Herramientas de Monitorización del trabajo en Red

L. Martínez, F. Mata, M. Pérez, P. Sanchez
Universidad de Jaén, Dept. Informática,
Jaén, España, 23071
martin@ujaen.es, *fmata@ujaen.es*, *lperez@ujaen.es*, *pedroj@ujaen.es*

ABSTRACT

With the incorporation of the Information Technologies to the sectors of the society and therefore also to the managerial sector, a world of new business opportunities has opened up but at the same time accompanied by some problems arisen soon after the use of these. Internet, the electronic mail, the broadband, etc, they are services and benefits that very utilized they allow to obtain a series of competitive advantages regarding the rest of organizations but that if they are not controlled they can become against the own company. In this contribution we present a series of tools that allow to control the circulation of the information in a net, as much to local level as toward the exterior, trying to assure that the resources of the organization are used appropriately, avoiding the possible problems that can arise of their wrong use.

Keywords: Security, Internet, Sniffer, Firewalls, Cookies, Keyword3, Keyword4, Keyword5.

RESUMEN

Con la incorporación de la Tecnologías de la Información y las Comunicaciones a todos los sectores de la sociedad y por tanto también al sector empresarial, se ha abierto un mundo de nuevas oportunidades empresariales pero a la vez acompañado de algunos problemas surgidos a raiz de la utilización de éstas. Internet, el correo electrónico, la banda ancha , etc, son servicios y prestaciones que bien utilizados permiten obtener una serie de ventajas competitivas respecto al resto de organizaciones pero que si no son controlados pueden volverse en contra de la propia empresa. En esta contribución presentamos una serie de herramientas que permiten controlar la circulación de la información en una red, tanto a nivel local como hacia el exterior, intentando asegurar que los recursos propios de la organización se utilizan adecuadamente, evitando los posibles problemas que pudiesen surgir de su mal uso.

Palabras claves: Seguridad, Internet, Sniffer, Cortafuegos, Cookies..

Este trabajo esta soportado por el Proyecto de Investigación TIC2002-03348.

INTRODUCCION

El uso e implantación de las redes de ordenadores en las empresas ha producido profundos cambios en la organización empresarial, en la mayoría de los casos, han sido positivos. Sin embargo, la infraestructura distribuida que proporcionan las redes de ordenadores y la cada vez creciente posibilidad de conexión directa a Internet desde el puesto de trabajo, también están dando lugar a una creciente preocupación por parte de los empresarios, jefes de personal, administradores de red, etc., del uso que los empleados hacen de estos servicios en su horario laboral.

Basta con revisar diversos datos publicados por importantes medios, organismos y empresas dedicadas al estudio del uso de Internet, tales como:

- En el año 2002 el 60,7% de los empleados estudiados dicen haber visitado páginas web para uso personal en horario laboral [9]**.**
- La primera razón de pérdida de productividad de los empleados en su trabajo es debido al uso de Internet.
- Uno de los términos más utilizados con mayor frecuencia en los buscadores es "*sexo*" [1].
- El dominio más visitado en EE.UU. por los trabajadores en horario de trabajo es el portal horizontal de servicios **Iwon** con una media de 16 visitas por trabajador al mes. (Publicado en BUSINESS 2.0)
- Se encontraron instalados programas de intercambio de temas musicales en más del 30% de los PCs investigados [2].
- El 32,6% de los trabajadores navegan por Internet sin un objetivo específico. (Emarketer)
- El 36% de los empleados navegan por sitios de información en el trabajo más que en su propia casa, llegando a dedicar un 68% más de tiempo
- Etc.

Todas estos datos indican que en el mejor de los casos, estos nuevos hábitos *sólo* hacen perder horas de trabajo y por tanto dinero a la empresa. Otros casos son la posibilidad de abrir agujeros de seguridad en el sistema de la empresa debidos a virus, bug de programas o accesos a sitios que intenten romper la seguridad de las máquinas que se conectan a sus servidores. También pueden crearse problemas legales a la empresa si se utilizan sus recursos para compartir archivos ilegales (*Software de intercambio de ficheros musicales, vídeos, etc).*

Por lo tanto parece claro que ante la forzosa implantación de las nuevas tecnologías en la empresa para mejorar los procesos de negocio, puede ser necesario al mismo tiempo implantar, en caso de que existan, distintas herramientas que permitan controlar o limitar el uso de los servicios, tanto de las redes de ordenadores en general como de Internet en particular.

A lo largo de esta contribución haremos una revisión general de las distintas posibilidades que nos proporciona la

tecnología para implantar límites y controles al uso de Internet y sus servicios.

the proceedings a high quality appearance, we ask you to make your paper look as much like this document as possible.

1 PREELIMINARES

Para entender las distintas posibilidades u opciones que puede implantar una empresa para vigilar el uso de sus recursos e infraestructuras basadas en redes de ordenadores en primer lugar repasaremos una serie de conceptos básicos para la compresión de estas herramientas.

En primer lugar un concepto fundamental es el de *Administrador de Sistemas* o SYSOP o ROOT. Que es la persona encargada de la gestión y administración de la Red de Ordenadores. Sobre él recae la responsabilidad de que el sistema funcione correctamente y proporcione los servicios para los que se implantó en la empresa. Además debido a los datos anteriores será el encargado de diseñar las políticas de control de uso de la red y de limitación de servicios en la misma. Por tanto, nos damos cuenta que juega el *role central* en el tema que nos ocupa de vigilancia del uso de la red de ordenadores por parte de los empleados. Por lo cuál debería quedar claramente delimitado en su contrato si él es el responsable de las prácticas de vigilancia o lo es la empresa para la que trabaja.

Una vez que ya sabemos a quién debe dirigirse el responsable de la empresa para implantar políticas de vigilancia y control, vamos a hacer un repaso de las distintas opciones con las que se encuentra un *Administrador de Sistemas*.

En primer lugar vamos a visualizar el esquema de conexión de una intranet corporativa de una empresa a hacia Internet (*Figura* **1**), para así entender mejor posteriormente el uso de las herramientas de control y limitación de acceso a Internet desde la intranet empresarial.

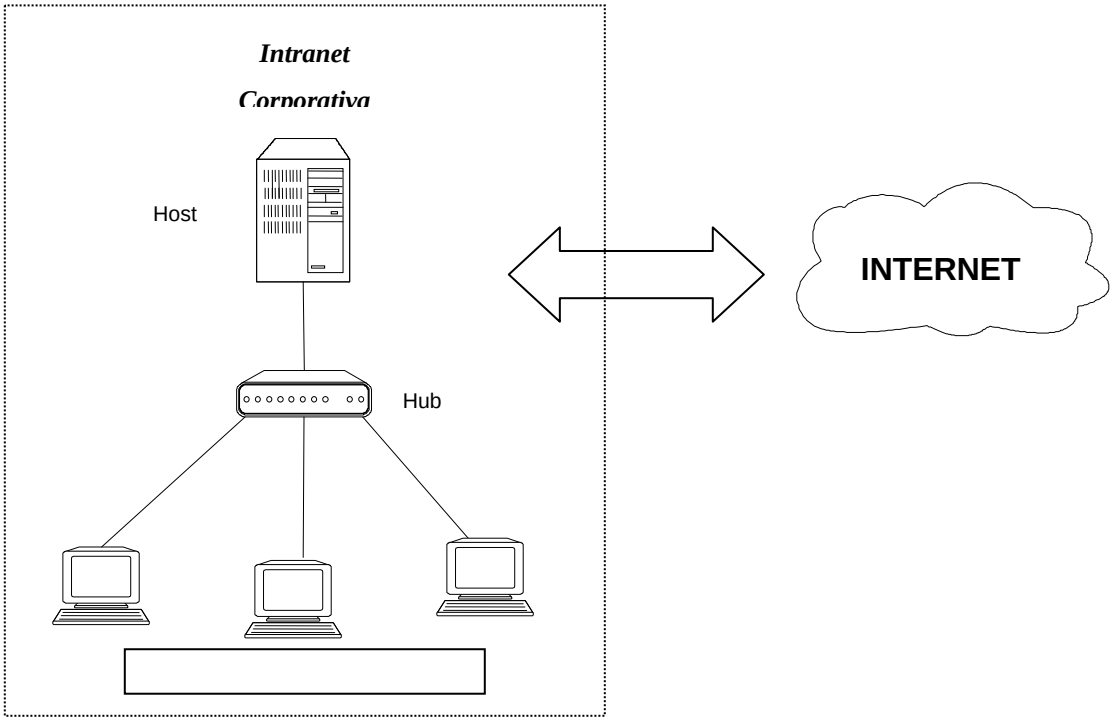


Figura 1. *Esquema de conexión de una Intranet Corporativa a Internet*

Conocidos el responsable de la gestión, administración y buen uso de la red y el esquema más simple de conexión que en un principio se utiliza desde las empresas para conectarse a Internet. Vamos a ver las distintas soluciones que puede utilizar el *Administrador de la Red* para que los usuarios de la misma (empleados) hagan un buen uso de ella.

2 HERRAMIENTAS DE CONTROL DE LA RED

Como vimos en la Introducción el acceso a Internet desde las empresas es cada vez más común debido a los servicios y ventajas que presenta con respecto a las necesidades de las empresas, pero al mismo tiempo dicho acceso hace que pueda existir cierta pérdida de productividad por parte de los empleados que acceden a la Red. Para evitar el mal uso del acceso a Internet por parte de los empleados el *Administrador* de la red empresarial puede utilizar distintas herramientas, tales como [8]:

- Firewall o Cortafuegos
- Proxy
- Programas de monitorización de la red
- Sniffers
- Cookies

A continuación vamos a ver cómo funcionan y que tipo de información obtienen cada una de estas herramientas:

3. 1 Cortafuegos

Un *Cortafuegos* es una herramienta que se utiliza fundamentalmente para proteger la red corporativa de la empresa de posibles ataques exteriores que podrían comprometer la seguridad interna de la compañía. [3]

El fundamento del *Cortafuegos* es actuar de puente entre la red local a proteger y la red más amplia a la que se quiere conectar (Internet), de forma que la circulación de información entre ambas redes esté controlada. Un esquema simple de implantación de un *Cortafuegos* podemos verlo en la Figura 2:

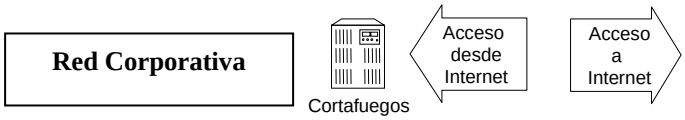


Figura 2. *Instalación de un Cortafuegos*

Por tanto, lo que hace un *Cortafuegos* es establecer una serie de **filtros y controles** de las direcciones de Internet a las que se puede acceder desde nuestra red corporativa y qué direcciones pueden acceder desde Internet a nuestra red [5,10]. El *Cortafuegos* creará informes sobre el intento de accesos a o de direcciones

prohibidas para mantener informado al *Administrador* de posibles problemas de seguridad o buen uso de la red. En estos informes se indica que ordenador es el que intenta saltarse un control o filtro del *Cortafuegos*. A continuación vemos distintos tipos de información que se puede obtener del uso de un *Cortafuegos:*

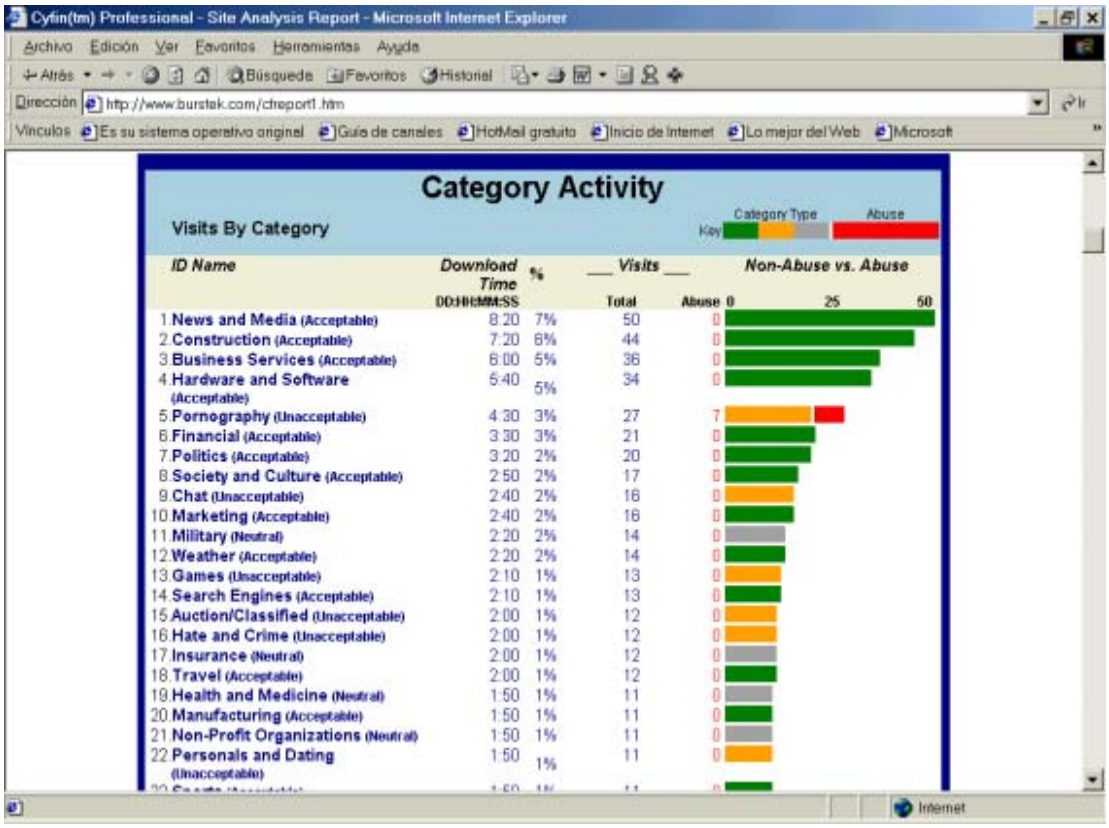


Figura 3. *Informe de un Cortafuegos*

Una de las mayores ventajas que presenta el uso de *Cortafuegos* es su flexibilidad y facilidad de configuración. Por lo que, el *Administrador* puede añadir, modificar o eliminar controles y/o filtros del *Cortafuegos*. Las decisiones de qué controles o filtros poner en el *Cortafuegos* se tomarán en un principio de forma general de acuerdo a información de seguridad que reciben todos los *Administradores* y con el tiempo la configuración particular de cada empresa se hará atendiendo a la información que generalmente se obtiene a través de los informes generados por el propio *Cortafuegos* o bien a través de información obtenida por otros programas que veremos a continuación cómo los *proxy*, *sniffers* y *programas de monitorización de la red*.

3.2 Proxy.

Un *Proxy* (Intermediario en español), es un programa que en función de la petición de un usuario decide abrir o no una conexión con el servidor de destino y reenviar los datos según los recibe [4]. El uso de un *proxy* no es transparente, en cuanto que requiere que los programas cliente lo reconozcan y le envíen la información a él en lugar del servidor de destino.

El *proxy* puede realizar diversas funciones muy útiles. Por ejemplo, en cuanto al tema que nos interesa en esta contribución un "*proxy* http" puede mantener una caché de las páginas más visitadas de forma que el *Administrador* puede conocer cuáles son los accesos más usuales que se hacen desde dentro de la red de la empresa. Un ejemplo de la información obtenida podría ser la siguiente:

#Version: 1.0
#Date: 12-Jan-1996 00:00:00
#Fields: time cs-method cs-uri
00:34:23 GET /www.xxx.com/bar.html
12:21:16 GET /www.sex.com/buy.html
12:45:52 GET /tradenews.com/news.html
12:57:34 GET /travelling.com/index.html

Es posible construir *Cortafuegos* a base de aunar *proxies* para cada servicio de acceso a Internet.

3.3 Programas de Monitorización.

El significado de monitorización es el de visualizar. Por tanto cuando hablamos de programas de monitorización de la red, nos estamos refiriendo a programas que son capaces de visualizar la información que viaja a través de la misma. Inicialmente los *Administradores* utilizaban este tipo de programas para detectar posibles problemas de funcionamiento en la red, pero cada vez es más habitual la inclusión de herramientas que permitan vigilar el uso de los servicios de acceso a Internet por parte de los usuarios de la red. Hasta el punto de que podemos asegurar que hoy en día, son las herramientas más utilizadas dentro de las empresas para controlar a los empleados en el uso que hacen de Internet [8].

Un programa de monitorización es capaz de devolvernos informes personalizados de cada usuario de la red con la siguiente información:

- Detectar abusos o accesos no autorizados.
- Páginas de Internet visitadas.
- Programas utilizados en el ordenador por parte del empleado.
- Claves de acceso utilizadas por el empleado.
- Copia de la información enviada a través de los servicios que hayamos configurado, normalmente *e-mail, chat y mensajería instantánea*
- Control de actividad en casos de tele-trabajo
- Visualización de pantallas de cada ordenador con el fin de ver que información está mostrando cada cierto tiempo.
- Recuperar dirección de páginas Web visitadas en Internet a partir de una palabra clave, fecha, etc.

- Etc.

Podemos ver que este tipo de programas son capaces de *escudriñar* con gran facilidad toda la información que genera un usuario de nuestra red y mostrárnoslos en distintos formatos (HTML, hoja de cálculo, texto plano, etc.). Por tanto, el control sobre la actividad realizadas por nuestros empleadas queda totalmente identificada sin el menor género de duda. A continuación incluyo informes generados por un programa de este tipo, tanto en formato HTML (Figura 4):

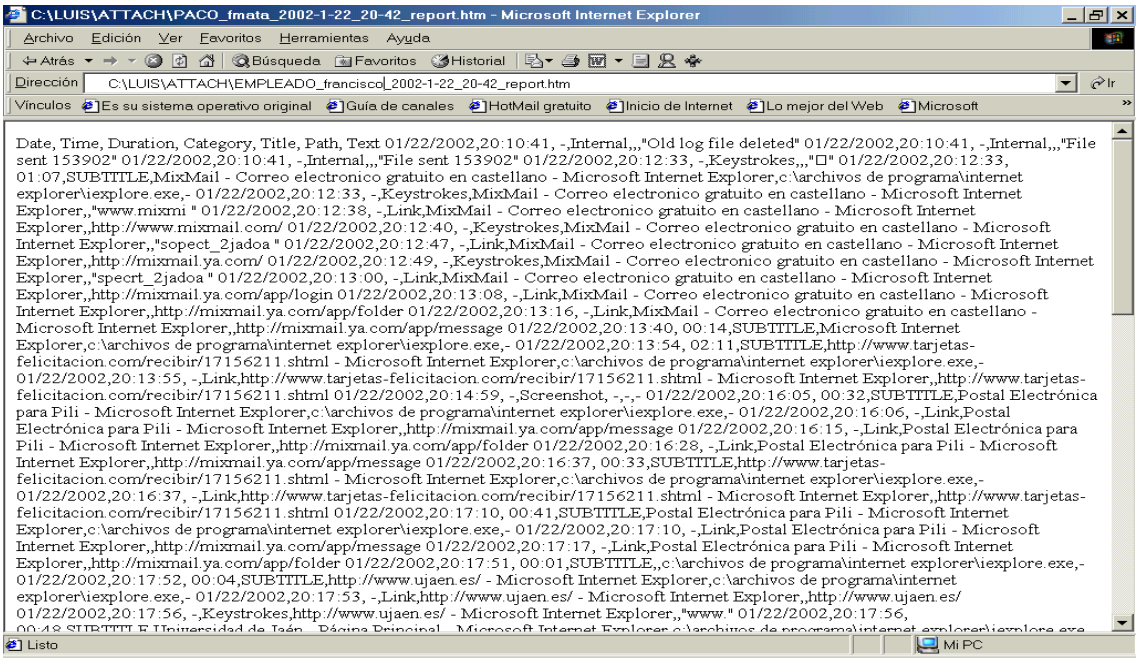
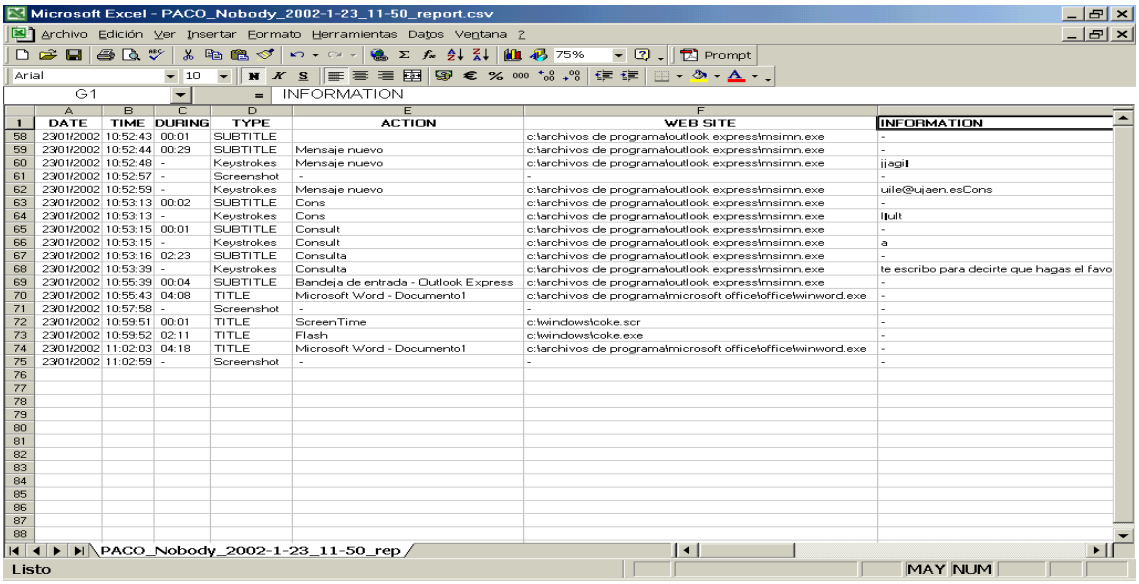


Figura 4. *Informe del EMPLEADO francisco en formato HTML*

como de hoja de cálculo (Figura 5):



	A	B	C	D	E	F	
1	DATE	TIME	DURING	TYPE	ACTION	WEB SITE	INFORMATION
58	23/01/2002	10:52:43	00:01	SUBTITLE		c:\archivos de programa\outlook express\msimn.exe	-
59	23/01/2002	10:52:44	00:29	SUBTITLE	Mensaje nuevo	c:\archivos de programa\outlook express\msimn.exe	-
60	23/01/2002	10:52:48	-	Keystrokes	Mensaje nuevo	c:\archivos de programa\outlook express\msimn.exe	jiagil
61	23/01/2002	10:52:57	-	Screenshot	-	-	-
62	23/01/2002	10:52:59	-	Keystrokes	Mensaje nuevo	c:\archivos de programa\outlook express\msimn.exe	uile@ujaen.esCons
63	23/01/2002	10:53:13	00:02	SUBTITLE	Cons	c:\archivos de programa\outlook express\msimn.exe	-
64	23/01/2002	10:53:13	-	Keystrokes	Cons	c:\archivos de programa\outlook express\msimn.exe	Ilult
65	23/01/2002	10:53:15	00:01	SUBTITLE	Consult	c:\archivos de programa\outlook express\msimn.exe	-
66	23/01/2002	10:53:15	-	Keystrokes	Consult	c:\archivos de programa\outlook express\msimn.exe	a
67	23/01/2002	10:53:16	02:23	SUBTITLE	Consulta	c:\archivos de programa\outlook express\msimn.exe	-
68	23/01/2002	10:53:39	-	Keystrokes	Consulta	c:\archivos de programa\outlook express\msimn.exe	te escribo para decirte que hagas el favo
69	23/01/2002	10:55:39	00:04	SUBTITLE	Bandeja de entrada - Outlook Express	c:\archivos de programa\outlook express\msimn.exe	-
70	23/01/2002	10:55:43	04:08	TITLE	Microsoft Word - Documento1	c:\archivos de programa\microsoft office\office\winword.exe	-
71	23/01/2002	10:57:58	-	Screenshot	-	-	-
72	23/01/2002	10:59:51	00:01	TITLE	ScreenTime	c:\windows\coke.scr	-
73	23/01/2002	10:59:52	02:11	TITLE	Flash	c:\windows\coke.exe	-
74	23/01/2002	11:02:03	04:18	TITLE	Microsoft Word - Documento1	c:\archivos de programa\microsoft office\office\winword.exe	-
75	23/01/2002	11:02:59	-	Screenshot	-	-	-

Figura 5. *Informe del EMPLEADO PACO en formato HTML*

Estos programas violan seriamente la intimidad de los empleados, especialmente cuando el trabajador no ha sido informado de que su labor está siendo vigilada. Hay que tener en cuenta que estos programas se instalan en cada ordenador a vigilar y se configura para que se envíen los informes al *Administrador* o al personal encargado de controlar la productividad vía email. Aunque, estos programas se encuentren instalados en el ordenador del empleado a vigilar suelen ser indetectables por él, debido a que se utiliza una instalación especial que oculta la existencia de dichos programas.

3.4 Sniffers.

Los *sniffers* son programas muy similares a los que acabamos de ver anteriormente, aunque presentan la particularidad de que suelen ser menos amigables y por tanto el *Administrador* debe tener conocimientos claros de qué información quiere obtener mediante el uso del *sniffer* [7].

Un *sniffer* lo que hace es pinchar la red de comunicación por la que viaja la información y hacer una copia de la misma [4]. Este tipo de herramienta se ha de configurar para que vigile un servicio específico sobre un ordenador determinado. Como he comentado anteriormente esta configuración no es sencilla. Una ventaja de los *sniffers* sobre los programas de monitorización es que no hay que instalar nada en el ordenador que queremos vigilar ya que como pinchamos la red con tener acceso a ella no hace falta acceder al ordenador a vigilar.

A continuación podemos ver el tipo de información que puede obtener un *Sniffer*, cuando un *Administrador* lo activa en su red corporativa:

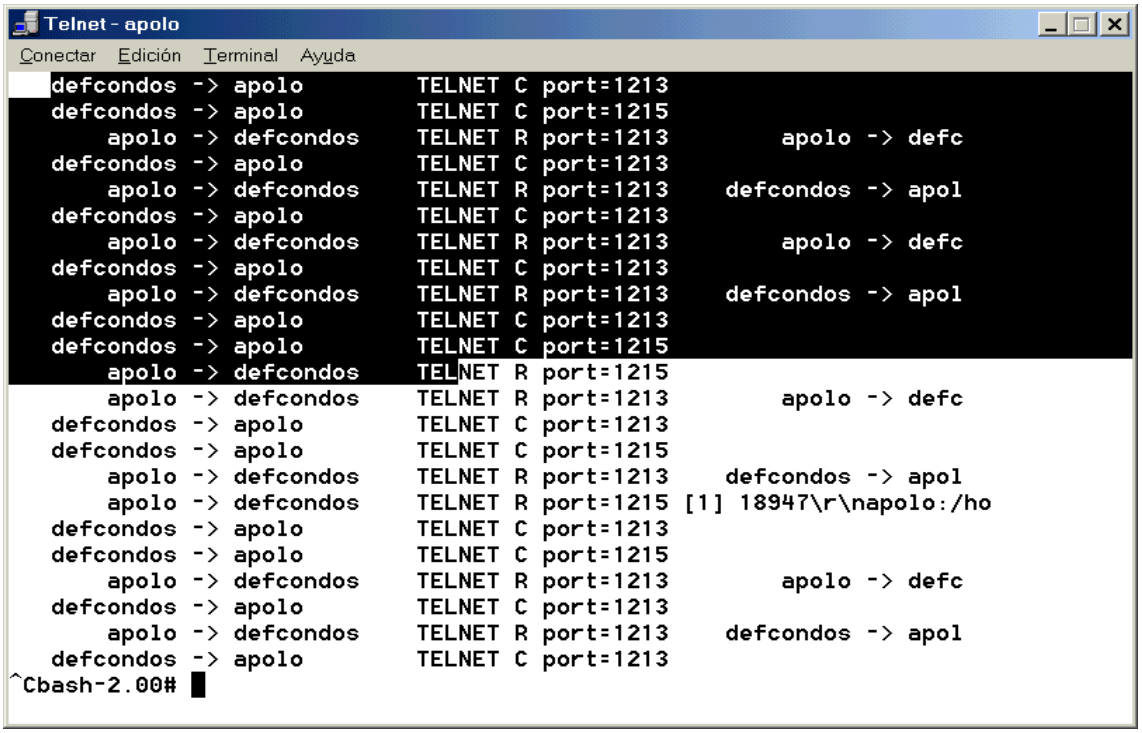


Figura 6. *Información de un sniffer*

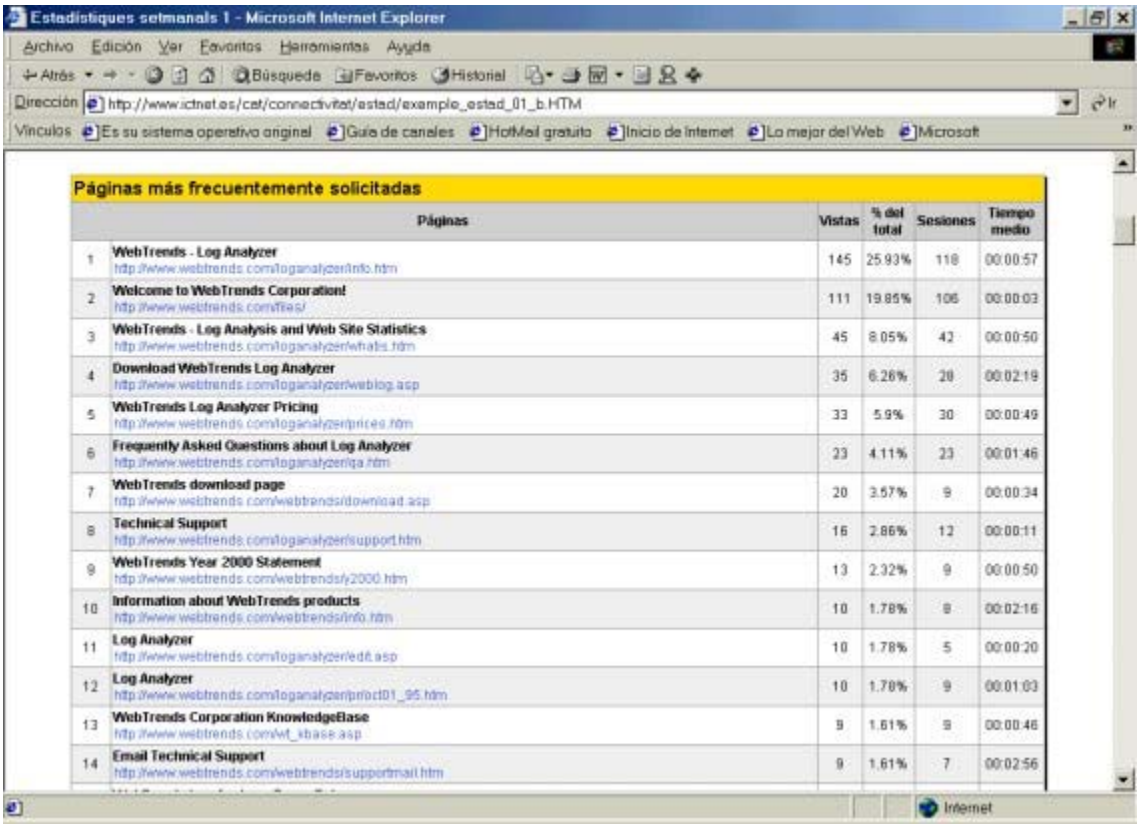
3.5 Cookies

Otro tipo de herramienta que se puede utilizar para vigilar la utilización del uso de Internet por parte de los usuarios son las conocidas *Cookies*. Una *Cookie* no es mas que es una pequeña **cadena de texto** que se almacena en el disco duro de su PC, a menos que lo borre (o caduque) [6]. No es un programa informático.

Las C*ookies* tienen dos funciones. La primera es mantener el estado de una aplicación. Básicamente, esto significa que cada vez que regresa a una Site, Usted empieza donde la había dejado. Por ejemplo, sólo necesita registrarse una vez para entrar en una Site. La segunda función es **rastrear su camino a través de la Web**. Esta segunda función permite conocer cuáles son los hábitos del usuario a la hora de navegar por la red, ya que la *Cookie* permite que se almacene los lugares visitados por el usuario y cuáles son las acciones que ha llevado dicho usuario en cada lugar de los que ha accedido.

Cara al *Administrador* de redes el mayor problema que presentan las *Cookies* es que los navegadores permiten configurar al usuario la posibilidad de aceptar o no que se instale en su disco la *Cookie*, por lo que en caso de rechazar la instalación el A*dministrador* no podrá obtener ninguna información sobre el usuario.

Un ejemplo de la información que se puede obtener a través de una *Cookie* puede ser la siguiente:



	Páginas	Vistas	% del total	Sesiones	Tiempo medio
1	WebTrends - Log Analyzer http://www.webtrends.com/loganalyzer/info.htm	145	25.93%	118	00:00:57
2	Welcome to WebTrends Corporation! http://www.webtrends.com/files/	111	19.85%	106	00:00:03
3	WebTrends - Log Analysis and Web Site Statistics http://www.webtrends.com/loganalyzer/whatis.htm	45	8.05%	42	00:00:50
4	Download WebTrends Log Analyzer http://www.webtrends.com/loganalyzer/weblog.asp	35	6.26%	28	00:02:19
5	WebTrends Log Analyzer Pricing http://www.webtrends.com/loganalyzer/prices.htm	33	5.9%	30	00:00:49
6	Frequently Asked Questions about Log Analyzer http://www.webtrends.com/loganalyzer/qa.htm	23	4.11%	23	00:01:46
7	WebTrends download page http://www.webtrends.com/webtrends/download.asp	20	3.57%	9	00:00:34
8	Technical Support http://www.webtrends.com/loganalyzer/support.htm	16	2.86%	12	00:00:11
9	WebTrends Year 2000 Statement http://www.webtrends.com/webtrends/y2000.htm	13	2.32%	9	00:00:50
10	Information about WebTrends products http://www.webtrends.com/webtrends/info.htm	10	1.78%	8	00:02:16
11	Log Analyzer http://www.webtrends.com/loganalyzer/edit.asp	10	1.78%	5	00:00:20
12	Log Analyzer http://www.webtrends.com/loganalyzer/prod01_95.htm	10	1.78%	9	00:01:03
13	WebTrends Corporation KnowledgeBase http://www.webtrends.com/wt_kbase.asp	9	1.61%	8	00:00:46
14	Email Technical Support http://www.webtrends.com/webtrends/supportmail.htm	9	1.61%	7	00:02:56

Figura 7. *Información de una Cookie*

4 CONCLUSIONES

El uso de Internet desde las empresas ha proporcionado la posibilidad a los empleados de las mismas de poder acceder a gran cantidad de servicios. Estos servicios en gran cantidad de ocasiones no están relacionados con el trabajo que deben llevar a cabo en su puesto lo que ocasiona una pérdida de productividad que se terminará reflejando en los resultados que deben alcanzar dichos empleados.

Para paliar esta pérdida de productividad y evitar posibles problemas de seguridad en la red empresarial se han desarrollado una serie de herramientas que permiten desde la creación de filtros y controles de acceso a los servicios de la Red hasta la copia de toda la información, que se origina en los procesos de comunicación de los distintos servicios de red, realizados por un empleado.

Parece lógico que la empresa vele por la seguridad de su red y por sus intereses empresariales, pero dónde está el límite que separa la preocupación de velar por los intereses empresariales de entrometerse en la privacidad del empleado. Esa es la cuestión principal a la hora de utilizar las herramientas presentadas en esta contribución, ya que una permisividad total al empresario a la hora de vigilar a sus empleados puede ser tan contraproducente como una permisividad total al empleado en el uso de los servicios de red.

BIBLIGRAFIA

1. Businnes 2.0, http://www.business2.com.
2. Emarketer, http://www.emarketer.com.
3. Ferrer D. Firewalls: La primera línea de defensa. http://www.kriptopolis.com, (Marzo 2003).
4. Fisch, E. *Secure computers and networks: analisis, design and implementation.* CRC Press, 2000.
5. Idg. Anonimato, cortafuegos, filtros de contenidos, motores de búsqueda. IWorld, (Octubre 2000).
6. Jenmings C. *La centésima ventana: guía para proteger la seguridad y la privacidad en la era Internet.* Deusto, 2000.
7. Panda Software. Sniffers y segmentación de la red local. . http://www.criptonomicom.com/documentos/2002/07012002.html.
8. Rodao M. Piratas Cibernéticos: Cyberwars, Seguridad Informática e Internet. Ra-Ma, 2001.
9. Ucla. *The UCLA Internet Report 2002, Surveying the Digital Future***.** http://www.ccp.ucla.edu/pdf/UCLA-Internet-Report-2001.pdf**.**
10. Zwicky E. Building Internet Firewalls, 2 Ed. O'Reilly, 2000.