

**Evento: XIV Forum de Ciencia y Técnica.**

**Título: ISAWEB. Monitoreo de Tráfico en Internet.**

**Autor: Otniel Barrera Palenzuela**

**Centro: ICID**

**Organismo: MIC**

**Municipio: Playa**

**Provincia: Ciudad Habana**

**2006**

**Tabla de Contenidos**

Tabla de Contenidos.....	2
I. Resumen .....	3
II. Introducción. ....	4
III. Materiales y Métodos.....	6
Identidad Visual. ....	6
Active Directory y LDAP.....	7
Isa Server. ....	8
WinKronos .....	8
Herramientas de Desarrollo utilizadas.....	8
IV. Desarrollo.....	10
1- BackupsBD:.....	10
2- Intranet: .....	10
3-IsaWeb: .....	10
Administración ISAWEB.....	11
IsaWeb (Windows Form).....	12
ActualizacionLoginsIntranet. ....	13
ISAWEB (Web Form).....	13
V. Valoración Económica y Social.....	17
VI. Conclusiones.....	20
VII. Recomendaciones.....	21
VIII. Bibliografía. ....	22
IX. Anexos .....	23
Anexo 1: Maqueta Web del ICID.....	23
Anexo 2: Elementos Componentes de los Logs del Isa Server .....	25

## ***I. Resumen***

Este trabajo versa sobre la forma de lograr un seguimiento efectivo y particularizado del acceso de los usuarios de una intranet a Internet. Toma como base la creación de un software en el ICID que lo permite (ISAwEB). Aborda los problemas de seguimiento al acceso a Internet y las características de ISAwEB.

Cuba está limitada para acceder a Internet debido al Bloqueo. Nos están veladas las tecnologías estadounidenses de comunicaciones y se nos prohíbe la conexión a cables submarinos de fibra óptica. El gobierno mantiene un uso racional de Internet, priorizando ámbitos como el social, salud, cultura, educación y ciencia y técnica.

Para lograr un uso racional y controlado de Internet en el ámbito empresarial es que se diseñó el producto: ISAwEB. Esta aplicación permite que un usuario autenticado pueda filtrar información relevante sobre el acceso de Internet.

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.

Para preservar la confidencialidad de la información, se asegura que una persona solo tenga acceso a información generada por su propio tráfico o el de sus subordinados. Todo esto se logra gracias a una rigurosa jerarquía tomada de la aplicación "Winkronos" (desarrollada en el ICID).

El diseño es compatible con la identidad corporativa del ICID, pero mantiene también una imagen propia.

Esta es una aplicación Web y su interfaz es sencilla, flexible, amigable e intuitiva. Se logró que se hiciera fácil el control individualizado del tráfico de Internet.

## ***II. Introducción.***

Cuba se conecta a la red de redes en mayo de 1994 y no por falta de computadoras o por errores en la red, sino porque hasta ese entonces permaneció bloqueado por Estados Unidos. En 1992, la ley Torricelli (que acentuaba el bloque dispuesto por Washington hace más de 40 años) identificó las comunicaciones con Cuba como una manera de debilitar a la Revolución cubana [2]. El uso de Internet y de cualquier nueva tecnología se usa creativamente y para el mayor beneficio social.

Un dato para tener en cuenta es que el 60 por ciento de los más de 43 millones de computadoras en el mundo conectadas al “ciberespacio” tienen dominio en la administración por parte de Estados Unidos, según se desprende de informes elaborados por la ONU.

El bloqueo que mantiene Estados Unidos sobre Cuba hace que tengamos que utilizar un ancho de banda y una conexión de satélite de altos costos y muy lentos. Pero la solución está a solo kilómetros si se conectara un simple cable de fibra óptica entre Cuba y la Florida.

A pesar de esto el país avanza en la rama de la computación y la informática. Según el informe de Cuba en la Cumbre Mundial sobre la sociedad de la Información en el 2004 el país disponía de 2,73 computadoras personales por cada 100 habitantes y al cierre del primer semestre del 2005 se cuantifican 335 mil computadoras, lo que representa una distribución de 2,98 PC por cada 100 habitantes [1]. En Cuba la Digitalización telefónica es del 85,6%, hay más de 1315 dominios (sólo en .cu). El ancho de banda Internet es de solo 41 Mbps de salida y 87 Mbps de entrada.

Es en los centros educacionales, culturales y científicos donde se concentra en Cuba la casi totalidad de los usuarios de Internet. Es por eso que ante las limitaciones existentes se impone que se haga un uso racional de la misma. Se debe luchar además contra el acceso a sitios cuyos contenidos violen la legislación vigente y sean contrarios a la ética y moral socialista. Esta es una tarea de todos, hay que actuar con firmeza contra las irregularidades. Ante la necesidad de tener un software de apoyo a la seguridad informática, el ICID decidió desarrollar una aplicación que permitiera que todos los

usuarios de Internet de la institución fueran sus propios garantes del uso que se le da a esta tecnología; este producto se llama: ISAWEB.

La necesidad de este software está dada porque la labor investigativa del ICID exige una utilización intensiva de Internet. De las 293 computadoras del ICID 119 tienen permiso para acceder a Internet, hay 182 usuarios con permisos de navegación. Sin embargo el ancho de banda para esta conexión es de solo 256 Kbps, divididos en dos líneas dedicadas de 128 Kbps, se hace imprescindible controlar el tráfico de los usuarios.

La navegación en estos momentos en el ICID genera volúmenes de información en el orden de los 211 369 registros diarios, 968 210 registros semanales, ocupando una capacidad de 120 Mb diarios.

### ***III. Materiales y Métodos***

ISAWEB más que generar información nueva, vincula información generada por distintas aplicaciones informáticas instaladas y utilizadas en el ICID y les da un nuevo significado. Las herramientas y aplicaciones con las que se relaciona ISAWEB son las siguientes:

#### **Identidad Visual.**

El ICID posee una Identidad Visual Institucional. Entiéndase como el conjunto de todos los signos fundamentales de carácter visual, a través de los cuales una entidad cualquiera puede comunicar su discurso de identidad.

Esto nos llevó a trabajar usando los signos fundamentales de la Identidad Visual del ICID [3]:

- el identificador (Ver figura 1)
- el código cromático (#6732BA (web))
- el código tipográfico (Lúcida Sans)

Estos signos están definidos incluso para el desarrollo de páginas Web, donde se definió una maqueta de la misma (Ver Anexo1: Maqueta Web del ICID)



Figura 1: Logotipo del ICID

## Active Directory y LDAP.

El ICID posee una red a la cual están conectadas la casi totalidad de las computadoras. Todas las computadoras de la red están incorporadas dentro del dominio “icid.cu”. Hay un servidor primario (DNS) que controla el acceso y los privilegios, tanto de las máquinas como de los usuarios del dominio. Para el servicio de Internet, hasta el momento, se ha otorgado acceso a 182 usuarios, todos a su vez, usuarios del dominio. ISAWEB implementa que los usuarios de la aplicación se validen como usuarios del dominio.

Active Directory es el servicio de directorio de Windows que proporciona una visión unificada de redes complejas. Reduce el número de directorios y espacios de nombres con los que debe trabajar un programador. Proporciona una forma sencilla de estructurar una red informática compleja. Un sistema Active Directory se organiza en un árbol jerárquico. Cada nodo del árbol representa un recurso o servicio disponible en la red, y contiene una serie de propiedades que pueden recuperarse y manipularse [4] (Ver figura2).

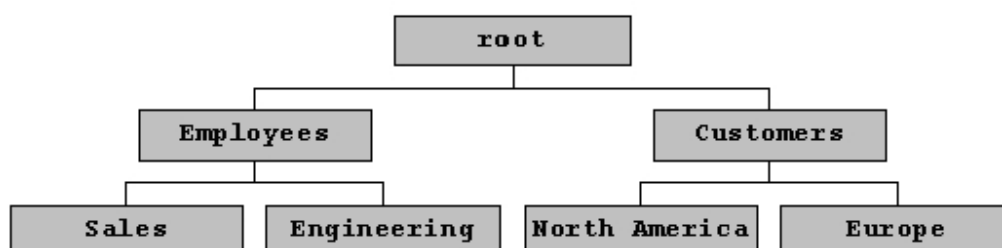


Figura 2: Ejemplo de un árbol de directorio sencillo.

La manera en que una aplicación puede acceder a información almacenada en un directorio de información es mediante un Protocolo de Acceso Ligero a Directorio, mejor conocido como LDAP (por sus siglas en inglés: Lightweight Directory Access Protocol) [4].

El protocolo LDAP es utilizable por distintas plataformas y basado en estándares, de ese modo las aplicaciones no necesitan preocuparse por el tipo de servidor en que se hospeda el directorio. De hecho, LDAP esta encontrando mucha más amplia aceptación a causa de ese estatus como estándar de Internet.

### **Isa Server.**

El servidor Proxy de Internet instalado en el ICID es el “Isa Server 2004”. Microsoft Internet Security and Acceleration (ISA) Server 2004 es un miembro fundamental de la familia de servidores Microsoft Server System, dirigido a cubrir las necesidades actuales en materia de seguridad en Internet.

Isa Server genera un grupo de ficheros (logs) donde almacena información relacionada con los diferentes servicios que brinda, estos ficheros son almacenados físicamente en el servidor. Los nombres de los logs de Internet tienen la siguiente estructura: **WEBEXTDaaaammdd.log**; donde cada letra **a** es un dígito de año, **m** de mes y **d** de día. Estos ficheros almacenan una gran cantidad de información sobre cada petición de página web en Internet y cada componente de dicha página. ISAwEB solo va a utilizar aquellos elementos de mayor trascendencia para almacenar en base de datos, y de esos solo un subconjunto (los más relevantes para los usuarios) se mostrarán al usuario de la aplicación (Vea Anexo 2: Elementos Componentes de los Logs del Isa Server).

### **WinKronos**

ISAwEB se vincula con parte de la base de datos de la aplicación WinKronos. Este es un sistema informático desarrollado en el ICID, destinado a facilitar el tratamiento de la información obtenida de los relojes electrónicos que almacenan las marcas de entrada y salida del personal de una empresa. Esta aplicación se desarrolló en Visual Fox Pro y su base de datos incluye tablas donde se almacenan los datos generales de todos los trabajadores y la jerarquía de subordinación, estas tablas son usadas por ISAwEB.

### **Herramientas de Desarrollo utilizadas.**

En ISAwEB no se genera información de entrada, toda la información que necesita es generada por otras aplicaciones. Estas aplicaciones almacenan la información en formatos que van desde ficheros textos, base de datos de Fox Pro (xbase files), registros de Active Directory y bases de datos de SQL Server. Se decidió estandarizar el acceso a



datos utilizando para ello SQL Server 2000. Para transformar toda esa información a bases de datos relacionales SQL se crearon aplicaciones de consola (desarrolladas en Borland Delphi) que se ejecutan como tareas de Windows en los servidores de Internet y de datos.

La parte fundamental de la aplicación ISAWEB se desarrolló en ASP.NET que es una tecnología del lado servidor de Microsoft para páginas web generadas dinámicamente, que ha sido comercializada como un anexo a Internet Information Server (IIS). La razón de esta elección es las potencialidades que brinda y la fácil vinculación con las herramientas y aplicaciones instaladas en el ICID, todas de factura Microsoft.

#### **IV. Desarrollo.**

Antes de explicar las partes que compone ISAWEB se hará una explicación de las bases de datos de SQL Server con que interactúa.

##### **1- BackupsBD:**

Esta es la base de datos transformada de la aplicación Winkronos. Solo utilizamos las tablas: *maestra* (donde esta la información general de todos los trabajadores, incluyendo el código de departamento al que pertenecen y el código de su jefe), *jefes* (relación de los códigos de los jefes con sus códigos como trabajadores, gracias a esta tabla se establece la jerarquía) *departamentos* (descriptor de departamentos)

##### **2- Intranet:**

Base de datos desarrollada para otra aplicación en la que solo se accede a la tabla *gralLoginUsuarios*, donde están relacionados los logins de los usuarios del dominio con sus nombres completos.

##### **3-IsaWeb:**

Base de datos principal para la aplicación. En ella se almacenan en 13 tablas distintas (*Semana1/ISA* a *Semana13/ISA*) los datos más relevantes de los Logs por semanas del Isa Server, estas tablas son controladas por la tabla *General* que determina los rangos de fechas de registros en cada tabla (Ver Figura3). En la tabla *fecha* se almacena la fecha en que se hará la próxima salva de seguridad de la base de datos completa. Esta base de datos puede ser de gran tamaño; en el caso del icid más de 6 Gbs.

idTabla	nombreTabla	fecha_inicio	fecha_fin
1	Semana1ISA	2006-01-01	2006-01-07
2	Semana2ISA	2006-01-08	2006-01-14
3	Semana3ISA	2006-01-15	2006-01-21
4	Semana4ISA	2006-01-22	2006-01-28
5	Semana5ISA	2006-01-29	2006-02-04
6	Semana6ISA	2006-02-05	2006-02-11
7	Semana7ISA	2006-02-12	2006-02-18
8	Semana8ISA	2006-02-19	2006-02-25
9	Semana9ISA	2006-02-26	2006-03-04
10	Semana10ISA	2006-03-05	2006-03-11
11	Semana11ISA	2006-03-12	2006-03-18
12	Semana12ISA	0000-00-00	0000-00-00
13	Semana13ISA	0000-00-00	0000-00-00

Figura3: Tabla “General” de la Base de Datos IsaWeb

ISAWEB es una aplicación modular con 4 módulos, a continuación se dará una explicación breve de cada uno de ellos y con quien se relacionan. Se explicarán en el orden en que deben ser instalados o usados:

### **Administración ISAWEB.**

Aplicación desarrollada en Delphi que llena por primera vez la base de datos “IsaWeb” y ejecuta la primera copia de seguridad, para eso se le debe entrar el rango de fechas de los ficheros que se quieren transformar (Ver Figura4).

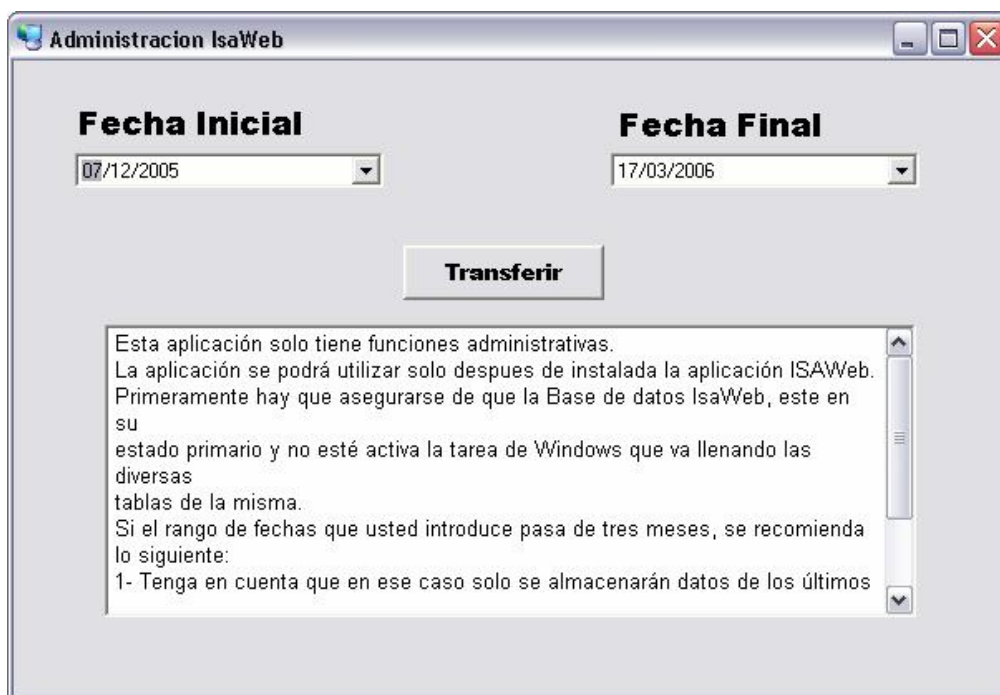


Figura 4: Interfaz de la aplicación “Administración Isa Web”

## IsaWeb (Windows Form).

Aplicación desarrollada en Delphi para ejecutarse como aplicación de consola dentro de una tarea programada de Windows. Esta aplicación corre en el servidor donde esté instalado el Isa Server. La tarea tiene que correr diariamente. IsaWeb (Windows Form) contiene un algoritmo muy similar al utilizado en la aplicación Administración ISAWEB. Este programa lee del Log con fecha un día anterior a la actual y toma aquellos campos que se determinaron como relevantes y los va almacenando en la tabla correspondiente de la base de datos “IsaWeb”.

## ActualizacionLoginsIntranet.

Aplicación desarrollada en C# utilizando Visual Studio .NET 2003 para ejecutarse como aplicación de consola dentro de una tarea programada de Windows. Esta aplicación corre en el servidor donde esté instalado el framework de .NET. Su función es actualizar la tabla *gralLoginsUsuarios* de la base de datos “Intranet”, para eso trabaja vinculada con Active Directory (mediante el protocolo LDAP) y la base de datos “BackupsBD”; debe ejecutarse una vez a la semana como mínimo.

## ISAWEB (Web Form).

Es la aplicación fundamental. Mediante ella los usuarios se interactúan con los datos de la base de datos “IsaWeb”. Primero los usuarios deben validarse como usuarios del dominio (Ver Figura 5). Si las credenciales son correctas la aplicación carga la página de filtrado de la información dependiendo del tipo de usuario conectado.



Figura 5: Página de Autenticación ISAWEB

Si el usuario validado es un trabajador sin cargos administrativos se le deshabilita la posibilidad de escoger ni departamentos ni usuarios, o sea, solo podrá ver información suya (Ver Figura 6). Si el usuario es jefe de departamento, subdirector, vicedirector o director, entonces se le habilitará la posibilidad de escoger entre los departamentos que le

están subordinados; solo después de escoger un departamento es que podrá escoger un usuario de esté departamento.



Figura 6: Página principal de ISAWEB

Hay que señalar que el filtrado no es obligatorio. La aplicación va generando una consulta dinámica a la base de datos dependiendo de las condiciones de filtrado que se introduzcan. En el caso de los departamentos y los usuarios, sino se seleccionan, la aplicación buscará todos los usuarios pertenecientes a todos los departamentos subordinados al usuario validado.

Siempre se debe escoger el rango de días en que se quiere realizar la consulta, esto se debe al gran tamaño de la base de datos. La información en cada una de las trece tablas puede sobrepasar en algunos caos, los 100 millones de registros, una consulta a

esta tabla puede demorar varios minutos. Si se hubiera mantenido toda la información en una sola tabla la cifra pudiera llegar a mil millones de registros, el tiempo de demoras de las consultas haría entonces impracticable el uso de la aplicación.

Los otros elementos de filtrado de la aplicación son:

- **Sitio:** Nombre o parte del nombre de un *Host* por el que se quiera filtrar.
- **Palabra Clave:** Parte del contenido de la dirección (URL) solicitada.
- **Dirección IP:** Número ip por el que se quiere hacer la búsqueda.
- **Fecha inicial y Fecha final:** Permiten entrar un rango de fechas para realizar la búsqueda.

Los reportes de la aplicación son:

- **General:** Muestra una información general de la búsqueda que se esta realizando con los siguientes campos: fecha, ip, Host, usuario, cantidad de bytes descargados, cantidad de bytes enviados, URL.
- **Simplificado:** Muestra una información general de la búsqueda, pero no haciendo visible todos los campos. Se muestran los siguientes campos: usuario, Host, fecha.
- **Favorito:** Muestra un reporte adecuado a la información filtrada con un listado ordenado descendentemente por los sitios más visitados y la cantidad de visitas.
- **Navegación:** Muestra un listado de los usuarios que más sitios han visitado y la cantidad de sitios visitados.
- **Descargas:** Muestra un listado descendente de los usuarios que más volumen de información descarga de Internet.
- **Logins -Trabajadores:** Listado que muestra a los jefes la relación de los logins y los nombres de sus subordinados.

El botón Rastrear es el que ejecuta el reporte y lo muestra al usuario. Cada reporte es personalizado tanto por las condiciones de filtrado que el usuario introdujo como por el tipo de usuario que es (Ver Figura 7 y 8).



Todo deja  
... RASTRO

[Inicio](#)

[Rastrear](#) 

**Reporte**

## Reporte Simplificado

2 of 2 

powered by  
**crystal** 

17/03/2006

Usuario

Sitio

Fecha

otniel	www.google-analytics.com	2006-03-14
otniel	www.google-analytics.com	2006-03-16

www.google-analytics.com

otniel

Figura 7: Ejemplo de un Reporte del tipo Simplificado.




Todo deja  
... RASTRO

[Inicio](#)

[Rastrear](#) 

**Reporte**

## Reporte de Sitios Favoritos

1 of 1+ 

powered by  
**crystal** 

17/03/2006

sitio

cantidad de visitas de usuarios

gdx.mlb.com	1.112
www.google.com.cu	165
mlb.mlb.com	165
mail.google.com	113
www.cubavsbloqueo.cu	82
mlbglobal.112.2o7.net	66
es.wikipedia.org	66
www.kremer-pigmente.de	65
www.mineranet.com.ar	56
upload.wikimedia.org	50
www.jrebelde.cubaweb.cu	50
www.habanaradio.cu	49
espn.deportes.espn.go.com	49
consultas.cuba.cu	47

Figura 8: Ejemplo de un Reporte del tipo "Favoritos".



## ***V. Valoración Económica y Social.***

El principal impacto de una aplicación como ISAwEB está dada en el ámbito social y no económico. ISAwEB permite que se monitoree el acceso de los usuarios de una empresa a Internet; que sitios se visitan, cuantas veces y cuando. En Internet se publican millones de sitios cuyo contenido no concuerda con las normas de una moral socialista, como pueden ser sitios xenófobos, terroristas, pornográficos, pedófilos, etc. El acceso a estos por usuarios irresponsables pudiera servir de pretexto al imperialismo y sus compinches para intentar desacreditar a la revolución. Sirva de ejemplo la ocasión en que acusaron falsamente al ICID de atacar cibernéticamente a instituciones del gobierno de los Estados Unidos.

No obstante lo anterior hay un peso económico detrás del mal uso de Internet. Desgraciadamente en Cuba no se han publicado análisis estadísticos sobre el uso de Internet en los centros laborales, por lo tanto en el presente trabajo se reflejarán estadísticas de algunos otros países y a estudios realizados dentro del ICID.

Según un estudio que ha realizado la firma Inology, los trabajadores españoles dedican más de 16 días al año a navegar por la Red durante la jornada laboral, por lo que cada trabajador pasa una media de 34,6 minutos diarios conectado a la Red. Según el estudio, durante el 52,75 por ciento del tiempo de navegación, algo más de 18 minutos, los trabajadores visitan páginas Web relacionadas con el ocio. Por otro lado, el 47,25 por ciento del tiempo, algo más de 16 minutos diarios, se destina cuestiones relacionadas con la corporación. Según recoge este estudio, este tipo dedicado a consultar Internet para aspectos no relacionados con el trabajo repercute en unos gastos para la empresa de más de 1.100 euros anuales por cada trabajador.[5]

Websense, Inc. (NASDAQ:WBSN), líder global en software de productividad de seguridad y filtrado web, anunció los resultados de su séptimo estudio anual Web@Work, la encuesta de la compañía realizada por Harris Interactive®. Del 15 al 24 de marzo de 2006, 351 tomadores de decisiones de Estados Unidos que trabajan para organizaciones con por lo menos 100 empleados, al menos uno por ciento de los cuales tiene acceso a internet, fueron entrevistados en línea, y del 16 de marzo al 4 de abril de 2006, 500 empleados de Estados Unidos mayores a 18 años que tienen acceso a Internet en el

trabajo y que laboran para organizaciones con por lo menos 100 empleados fueron encuestados vía telefónica sobre el uso del Web y aplicaciones de software en su lugar de trabajo.

**TIEMPO INVERTIDO**—93 por ciento de los encuestados dijo que pasan por lo menos algo de tiempo accediendo a Internet en el trabajo.

**NAVEGACIÓN PERSONAL**—61 por ciento de los empleados que utilizan una conexión a Internet propiedad de su empresa admitieron que pasan por lo menos algo de tiempo navegando por sitios Web no relacionados con el trabajo durante el día laboral. De aquellos empleados que tienen acceso a sitios Web no relacionados con su trabajo, el tiempo promedio invertido a navegar por Internet en el trabajo es de 12.81 horas por semana, y el tiempo promedio de navegar por sitios Web no relacionados con sus actividades laborales es de 3.06 horas por semana. Esto significa que, en promedio, 24 por ciento de su tiempo dedicado a navegar por Internet no está relacionado con su trabajo.

**TIEMPO INVERTIDO EN SITIOS WEB NO RELACIONADOS CON EL TRABAJO**—es interesante que aún haya discrepancia entre cuánto tiempo creen los tomadores de decisiones IT que los empleados invierten en visitar sitios de Internet no relacionados con el trabajo y el tiempo que dicen los empleados invertir – los tomadores de decisiones IT estiman que sus empleados pasan en promedio 5.7 horas a la semana navegando sitios Web no relacionados con el trabajo, en tanto que los empleados, en promedio, sólo admiten pasar 3.06 horas a la semana visitando sitios no relacionados con el trabajo. [6]

En Estados Unidos el costo por la navegación no productiva asciende a más de 55 billones de dólares y entre 30 por ciento y 40 por ciento de pérdida productiva cada año, según un estudio de Nielsen/NetRatings, Inc.[7]

En estudios realizados en el ICID se comprobó que de 3379 sitios distintos visitados en un trimestre sólo el 48,57% estaban relacionados directamente con el trabajo. Entre los sitios no relacionados con el trabajo más visitados se encuentran los de correo electrónico, descargas de software, chateo, deportes y fotografías. Estos datos confirman

las tendencias mencionadas en cuanto al uso de Internet en las empresas, por lo tanto se puede inferir que las pérdidas de tiempo sean muy similares, pudiéndose fijar en el orden de las 5 horas semanales por usuario.

Dado que la mayoría de los usuarios que poseen acceso en Internet son investigadores, se puede fijar como salario promedio de cada trabajador \$ 400 mensuales. Tomando como base 24 días laborales de 8 horas cada uno. El salario promedio por hora sería de alrededor de \$ 2,10 por hora. A cada trabajador se le estaría pagando \$42 pesos al mes por hacer algo que no está relacionado con el trabajo. Al haber 182 usuarios con permiso de navegación, esa cifra aumenta a \$7644 mensuales y \$91728 anuales, solo en concepto de salarios. La cifra crecería exponencialmente si se pudiera calcular el valor del trabajo dejado de hacer.

Es imprescindible mencionar que estos datos no significan que en el ICID no exista una adecuada política de seguridad informática, muy al contrario se implementa una política rigurosa en este sentido. Lo que sucedía es que hasta la implementación de la aplicación ISAWEB era prácticamente imposible monitorear el acceso a Internet de los usuarios con permiso. La situación ha ido cambiando drásticamente a partir de la implantación del mismo.

Una situación similar a la del ICID antes de implementar la aplicación ISAWEB, o incluso peor, seguramente existe en la mayoría de las instituciones del país con acceso a Internet.

Ante estos resultados, queda patente la necesidad aún existente de que las empresas establezcan mecanismos de control para un uso eficiente y correcto de Internet como herramienta de productividad.

## VI. Conclusiones.

Para Cuba el desarrollo de la Informática es una prioridad. El país realiza ingentes esfuerzos para que en un corto plazo la informática se convierta en una fuente generadora de recursos, tal como lo es actualmente el Polo Científico. Hoy no se puede hablar de Informática sin hablar de la Red de Redes, por lo tanto y a pesar del bloqueo, Cuba continuará mejorando las condiciones de conexión y la cantidad de usuarios. No obstante debe primar el uso racional y adecuado a nuestras normas morales de Internet, softwares como ISAWEB son de vital importancia para poder lograr estos objetivos.

En Cuba solo la empresa Segurmática, comercializa un analizador de accesos a Internet realizados a través de un servidor Proxy, llamado: **AAInternet**. Este software no llena los requisitos de seguridad del ICID, ni aprovecha las capacidades técnicas instaladas en el centro.

AAInternet tiene una gran cantidad de limitantes:

- Es una aplicación Windows que debe ser instalada en una Terminal, solo puede trabajar con ella quien esté en esa Terminal.
- Hay que copiar hacia la máquina donde esté instalada la aplicación todos los Logs generados por el servidor Proxy.
- No se almacenan los registros en base de datos para consultas posteriores.
- No se establecen Jerarquías para acceso a la información de tráfico. Una sola persona es la que maneja ese gran volumen de información.

ISAWEB por su parte, soluciona todos estos inconvenientes:

- Al ser una aplicación Web puede ser consultada por cualquier usuario desde cualquier Terminal de la red.
- Las bases de datos son centralizadas, y el proceso de inserción de datos es independiente a la aplicación principal.
- Se establece una jerarquía que permite que la labor de seguridad informática se descentralice entre todos los directivos, e incluso participe el trabajador.

## ***VII. Recomendaciones.***

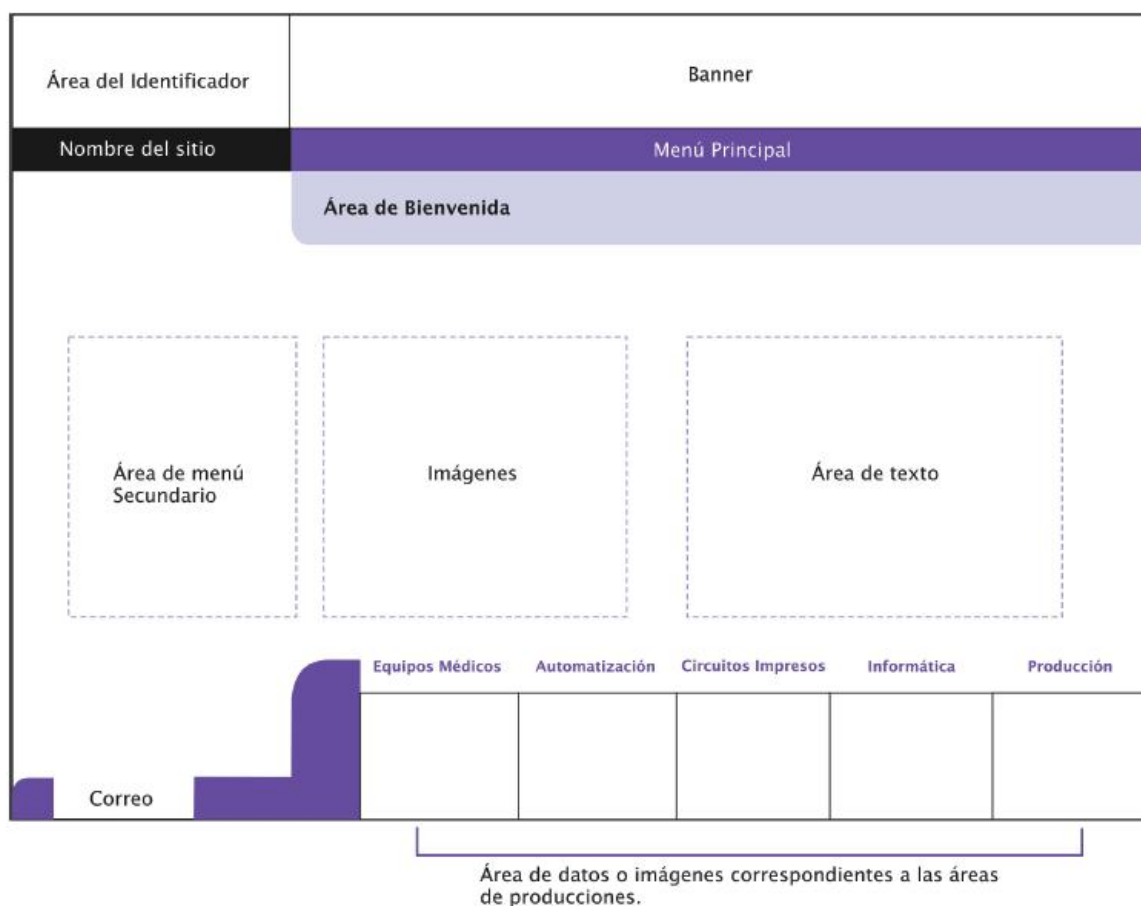
- 1) Generalizar el uso del ISAWEB en aquellas instituciones que tengan la necesidad de controlar su acceso a Internet, donde existan las condiciones técnicas o se puedan crear.
- 2) Trabajar para que ISAWEB permita elaborar información a partir de los Logs generados por los servidores Proxy de más amplia utilización en el país y no solo a partir del Isa Server.

## VIII. Bibliografía.

- [1]. Anónimo, "Cuba en la Cumbre Mundial sobre La Sociedad de la Información. Informatización en Cuba". [www.cubaminrex.cu/Sociedad\\_Informacion/Cifras.htm](http://www.cubaminrex.cu/Sociedad_Informacion/Cifras.htm).
- [2]. Santiago Masetti, "La verdad sobre Internet y los 'disidentes' cubanos". [www.trabajadores.cubaweb.cu/fijos/cuba/cuba-en-el-kolimador/laverdad.htm](http://www.trabajadores.cubaweb.cu/fijos/cuba/cuba-en-el-kolimador/laverdad.htm) (19-07-2004)
- [3]. Tesis de diploma: David González Pérez, Evid dry Valdés Peña (ISDI). "Identidad Visual Institucional, ICID". (2005)
- [4]. Otniel Barrera Palenzuela, "Aplicaciones ASP.NET vinculadas con Active Directory mediante el protocolo LDAP". Artículo en vías de publicarse. (2005)
- [5]. Encarna González, "Los trabajadores pasan en Internet más de 30 minutos diarios en el trabajo". ( 27/06/2006 ).  
<http://www.idg.es/pcworldtech/mostrarArticulo.asp?id=177386&seccion=seguridad>  
PCWorld Profesional.
- [6] Anónimo. "WEBSense PRESENTA ESTUDIO: VER CONTENIDO PARA ADULTOS EN EL TRABAJO ES UNA DE LAS PRINCIPALES PREOCUPACIONES PARA PONER EN RIESGO EL EMPLEO". ( Martes 13 de Junio del 2006 ).  
<http://www.chiletech.com/link.cgi/Empresas/W/WEBSense/17152>
- [7] Julián Sánchez." Empleados abusan de conexión a internet".( Domingo 04 de diciembre de 2005 ).  
<http://www.eluniversal.com.mx/primera/25687.html>  
El Universal Online.

## IX.Anexos

### Anexo 1: Maqueta Web del ICID.



 <b>ICID</b> Instituto Central de Investigación Digital	Banner					
<a href="http://www.icid.edu.cu">www.icid.edu.cu</a>	<a href="#">Productos</a>	<a href="#">Historia</a>	<a href="#">Seguridad</a>	<a href="#">Medios Básicos</a>	<a href="#">Balance</a>	<a href="#">Eventos</a>
Bienvenidos a la página del ICID						
<ul style="list-style-type: none"> <li>Nuevas</li> <li>Biblioteca</li> <li>Directorio</li> <li>Calidad</li> <li>Superación</li> <li>Vida Interna</li> </ul>	<div data-bbox="651 645 853 891" data-label="Image">  </div> <div data-bbox="949 649 1316 772" data-label="Text"> <p>El Desfibrilador es un equipo para la medicina de alta tecnología digital. desarrollado por el ICID.</p> <p>Su empleo en los servicios de emergencia le facilita a los paramédicos el diagnóstico de los signos vitales del paciente con un elevado grado de rapidez.</p> </div>					
<a href="#">E-Mail</a>	<a href="#">Equipos Médicos</a> 	<a href="#">Automatización</a> 	<a href="#">Circuitos Impresos</a> 	<a href="#">Informática</a> 	<a href="#">Producción</a> 	



## Anexo 2: Elementos Componentes de los Logs del Isa Server

Field position	Descriptive name (field name)	Description
1	Client IP (c-ip)	The Internet Protocol (IP) address of the requesting client.
2	Client user name (cs-username)	Account of the user making the request. If ISA Server Access Control is not being used, ISA Server uses <i>anonymous</i> .
3	Client agent (c-agent)*	The client application type sent by the client in the Hypertext Transfer Protocol (HTTP) header. When ISA Server is actively caching, the client agent is <i>ISA Server</i> . For Firewall service, this field includes information about the client's operating system. Click here to see a table of possible values.
4	Authentication status (sc-authenticated)*	Indicates whether or not client has been authenticated with ISA Server. Possible values are <i>Y</i> and <i>N</i> .
5	Date (date)	The date that the logged event occurred.
6	Time (time)	The time that the logged event occurred. In W3C format, this is in Greenwich mean time.
7	Service name (s-svcname)*	The name of the service that is logged. <ul style="list-style-type: none"> <li>• <b>w3proxy</b> indicates outgoing Web requests to the Web Proxy service.</li> <li>• <b>fwsrv</b> indicates Firewall service.</li> <li>• <b>w3reverseproxy</b> indicates incoming Web requests to the Web Proxy service.</li> </ul>
8	Proxy name (s-computername)*	The name of the computer running ISA Server. This is the computer name that is assigned in Windows 2000.
9	Referring server	If ISA Server is used upstream in a chained configuration, this

Field position	Descriptive name (field name)	Description
	name (cs-referred)*	indicates the server name of the downstream server that sent the request.
10	Destination name (r-host)	The domain name for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was retrieved from the Web Proxy server cache and not from the destination.
11	Destination IP (r-ip)	The network IP address for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was sourced from the Web Proxy server cache and not from the destination. One exception is negative caching. In that case, this field indicates a destination IP address for which a negative-cached object was returned.
12	Destination port (r-port)*	The reserved port number on the remote computer that provides service to the current connection. This is used by the client application initiating the request.
13	Processing time (time-taken)*	This indicates the total time, in milliseconds, that is needed by ISA Server to process the current connection. It measures elapsed server time from the time that the server first received the request to the time when final processing occurred on the server—when results were returned to the client and the connection was closed. For cache requests that were processed through the Web Proxy service, <i>processing time</i> measures the elapsed server time needed to fully process a client request and return an object from the server cache to the client.
14	Bytes sent (cs-bytes)	The number of bytes sent from the internal client to the external server during the current connection. A hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were sent to the remote computer.
15	Bytes received (sc-bytes)	The number of bytes sent from the external computer and received by the client during the current connection. A hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were received

Field position	Descriptive name (field name)	Description
		from the external computer.
16	Protocol name (cs-protocol)	Specifies the application protocol used for the connection. Common values are HTTP, File Transfer Protocol (FTP), Gopher, and Secure Hypertext Transfer Protocol (HTTPS). For Firewall service, the port number is also logged.
17	Transport (cs-transport)*	Specifies the transport protocol used for the connection. Common values are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
18	Operation (s-operation)*	Specifies the application method used. For Web Proxy, common values are GET, PUT, POST, and HEAD. For Firewall service, common values are CONNECT, BIND, SEND, RECEIVE, GHBN (GetHostByName), and GHBA (GetHostByAddress).
19	Object name (cs-uri)	For the Web Proxy service, this field shows the contents of the URL request. This field applies only to the Web Proxy service log.
20	Object MIME (cs-mime-type)*	The Multipurpose Internet Mail Extensions (MIME) type for the current object. This field may also contain a hyphen (-) to indicate that this field is not used or that a valid MIME type was not defined or supported by the remote computer. This field applies only to the Web Proxy service log.
21	Object source (s-object-source)	Indicates the source that was used to retrieve the current object. This field applies only to the Web Proxy service log. <a href="#">Click here to see a table of some possible values.</a>
22	Result code (sc-status)	This field can be used to indicate: <ul style="list-style-type: none"> <li>For values less than 100, a Windows (Win32) error code</li> <li>For values between 100 and 1,000, an HTTP status code</li> <li>For values between 10,000 and 11,004, a Winsock error code</li> </ul> <a href="#">Click here to see a table of some possible values.</a>
23	Cache info (s-cache-info)**	This number reflects the cache status of the object, which indicates why the object was or was not cached. This field applies only to the Web Proxy service log. <a href="#">Click here to see a table of some possible</a>

Field position	Descriptive name (field name)	Description
		values.
24	Rule #1 (rule#1)**	<p>This reflects the rule that either allowed or denied access to the request, as follows:</p> <ul style="list-style-type: none"> <li>• If an outgoing request is allowed, this field reflects the protocol rule that allowed the request.</li> <li>• If an outgoing request is denied by a protocol rule, this field reflects the protocol rule.</li> <li>• If an outgoing request is denied by a site and content rule, this field reflects the protocol rule that would have allowed the request.</li> <li>• If an incoming request was denied, this field reflects the Web publishing or server publishing rule that denied the request.</li> <li>• If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case, the field is empty.</li> </ul>
25	Rule #2 (rule#2)**	<p>This reflects the second rule that either allowed or denied access to the request.</p> <ul style="list-style-type: none"> <li>• If an outgoing request is allowed, this field reflects the site and content rule that allowed the request.</li> <li>• If an outgoing request is denied by a site and content rule, this field reflects the site and content rule that denied the request.</li> <li>• If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case, the field is empty.</li> </ul>
26	Session ID (sessionid)**	<p>This identifies a session's connections. For Firewall clients, each process that connects through the Firewall service initiates a session. For secure network address translation (SecureNAT) clients, a single session is opened for all the connections that originate from the same IP address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.</p>
27	Connection ID (connectionid)**	<p>This identifies entries that belong to the same socket. Outbound TCP usually has two entries for each connection: when the connection is established and when the connection is terminated. UDP usually has</p>

Field position	Descriptive name (field name)	Description
		two entries for each remote address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.

\* Estos campos no son relevantes para la aplicación ISAWEB.

\*\* Los campos 23, 24, 25, 26, 27 no se ejecutan en el centro.

**XVI Forum de Ciencia y Técnica**  
**Relación de Autores, Coautores y Colaboradores**  
**ISAWEB. Monitoreo de Tráfico en Internet.**

<b>Nombre</b>	<b>Categoría</b>	<b>%</b>	<b>Institución</b>	<b>Firma</b>
Otniel Barrera Palenzuela	Autor Principal	65	ICID	
Misleydi Alonso Marrero	Coautor	20	ICID	
Deiny García Pérez	Coautor	15	ICID	
Ernesto Rafael Prieto	Colaborador		ICID	
Alejandro Fernández González	Colaborador		ICID	

La Habana, Junio 28 de 2006