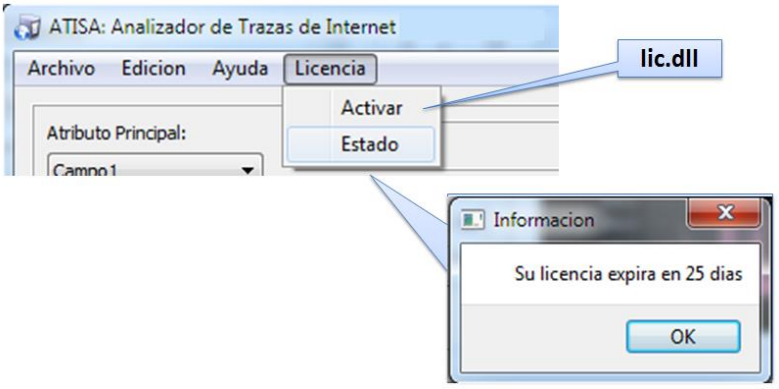


Figura 5. Menú Licencia del Sistema ATISA

Para solicitar una licencia de explotación del Sistema ATISA, será necesario seguir las instrucciones generadas a partid de la opción Activar.

CONCLUSIONES

El desarrollo de la aplicación ATISA representa para la Empresa de Seguridad y Protección de la Aviación Civil una fortaleza, en el monitoreo y análisis del tráfico de Internet, como instrumento para garantizar la seguridad informática. En este sentido, es posible arribar a las siguientes conclusiones:

- El control del tráfico en Internet constituye una necesidad para cualquier entidad que navegue por la red de redes, y en este sentido contar con las aplicaciones oportunas para su disponibilidad y monitoreo es de vital importancia.
- El Analizador de Trazas de Internet (ATISA), constituye una nueva solución para el control y análisis de la navegación en la entidad, que carece de herramientas factibles para este proceso.
- El empleo de la herramienta ATISA potencia la seguridad informática y humaniza el trabajo de los especialistas de estas áreas.

Finalmente se recomienda la generalización a otras empresas de la aviación o el país que empleen registros de Internet los archivos “logs” generados por los proxys ISA Server o Squid.

BIBLIOGRAFÍA CONSULTADA

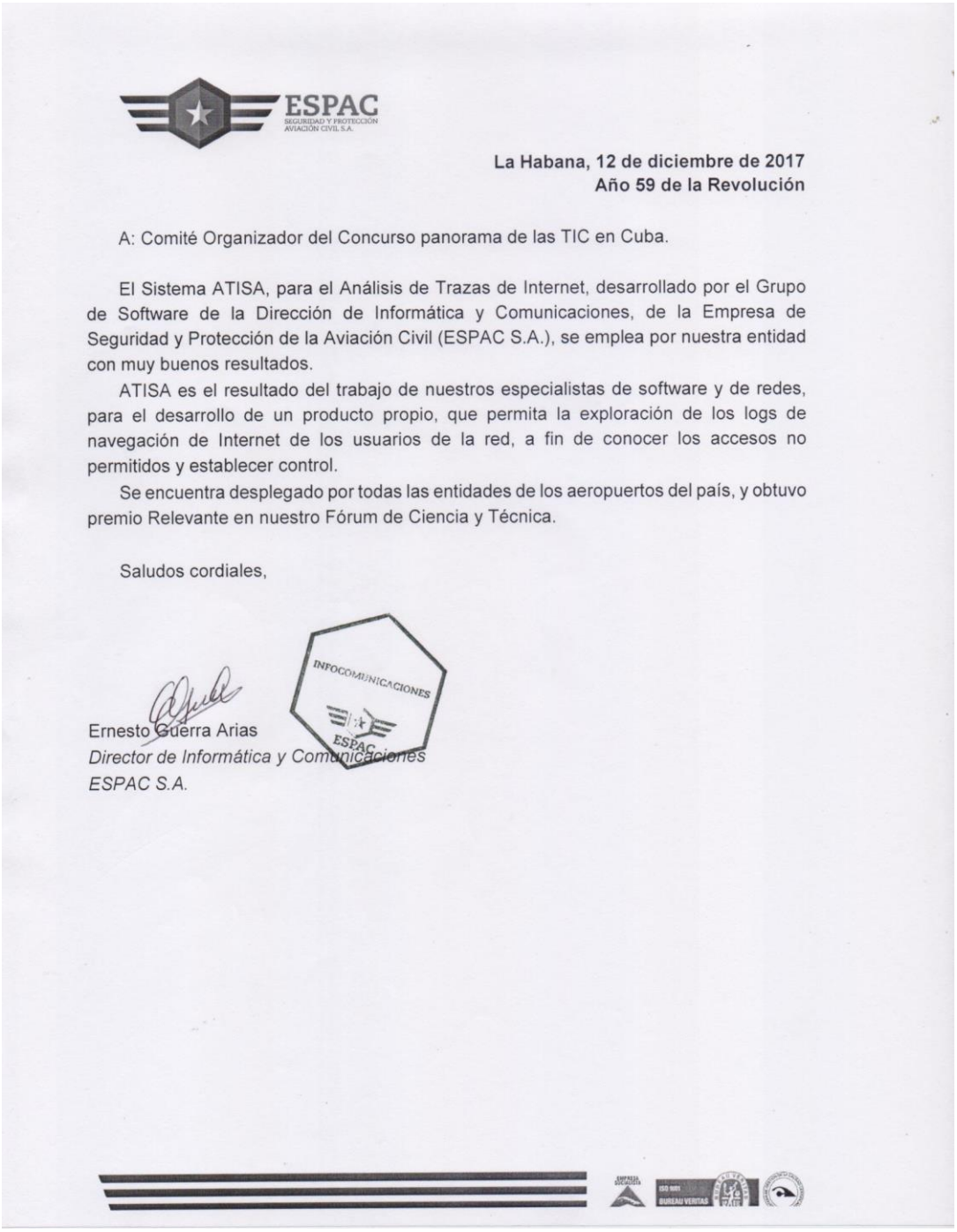
- Adminso. Administración de Sistemas Operativos: ISA Server. Consulta en línea el 22/06/2015. Disponible en: http://www.adminso.es/index.php/ISA_Server
- Control de Tráfico. Conceptos. Consulta en línea el 22/06/2015. Disponible en: http://www.um.edu.ar/catedras/PPT03/document/Modulo_III/Traffic-Control/ppt0c3-tc-01.html
- CristianAriel27. 5-Implementación de seguridad de la red y del perímetro. Consulta en línea el 22/06/2015. Disponible en: http://es.scribd.com/doc/38898598/5-Implementacion-de-seguridad-de-la-red-y-del-perimetro#scribd
- E-project Group. SurfControl Web Filter. Consulta en línea el 22/06/2015. Disponible en: http://www.e-projectgroup.cl/Partners/SurfControl/surfcontrol_webfilter.htm
- Gutierrez Calderón, Alejandra et al. Manual de Instalación y Configuración de ISA Server 2006 en Windows Server 2003. Consulta en línea el 22/06/2015. Disponible en: http://es.slideshare.net/edaincc/tutorial-isa-server-2006
- Incibe: Instituto Nacional de Ciberseguridad. Control de tráfico de red. Consulta en línea el 22/06/2015. Disponible en:

https://www.incibe.es/extfrontinteco/icd/pdf/Control_de_Trafico_de_Red.pdf

- Logreport, Egon Willighagen. Analizando los ficheros log de sus aplicaciones de Internet. Consulta en línea el 22/06/2015. Disponible en: http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/September2001/article213.shtml
- Microsoft Corporation. ¿Qué es ISA Server 2006? Consulta en línea el 22/06/2015. Disponible en: https://www.microsoft.com/spain/isaserver/prodinfo/whatis.mspx

ANEXOS

Anexo 1. Aval de la Dirección de Informática y Comunicaciones, de la Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.).



ESPAC
SEGURIDAD Y PROTECCIÓN AVIACIÓN CIVIL S.A.

La Habana, 12 de diciembre de 2017
Año 59 de la Revolución

A: Comité Organizador del Concurso panorama de las TIC en Cuba.

El Sistema ATISA, para el Análisis de Trazas de Internet, desarrollado por el Grupo de Software de la Dirección de Informática y Comunicaciones, de la Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.), se emplea por nuestra entidad con muy buenos resultados.

ATISA es el resultado del trabajo de nuestros especialistas de software y de redes, para el desarrollo de un producto propio, que permita la exploración de los logs de navegación de Internet de los usuarios de la red, a fin de conocer los accesos no permitidos y establecer control.

Se encuentra desplegado por todas las entidades de los aeropuertos del país, y obtuvo premio Relevante en nuestro Fórum de Ciencia y Técnica.

Saludos cordiales,

INFOCOMUNICACIONES
ESPAC

Ernesto Guerra Arias
Director de Informática y Comunicaciones
ESPAC S.A.

Anexo 2. Premio RELEVANTE, en el Evento de Nacional del Fórum de Ciencia y Técnica 2015, de la Empresa de Seguridad y Protección de la Aviación Civil (ESPAC S.A.)

Anexo 3. Aval de Participación del IV Taller Internacional de las TIC en la Gestión de las Organización. Informática 2016

Informática 2016
XVI CONVENCIÓN Y FERIA INTERNACIONAL
16TH INTERNATIONAL CONVENTION AND FAIR

Conectando sociedades
Connecting societies

La Habana, Cuba
Del 14 al 18 de marzo
Havana, Cuba
March 14th to 18th

El Comité Organizador de la XVI Convención y Feria Internacional Informática 2016 otorga el presente:

The Organizing Committee of the 16th International Convention and Fair Informática 2016 grants this:

CERTIFICADO
CERTIFICATE

A / To:

Raycos Brito Sarasa

Por haber presentado la Ponencia / Having presented the Paper

ATISA: analizador de trazas de internet para ISA SERVER /
ATISA: Internet Trace Analyzer for ISA Server

En el evento / In the event

IV Taller Internacional las Tic en la Gestión de las Organizaciones /
4th International Workshop the IT in the Organizations Management

Ing. Wilfredo González Vidal
Presidente Ejecutivo del Comité Organizador / Executive President of the Organizing Committee
Viceministro del Ministerio de Comunicaciones / Vice Minister of Communications

www.informaticahabana.cu

Anexo 4. Aval de Participación del I Taller Nacional del Transporte. MITRANS 2017.

SÍNTESIS CURRICULAR DE LOS AUTORES:

Raycos Brito Sarasa. Ingeniero Informático, Máster en Ciencias Informáticas, Profesor Auxiliar, Especialista Principal en Ciencias Informáticas. *Centro de trabajo*: Dirección de Informática y Comunicaciones ESPAC S.A, Carretera a Aerocaribbean, km 1 ½, Wajay, Boyeros, Aeropuerto Internacional José Martí. La Habana, Cuba. *Correo electrónico*: rbrito@espac.avianet.cu. *Líneas de Investigación*: minería de datos y aprendizaje automático, ingeniería de software y comercio electrónico.

Reinier González Gazapo, Técnico Medio en Instrumentación y Control Automático, Especialista en Ciencias Informáticas. *Centro de trabajo*: Dirección de Informática y Comunicaciones ESPAC S.A, Carretera a Aerocaribbean, km 1 ½, Wajay, Boyeros, Aeropuerto Internacional José Martí. La Habana, Cuba. *Correo electrónico*: reinier.gonzalez@espac.avianet.cu. *Líneas de Investigación*: programación en Python, Java script y Android.