I. Introducción

El 70% de las visitas a páginas web relacionadas con la pornografía tienen lugar durante la jornada laboral. Más del 60% de las compras a través de Internet o el envío y recepción de ejecutables se realizan desde la oficina. Además, los menores tienen libre acceso, en la mayoría de los casos, a páginas de contenido sexual, racista y violento. Para evitar esto, hay muchas compañías que se dedican a desarrollar software de limitación de contenidos para que los padres o empresarios predeterminen los accesos a través de Internet desde sus computadoras.

Internet es una fuente de información y de comunicación casi inagotable. La red se ha hecho su sitio tanto en el entorno empresarial como en los hogares. Las empresas la utilizan para mejorar sus comunicaciones y facilitar su trabajo, tanto interno como externo. El público general busca en ella información y oportunidades de ocio. Hemos asistido a la creación de empresas en línea, a la cultura del "chateo" y miles de aplicaciones más. Pero con Internet también nació la polémica, y es que su libertad de movimiento, el acceso libre y anónimo a todos los contenidos también supuso y supone una cuestión pública que sigue siendo fuente de debates en todo los ámbitos. La democratización de la información hace que cualquier persona pueda acceder a contenidos, hasta ahora "censurados", a partir de un clic de ratón. La polémica surgió con los primeros contenidos pornográficos y violentos y, hoy por hoy, todavía se reconoce que pese a todos los avances de la red, el control de sus contenidos es todavía una cuestión pendiente y de difícil solución.

A pesar de todo ello, existen varias empresas dedicadas a proponer sistemas de filtrado de contenidos, que hacen posible limitar el acceso a páginas web que se consideran inapropiadas para menores o bien en el entorno empresarial, donde el mal uso de Internet conlleva altos costes a la empresa. Son sistemas que bloquean el acceso a sitios web, clasifican las páginas web basándose en contenidos para adultos pornografía, violencia, racismo, droga, sectas, etc.), establecen tiempos de control para usuarios individuales y graban las actividades de estos internautas que han navegado permitiendo luego el control de dichas visitas.

Desde la introducción de los primeros programas de control en 1995, han ido apareciendo productos relativamente sencillos de utilizar, que permiten controlar y bloquear el acceso a determinados contenidos o aplicaciones.

II. Breve reseña histórica

El primer sistema de filtrado fue implementado por desarrolladores australianos debido al incremento del acceso de niños a páginas con alto contenido dañino y se realizaba según la clasificación de las páginas. Su trabajo comenzó junto con la masificación de la Internet, en 1995.

El consorcio *3W* fue el encargado de analizar y establecer estándares para la elaboración y contenido de páginas, hasta ahora este Consorcio es el encargado de estas tareas. La primera empresa que se dedicó a certificar sitios y quien todavía lo hace es RSAC que a través del Internet Content Rating Association dan a las páginas según categorías niveles de confiabilidad y tipificación. En 1996 el Internet Explorer versión 3.0, Integró el sistema de calificación de la RSACi (Recreational Software Advisory Council on Internet) al Asesor de Contenidos del browser. Mientras que en 1998, el Netscape Navigator adoptó idéntica medida en su función NetWatch.

Ambos navegadores trabajan con las normas de la ICRA (Internet Content Rating Association, o Asociación de Clasificación de Contenidos en Internet ,entidad sin fines de lucro soportada por actores de la industria. Esta asociación internacional independiente, otorga a los padres herramientas para realizar con fundamentos el filtrado de contenidos. Sus principales objetivos son: proteger a los niños contra contenidos potencialmente nocivos y proteger la libertad de expresión en Internet.

La empresa norteamericana N2H2, ubicada en Seattle, fue una de las pioneras, se ha especializado en ofrecer filtros a colegios, bibliotecas, empresas y proveedores de acceso a Internet en Estados Unidos, Canadá, Gran Bretaña y Australia. A nivel comercial masivo CyberPatrol fue le primer filtro en el mercado.

III. ¿Qué son los filtros?

Un filtro es un programa compuesto de uno o mas robots de análisis y una base de datos. Un robot de análisis es un pequeño programa o script que lee el contenido de una página web en busca de un elemento en particular, ya sea éste una conjunción de caracteres, un formato o algún otro elemento característico e identificable que deseamos saber si está presente en dicha página web.

Los ejemplos más típicos de robots de análisis son: lectores de encabezado y estructura, lectores simples de texto y lectores complejos de texto, también conocidos como lectores de asociaciones de palabras. Estos últimos trabajan de forma ligeramente diferente al resto, ya que no buscan un elemento en particular sino combinaciones de elementos en forma de palabras o frases que puedan disparar la alarma del robot.

Funcionamiento básico

Cada vez que un usuario solicita una dirección web todos y cada uno de los robots revisan por turno el contenido de dicha dirección. Basta con que uno de ellos encuentre el elemento que buscaba para que suene la alarma y se termine el proceso de revisado, con lo cual se archiva la dirección dentro de la base de datos y se le pasa al usuario un mensaje explicándole las razones por las cuales no se permite acceder a dicha dirección.

El papel de la base de datos es que independiente del numero y tipo de robot de análisis que tenga el filtro, el primero en actuar siempre compara la dirección web suministrada por el usuario contra la base de datos, de esta manera si dicha dirección coincide con algunas de las presentes en la base de datos directamente mostrará el mensaje de filtrado sin tener que perder tiempo buscándola en Internet.

IV. Tipos de filtros

Filtros de direcciones

Este tipo de filtros tiene la particularidad de trabajar únicamente con el nombre de la página solicitada. Se basan en lo que llamamos una ACL (Access Control List), que consiste en una lista de palabras claves que pueden *permitir* o *denegar* el acceso. Las listas son chequeadas según el orden en que fueron escritas y la búsqueda en las listas termina cuando se encuentra alguna de las reglas que figura en las listas. Por ejemplo si deseamos que nuestros usuarios no accedan a sitios de recetas de cocina, creamos una regla que prohíba el acceso a cualquier URL que contenga la palabra “cooking” o “cocina”. Esto se hace simplemente con unas líneas de código (específicamente tres) en la configuración del servidor.

Estos filtros se implementan con el Squid que permite también el control de puertos, la redirección de páginas y permisos especiales según el cliente. El Squid es un “WEB PROXY CACHE” diseñado para correr sobre sistemas Unix.

La rapidez es la principal ventaja de este sistema pero si se utiliza como método único de filtrado es poco eficiente ya que no puede filtrar texto que se encuentra dentro de los documentos ni scripts de lenguajes como JavaScript o VBscript anidados dentro de un documento HTML . La Universidad Católica de Asunción aplica este método. Es conveniente aclarar que el Squid es utilizado como parte importante en otros filtros.

Filtros de contenido

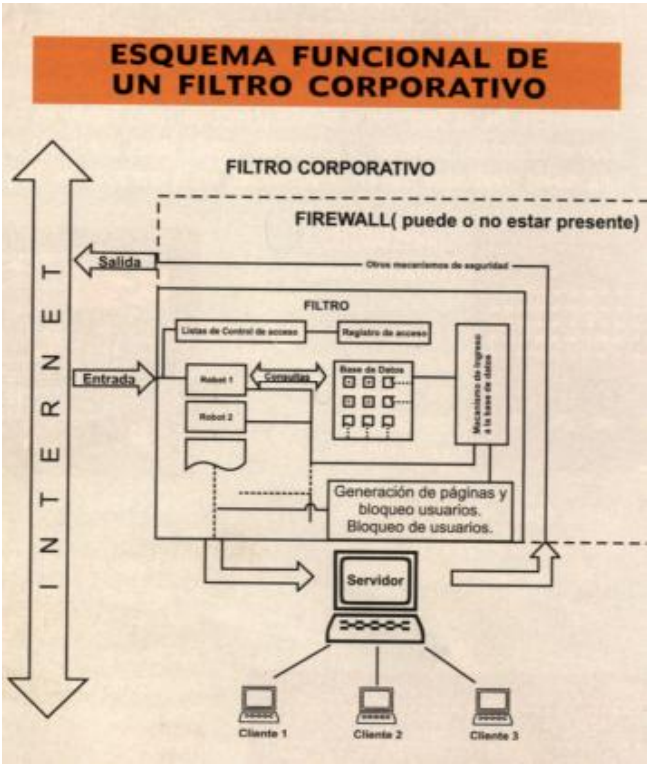
Las herramientas de filtrado de contenidos obligan a que los accesos a la Web de las organizaciones cumplan determinadas políticas, verificando cada usuario en una base de datos de URL's. Dado que esta base de datos contiene cientos de miles (y creciendo) de URL's, esta organizada por categorías, para facilitar las políticas de administración. Por ejemplo, una organización puede decidir el bloqueo de todos los sitios relativos a Apuestas, Sexo, o docenas de áreas relativas a otros sujetos. Dado que diariamente se construyen nuevos sitios Web, los servicios de filtrado de contenidos añaden, continuamente, nuevos sitios a la base de datos maestra. Para esto se cuenta con personas que se dedican a buscar especialmente las páginas de acuerdo al tema que se desea filtrar e ir añadiéndolas a la base de datos.

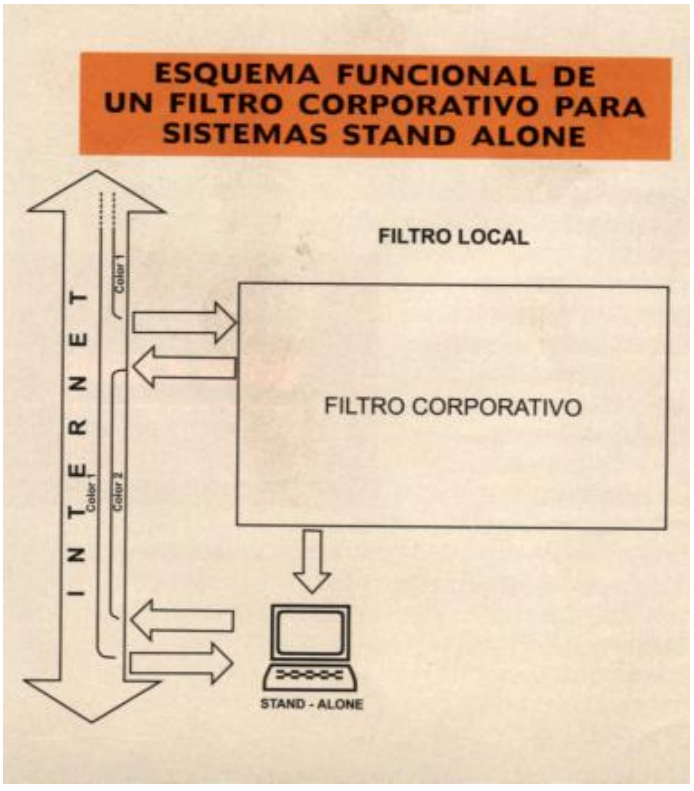
Los filtros de contenido pueden clasificarse según su lugar de instalación: los que se instalan en las computadoras clientes o sobre sistemas stand-alone (computadoras que no están en una red) también llamados filtros locales; o en los servidores de la red o filtros corporativos, para impedir el despliegue de información conforme a una serie de parámetros configurables por el usuario o el administrador del sistema.

Básicamente los dos tipos funcionan de la misma manera en cuanto al filtrado de Internet. La diferencia principal entre ellos radica en que los filtros locales centran su seguridad contra ataques provenientes del propio usuario del sistema (asumimos que el uso de filtros es impuesto al usuario), mientras que los filtros corporativos se organizan de tal manera que puedan rechazar ataques provenientes de Internet, confiando la seguridad interna principalmente al sistema operativo y a sus políticas de seguridad. Es por esto que en muchos casos los filtros corporativos son, en realidad, firewalls por software que entre sus muchas utilidades de seguridad, filtran las páginas a las que acceden los usuarios.

También existen algunos programas que no se adecuan a la clasificación normal, como los filtros de contenido para sistemas stand-alone. Este sistema combina filtro local con la seguridad de un filtro corporativo, los pasos que realiza este sistema son: el cliente pide una pagina web, el analizador lógico toma el pedido y revisa su caché para ver si tiene registrada la página, si es así, automáticamente deniega el acceso a la misma. Si la pagina no esta registrada, el analizador toma una copia y revisa su contenido buscando palabras o frases que estén restringidas. Si no encuentra ninguna la pagina es mostrada al cliente.

Gráficos esquemáticos del funcionamiento básico de los filtros.





Otra clasificación esta dada por

a. Sistemas de Clasificación Voluntarios
b. Sistemas de Clasificación de Terceros
c. Sistemas de Detección de Palabras
d. Ambientes Controlados

a) Sistemas de Clasificación Voluntarios

Consisten en que los creadores de un sitio Web, acuden voluntariamente con una "agencia" de clasificación y, en base a la información proporcionada por aquellos, la agencia emite una etiqueta en lenguaje HTML que deberá ponerse como parte del código de las páginas Web. Cuando un programa de navegación, compatible con este sistema, encuentre la página, podrá determinar, en base a los parámetros establecidos por el usuario y a la etiqueta HTML, si la página puede desplegarse o no. Este es el sistema que utiliza el Microsoft Internet Explorer.

Hay que tener en cuenta que estos filtros deben de activarse y configurarse manualmente (normalmente están desactivados) y tienen la desventaja de que muchos de los sitios Web pudieran estar mal clasificados o incluso no tener clasificación alguna (quizás sea el caso de la mayoría).

Una ventaja de este sistema, es que se apega a estándares de clasificación (por ejemplo al estándar PICS -Plataforma para la Selección de Contenidos en Internet-), por lo que los criterios para clasificar los sitios Internet son transparentes; además el usuario puede en principio, elegir el sistema de clasificación que más se adecue a sus valores y preferencias.

b) Sistemas de Clasificación de Terceros

En este caso la clasificación de las páginas Web no la efectúa el usuario ni el creador de la página, sino una tercera parte. Normalmente la puesta en práctica de este sistema se lleva a cabo mediante un programa de computación instalado en la máquina del usuario y la utilización de listas de sitios no aptos. El clasificador puede ser el mismo desarrollador del software, o bien otra persona.

La clasificación realizada por los desarrolladores del software restringe en cierta medida las opciones disponibles para el usuario ya que en general, los sitios Web son autorizados o no autorizados (no hay término medio) en base a los criterios establecidos por el desarrollador (es el caso de programas como Net Nanny o CyberPatrol). Por otro lado, hay otras metodologías basadas en el estándar PICS, en las que se establecen clasificaciones y graduaciones para que el usuario configure su máquina en base a sus valores y preferencias; no se proporcionan listas propiamente, sino un sistema de clasificación aplicado a las páginas que permite determinar su contenido (es el caso de NetShepherd que es una empresa que proporciona el servicio de clasificación).

c) Sistemas de Detección de Palabras

Consiste en el bloqueo de sitios Web si en el contenido de las páginas se detectan palabras que pueden significar la presencia de material cuestionable.

El principal defecto de estos sistemas es que se requeriría de un análisis contextual del contenido para determinar si el uso de determinada palabra verdaderamente implica que el sitio es adecuado o no, lo que es difícil de implementar por los desarrolladores de software; de hecho, programas como Net Nanny que los incorporan, también proporcionan herramientas adicionales tales como listas editables de sitios no adecuados, listas elaboradas por el usuario etc.

d) Ambientes Controlados

Se encuentran en desarrollo productos ofrecidos por los proveedores de acceso a Internet que pueden ser presentados como opción a los padres de familia que deseen que la cuenta de sus hijos contenga restricciones en su acceso a Internet. Los mecanismos utilizados van desde la restricción para visitar y participar únicamente en foros destinados a niños, pasando por el bloqueo de ciertos servicios (charlas en línea, conversación por voz, etc.), filtrado de las herramientas de búsqueda; hasta la utilización de listas de sitios "prohibidos". Quizás este sistema se preste a una mayor colaboración usuario-proveedor, aunque no deja de tener el inconveniente de que el principal responsable de los sistemas de filtrado es el proveedor, quien utiliza su escala de valores, o la de alguna organización que lo asesore, para la clasificación de los sitios.

V. Otras propiedades del filtrado

Los programas de filtrado de contenidos no se ocupan únicamente de “censurar” páginas en el ámbito privado o empresarial. Hay otros que además se ocupan de limitar la entrada de contenidos publicitarios y ventanas emergentes que ralentizan y aumenta el tiempo de descarga. El más conocido es Internet Watcher 2000, aunque también incluye sistemas de limitación de contenidos no publicitarios. Se trata de un acelerador de la Red al que se ha añadido un sistema asegurador con el fin de optimizar enormemente su conexión a la Red con una ampliación aproximadamente de un 50% en el ancho de banda.

Además es posible implementar sistemas que restrinjan el tamaño o la extensión de los archivos que se permiten bajar o enviar a través de Internet o por intranet. Dansguardian da estas ventajas, entre otros.

Otra opción es Ad Banner y URL Filter de la compañía Nit. Con la ayuda de este programa es posible filtrar los banners y limitar el material al que se tiene acceso desde nuestro servidor. Este módulo (plug-in) funciona en un segundo plano por lo que el filtrado no se hace patente en la imagen del monitor. Para configurar el programa es necesario seleccionar la opción ADIEFilter Property, que se encuentra dentro de herramientas en la barra de menú del Internet Explorer.

VI. Uso de los filtros

En la empresa

"El acceso de los trabajadores a páginas web que no tiene nada que ver con su actividad laboral supone a la empresa unas pérdidas aproximadas de 8.000.000 de guaraníes por empleado al año. Las consultoras han hecho sucesivos estudios mundiales y cifran en un 45% las empresas que utilizan algún tipo de protección para controlar el uso que hacen sus empleados de Internet o del comercio electrónico en Europa. El 30% del tiempo de navegación de cada trabajador es empleado en cuestiones no relacionadas con el trabajo y el 70% del tráfico pornográfico en Internet se lleva a cabo durante la jornada laboral" (fuente: Websense).

Las consecuencias del mal uso de la Red son drásticas. Durante este año el New York Times despidió a más de 20 trabajadores por un uso inadecuado de su correo electrónico. Xerox también se ha visto obligada a despedir a varios trabajadores por pasar gran parte de su jornada laboral en sitios web relacionados con sexo. Lo mismo ocurrió en Iberdrola, Pacific Bell o AT&T. El control del uso de la Red se está realizando especialmente en EE.UU donde ya se habla del 84% de las empresas. En Europa, las primeras propuestas tecnológicas de filtrado están empezando a hacen furor.

La mayoría de las empresas ofrecen a sus empleados acceso a Internet y correo electrónico a partir de su red corporativa, por ello defienden su derecho a controlar las visitas que los empleados hagan a diferentes sitios web e incluso el uso del correo electrónico ya que finalmente el usuario está utilizando un bien de la empresa cuyo fin es incrementar su productividad. Para controlar el uso que se hace de estas tecnologías en horario laboral, múltiples empresas han desarrollado diferentes soluciones que utilizan todo tipo de filtrados para delimitar el acceso de los empleados a diferentes contenidos.

Entre las compañías que proponen este tipo de servicios está Edunet. Según la propia empresa el uso de estos sistemas representa un ahorro de 9.000.000 de guaraníes por empleado al año. Su programa, e-optionet, ahora llamado optenet, puede instalarse en el servidor de la empresa, lo que permite que todas las computadoras que estén conectadas a él dispongan de sistema de elección de contenidos. Este software analiza los contenidos y los elige a partir de una lista de protección predefinida, con más de 120.000 direcciones que se actualizan a diario. La efectividad de este analizador está en torno al 90% y se encuentra disponible en seis idiomas: español, inglés, francés, portugués, alemán e italiano, lo que facilita la detección de estos contenidos. Edunet ya cuenta con clientes como Arrakis, Telefónica Data, los cibercafés Conect@te, el Vaticano y numerosas pymes.

La compañía Websense también es una de las encargadas en desarrollar estos sistemas. Websense Enterprise (WSE) es una aplicación compuesta de varios módulos software que combinados ofrecen un potente sistema de control de acceso a Internet. La detección de los contenidos pasa por varias fases. El módulo de monitorización observa todo el trafico entre la red e Internet y almacena informaciones en base a las reglas definidas en el módulo de gestión.

Este fichero log incluye información de los usuarios de la red, el tipo de servidores Web visitados, el ancho de banda consumido y los intentos de violación de la política empresarial de acceso a Internet. Además, consta de un módulo de gestión que permite definir los privilegios de acceso a Internet para los usuarios de la red.

La configuración incluye el tipo de servidores Web autorizados por usuario, por horas y días de la semana. Este módulo funciona en unión con el módulo de monitorización para bloquear el acceso a servidores indeseados y generar alarmas en caso de violación de las reglas. Finalmente el módulo de informes genera gráficos y hojas de datos con informaciones sobre el tráfico entre la red e Internet. Recoge las informaciones de los ficheros logs creados por el módulo de monitorización y crea diagramas en distintos formatos que pueden ser, luego, distribuidos a usuarios y/o administradores de departamentos. Este módulo genera más de 20 tipos de informes y es un "módulo distribuido". De esta forma, puede ser activado desde cualquier punto de la red y los administradores de departamentos pueden usarlo desde sus puestos de trabajo para crear informes sobre sus usuarios y equipos.

La empresa australiana Eye-T Tecnology ha creado un programa para luchar contra el tráfico de material pornográfico a través de la computadora. Eyeguard (ojo guardián) trata de evitar que se vean las imágenes de contenido sexual. A diferencia de otros filtros Web, que impiden el acceso a sitios web pornográficos, Eyeguard protege el contenido y se centra en las imágenes ya sean fotografías o videos y una vez instalado permanece siempre activo. Este programa es capaz de analizar los colores que están presentes en la imagen, de esta manera al detectar "demasiados" color carne, da por hecho que se trata de una imagen de contenido sexual. Una vez detectada, las imágenes se bloquean de forma automática y según prefiera la empresa, puede que el empleado no se dé cuenta de que el programa lo ha detectado o por lo contrario paraliza completamente la computadora. De cualquiera de las maneras, el software mantiene parte de la imagen en su memoria para que pueda verla el jefe.

En las casas

De acuerdo a un estudio reciente del Centro de Políticas Públicas Annenberg en los EEUU (Annenberg Public Policy Center), 78% de los padres de familia de ese país están preocupados por el tipo de contenido que sus hijos pueden obtener en línea. Si bien el 75% de los encuestados creen que Internet es una herramienta de aprendizaje positiva, cerca de la mitad expresó su temor de que la Red interfiera con la enseñanza de valores positivos.

Aunque la mayoría de los programas de filtrado de contenido son aptos para cualquier entorno (empresas, colegios, hogares, etc.), muchas de las compañías fabricantes ofrecen versiones explícitas para cada entorno o incluso programas diferentes.

La polémica sobre el libre acceso de menores a contenidos más o menos controvertidos que acompaña a Internet desde su nacimiento, toma especial relevancia en los últimos años. En julio del año pasado, el presidente norteamericano Bill Clinton se pronunció al respecto y anunció nuevas medidas legales para limitar el acceso de menores a páginas web con

contenidos pornográficos. La tarea no se prevé sencilla, ya que la limitación de contenidos, en muchas ocasiones, se contradice con libertades fundamentales de la Constitución. Mientras se barajan opciones como la clasificación de páginas web igual que las películas de cine, Microsoft ya ha recomendado el uso de la "Plataforma para la Selección de Contenidos por Internet" (PICS). Como ya mencionamos este sistema añade a las páginas web una etiqueta que explica la clasificación de la página para que pueda ser leída por los buscadores.

Uno de los productos que se encuentran en esta categoría es Internet Guard Dog de McAfee. Esta tecnología vigila tanto los mensajes que son enviados a un menor como la información que este trate de enviar desde la computadora. A partir de una base de datos de contenidos censurables, los mensajes que sean considerados inapropiados, se les impide que lleguen a un menor o que él los envíe. Estos casos se recogen en un registro de infracciones al que solamente los padres o supervisores tienen acceso, en el que queda patente el contexto en que se envió el mensaje y de quién vino. Además, el sistema también puede impedir a los menores el acceso intencionado o accidental a sitios web mediante una lista personalizable donde se establecen los filtros, ya sean palabras o sitios web.

CYBERsitter 2000 de la empresa Solidoak Software le brinda a los padres la posibilidad de limitar el acceso de los niños a ciertos materiales objetables que se encuentran en Internet. Con esta herramienta será posible bloquear, bloquear y guardar o simplemente alertarlos cuando deseen visitar ciertos sitios. Sus características incluyen el bloqueo de direcciones, grupos de noticias, chats, correos electrónicos e ICQ. Posee un "sistema inteligente de filtrado" que reconoce incluso sitios nuevos, puede llevar un registro de "desobediencia" por parte del usuario y controlar el acceso a Internet (pudiendo configurarse días u horas). Además, dispone de un sistema automático de actualización de sus bases de datos e incluso se puede especificar el bloqueo en categorías o servicios. Esta versión, como casi las de todas la empresas, puede trabajar con cualquier tipo de conexión (módem, RDSI, Cable Módem, DSL y LANs). Es posible ejecutarlo en cualquiera de las versiones de Windows. Solidoak ha incluido una nueva función de control remoto con la que es posible seleccionar el puerto para bloquear (HTTP, NNTP, IRC, IRQ, SMTP, POP3). Este programa garantiza el filtrado por encima del 97% de todo material objetable.

También Hearsoft ha tomado cartas en el asunto con su programa de evaluación de archivos de imágenes para contenido censurable que se integrará en un navegador para niños, Internet Safari, como parte de las opciones de seguridad del mismo. Las aplicaciones del bloqueo de imágenes serán muy amplias como la integración en navegadores de Internet o programas de correo electrónico.

Como vemos, el usuario que quiera limitar el acceso a Internet en sus hogares puede optar entre una lista muy extensa. Los más utilizados en EE.UU son Cyber Patrol y NetNanny. El primero ofrece programas dirigidos a todos los ámbitos pero tiene unas versiones especiales para las computadoras personales para el usuario doméstico. Por su parte, NetNanny es una aplicación desarrollada para poder permitir la monitorización de correos electrónicos, programas para charlar por medio del protocolo IRC, grupos de noticias y aplicaciones que funcionen off-line.

Pero también desde el otro lado se han tomado medidas. La propia industria pornográfica ha desarrollado en los últimos años un sistema para alejar de los menores el material orientado al público adulto. El resultado de estos esfuerzos ha sido el llamado sistema de verificación de edad. Adult Check es hoy el sistema más extendido de protección y funciona de manera ejemplar siempre y cuando el menor no esté en posesión de una tarjeta de crédito. El usuario de este tipo de página web tiene que solicitar su identificación Adult Check por la que ha de pagar una cuota anual y firmar un contrato en el que asegura su mayoría de edad. Una vez hecho esto, se abre una extensa base de datos con contenidos para adultos.

En Bibliotecas

Todos los recursos que se proveen en las bibliotecas se ofrecen igualmente a todos los usuarios con el entendimiento de que es la responsabilidad de cada usuario utilizar buen juicio, demostrar respeto a otros usuarios, y mantener conducta apropiada mientras utilizan todos los recursos y las instalaciones de la Biblioteca Pública.

Sin embargo las computadoras Internet no pueden ser utilizadas para cualquier actividad ilegal, ni para acceder materiales ilegales, ni para acceder materiales que por las normas o convenciones de la comunidad local se consideren como obscenidad.

En algunas bibliotecas el personal está autorizado a actuar inmediatamente de manera adecuada para implementar las Reglas de Conducta, y/o a prohibir el uso por personas que no cumplen con el reglamento aceptable del uso del Internet. Por estas razones muchas bibliotecas han implementado sistemas de filtrado.

En escuelas

La protección de los niños ante los contenidos que circulan en Internet es una tarea importante, ya sea en los hogares como en las escuelas, para evitar que los menores accedan a páginas inadecuadas, muchas de las cuales están relacionadas con la pornografía, el racismo o la xenofobia.

Cada vez son mas las instituciones educativas a las computadoras como “medio de iniciar a los alumnos en un nuevo estilo de aprendizaje”, lo que conlleva establecer contactos con otras personas y con nuevas fuentes de información. Sin embargo los docentes con experiencia en el aprendizaje informatizado saben que su función ha de cambiar. Si las computadoras no se utilizan como es debido, pueden ser un estorbo para el aprendizaje. Es primordial que el maestro guíe a los alumnos. El número de escuelas de EEUU conectadas a Internet se ha duplicado en los últimos tres años. Según las últimas estadísticas, el 82% ya tiene algún tipo de conexión. A finales del próximo año escolar, el 96% estarán conectadas. En Canadá las cifras se manejan en los mismos rangos y si bien en Latinoamérica no crecen a ese ritmo si se van incrementando los escuelas y colegios con conexión. Tanto en Uruguay como en Argentina y Paraguay existen proyectos para instalar filtros en todos los lugares donde los menores tengan acceso a la red.

Internet debe ser una alternativa más donde los alumnos guiados por los docentes llevan adelante proyectos de investigación. Pero para llegar a encontrar la información debe existir, primero, una adecuada planificación, que sólo se adquiere utilizando métodos de búsqueda que apliquen principios lógicos de filtros y selección.

Los protectores para Internet, integrados a los navegadores habituales sólo necesitan ser activados para filtrar contenidos nocivos pero cabe resaltar que ninguno es mejor que la presencia de mayores cuando los más chicos navegan por la web. Es una plataforma adecuada para comenzar a trabajar por la protección de los niños en casa o escuelas, tarea en la que cualquier filtro sólo juega un papel de colaborador.

La presencia de los mayores resulta siempre insustituible, y no existe ni existirá filtro, ya sea gratis o pago, que pueda cubrir esta responsabilidad. Si bien todos estos filtros son ciertamente una ayuda, no se debe caer en la ingenuidad de pensar que detendrán cualquier contenido inadecuado, ni siquiera el esperado en todos los casos, por pago o gratuito que sea.

VII. Aspectos legales

En junio del 2000, la Comisión Europea consideró la necesidad de la puesta en marcha de centros para denunciar los contenidos ilícitos ya sean degradantes, pornográficos o violentos que circulan por la Red. En un principio se instalarán ocho centros para el control en otros tantos países. Además de este proyecto, la Comisión Europea financia actualmente diez programas de lucha contra los contenidos ilícitos en Internet, a lo que destina 25 millones de euros.

La protección de menores es una labor que se está tomando muy en serio en la política de la Unión Europea. En un principio las medidas estaban orientadas a evitar a los proveedores de servicios en Internet (ISP) el establecimiento de controles sobre contenidos, pero existen una serie de excepciones.

Por ejemplo, la Decisión del Consejo del 29 de mayo de 2000, establece una serie de obligaciones relativas a la lucha contra la pornografía en Internet (especialmente la infantil). Por ello hay que informar a las entidades competentes acerca del material de pornografía infantil del que los proveedores hayan recibido información y retirar dicho material.

Por otro lado, hace unos meses un juez de Miami ordenaba a Yahoo y America Online revelar la identidad de un cibernauta anónimo acusado de difamación por un empresario de Florida. Este fallo fue el primero que cuestiona los supuestos derechos constitucionales que tiene una persona para expresarse de forma anónima en los servicios de charla de Internet.

Mientras esto sucedía en Estados Unidos, en Gran Bretaña el gobierno avanzaba sus planes para permitir a los servicios de seguridad vigilar el tráfico en Internet. En España también se ha producido alguna sentencia al respecto. El Tribunal Superior de Justicia de Andalucía asegura que el registro de las terminales de computadora de los empleados por parte de su empresa vulnera el derecho a la intimidad de estos, a no ser que el empresario justifique la actuación. La sentencia reconoce que se puede producir el registro, pero sólo

cuando corra peligro el patrimonio empresarial y el de los demás trabajadores de la empresa. Recuerda también que la computadora es un instrumento de trabajo propiedad de la empresa y que no debe ser utilizado para otros fines distintos a la realización de la actividad profesional.

En EEUU se espera la decisión del Tribunal Supremo respecto a la Ley de Filtros de Internet, los abogados de las libertades y grupos de bibliotecas están preparando una demanda sobre esta ley, aprobada recientemente en el congreso de los EEUU. El senador John McCain presentó un proyecto de ley para el Filtrado de Internet en las Escuelas que exige que las escuelas que reciben fondos públicos para fomentar el acceso universal filtren los sitios considerados "inadecuados" por sus comunidades. Por otra parte, la Ley de Protección de la Infancia, propuesta por el congresista Ernest Istook, es parecida, pero va todavía más allá extendiendo la exigencia de filtrado a todo ordenador que esté subvencionado con fondos públicos.

Los grupos de defensa de los derechos civiles más importantes se oponen a estos proyectos legislativos y a cualquier medida que haga obligatorio el filtrado de la red en instituciones públicas, por considerar que viola los derechos protegidos por la Primera Enmienda. La Unión Civil Americana de las Libertades (ALCU) y la Asociación Americana de Bibliotecas (ALA), apoyadas por otros grupos, están preparando pleitos en Philadelphia, Pennsylvania en un intento de tumbar el Acto de Protección de los Niños en Internet (CIPA), ya que según ellos bloquea constitucionalmente la información protegida tanto para niños como para adultos.

CIPA, solicita escuelas y bibliotecas federales para instalar los filtros de contenidos de Internet que bloquean el material desagradable para los menores de edad. A menos que sean paradas por alguna acción legal, esas escuelas y bibliotecas deberán instalar los filtros para Internet el próximo mes o perderán los fondos federales destinados a proporcionar al acceso Internet.
Los críticos de CIPA demandan que no hay actualmente software en el mercado que pueda distinguir adecuadamente entre la información legal y la ilegal en el Internet.

VIII. Actualidad Nacional

En nuestro país hay varias empresas que brindan el sistema de filtrado para empresas, colegios, universidades y hogares.
Una de ellas es Redetica que utiliza el tipo de filtro corporativo para sistemas stand-alone. Los servicios que prestan son:

- Protección contra el contenido indeseado de Internet a través de un filtro.
- Protección de los datos y archivos de la computadora a través de jerarquías de usuarios, encriptaciones y antivirus.
- Protección de fuga de datos con restricciones físicas al dispositivos capaces de servir como puente de salida de información (disquetera, impresora, etc.)

Un ISP (Proveedor de señales de internet) que presta este servicio es Netvision que utiliza un sistema llamado SGI (Sistema de Gestión de Internet) que le permite monitorear y controlar la navegación y uso de Internet de su corporación.

Una empresa que ya no presta estos servicios es Alvimer, que utilizaba el sistema de filtrado de Norton.

Telesurf por su parte tiene planes de implementar estas prestaciones.

Por parte de los usuarios hay una creciente concientización y preocupación por el uso inadecuado que se está dando a la Red, es por eso que colegios como San José, Campoalto, Goethe cuentan ya con filtros. Así también empresas como A.J. Vierci, Ultima Hora, Mc. Donald´s entre otras .

A nivel nacional existe una legislación al respecto, por ahora sólo en el ámbito de protección al menor, de acuerdo a lo establecido en la Constitución en el artículo 58 (De la Protección al Niño), este proyecto ya está aprobado pero su implementación no está siendo puesta en marcha aún. En esta ley del Código del Menor se establece que en los lugares donde haya menores que usen Internet deben estar protegidos por filtros.

IX. Nuevas tecnologías y sus problemas

Hoy en día los accesos a Internet permiten varios tipos de terminales, entre ellos los teléfonos móviles. Por todo ello, los contenidos pornográficos están llegando también a las terminales WAP, de hecho ya hay varias direcciones de Internet que se dedican a ello. Esta cuestión es demasiado novedosa y por ello todavía no hay programas preparados para la filtración de contenidos en estas terminales, pero ya hay opiniones al respecto. La asociación Morality in Media con sede en EE.UU ya ha advertido de los peligros de la nueva tecnología que se aproxima. La máxima preocupación nace una vez más del libre acceso a contenidos “inmorales” por parte de los más jóvenes.

También está el caso de la transmisión satelital. Existen regiones enormes que tienen poca o ninguna infraestructura terrestre. La tecnología satelital es la única alternativa para proporcionar servicios de Internet en estas regiones. Existen empresas que pueden entregar acceso confiable y a alta velocidad a casi cualquier sitio dentro de su sombra VSAT sin importar la clase de terreno. Esto representa una ventaja significativa debido a que no existe infraestructura terrestre en muchas de estas zonas. En estos mercados el sistema de filtrado debe variar. Intellicom es un empresa que implementó un sistema llamado K.I.D.S. que atiende las necesidades específicas de instituciones educativas. SkyPOP, de la misma empresa proporciona una red troncal de Internet instantánea para el mercado de los ISPs que funciona como una puerta de enlace con servicios completos. K.I.D.S. combina la red SkyPOP con un firewall integrado que brinda filtros personalizables para impedir que los estudiantes y otros usuarios reciban contenido entrante cuestionable. K.I.D.S. permite a las escuelas establecer y configurar sus propios parámetros para filtros.

Como el tema es polémico y actual también se han pronunciado al respecto las identidades bancarias. Sus quejas al respecto vienen por otro lado: la dificultad de realizar los cobros a los usuarios de páginas web con contenidos pornográficos y los fraudes de las propias empresas. En ocasiones se ha llegado a cobrar dos, tres y hasta diez veces una misma visita como han declarado empleados de la web Clublove.com. A partir de todos estos problemas la empresa de tarjetas de crédito American Express encargó un

estudio de la situación cuyos resultados fueron muy relevantes: casi un 80% de las compras pornográficas en la Red terminan en una reclamación ante la entidad bancaria. Por todo ello, ha invalidado la utilización de sus tarjetas en este tipo de pagos ya que el poco control hace que niños utilicen las tarjetas de miembros mayores de la familia y el cobro real del dinero se retarda o se hace imposible. Un sistema real de verificación de edad que además contuviese algún dato del usuario, solucionaría esta problemática, según American Express.

Pero como en casi todo lo que ocurre en la Red, los hackers también tienen algo que decir en esta cuestión. Gracias a Eddy Jansson y Matthew Skala los menores ya pueden acceder a todas las páginas censuradas por algunos filtros de contenidos como CyberPatrol o NetNanny. Ahora ambos se enfrentan a varias demandas, entre ellas la de MicroSystems por la publicación de su herramienta de descodificación (Cphack) en una web de libre acceso. Razones de este tipo llevan a que la información sobre el diseño específico de los filtros no este disponible en los sitios y sea bastante cerrada su divulgación. Cada empresa implementa las técnicas básicas de manera diferente y combinándolas de modo a, no solo, mejorar su eficacia, sino a disminuir su vulnerabilidad.

X. Conclusión

La masificación de Internet como vimos ha traído muchas novedades y con ellas los problemas que siempre surgen ante las nuevas tecnologías y su correcta aplicación. Debemos considerar que ante todo es un tema opinable y si bien se puede hacer mucho daño desde la red, es en si toda una revolución en la era de la comunicación y la información.

Hoy en día la información que circula por la Internet es de una variedad asombrosa. Y así como se han ampliado las fuentes de conocimiento, crecieron los peligros. El sexo ya no es el único polo de atracción con poder para alarmar a los padres. Existen sitios donde se explica paso por paso cómo construir una bomba, fabricar una droga casera o utilizar una tarjeta de crédito robada.

El uso de los filtros es una alternativa y una de las formas de establecer cierto control a personas y lugares que lo requieren. Como ya mencionamos, los filtros no pueden suplantar el consejo acertado de los padres y profesores pero si ayudar de manera eficaz. Consideramos que su uso en colegios y escuelas es imprescindible, en el hogar también, pero recalcamos lo que anteriormente dijimos que estos no suplantan a la educación que cada padre debe dar a sus hijos, y que la comunicación entre estos es irreemplazable.

Se comprobó por encuestas que la mayor preocupación de los padres sobre el uso de la Internet se centraba en la protección contra el riesgo de fraude crediticio y el abuso de la información personal. Luego, le seguían la exposición a la pornografía, el correo electrónico no solicitado, la invasión de extraños y la exposición a otro tipo de contenido inapropiado. A pesar de esto, es peor que los menores se enfrenten a un número significativo de problemas con contenidos inapropiados y experiencias desagradables. Los filtros en la casa pueden remediar en parte estos problemas.

Además del ámbito ético-moral que puede discutirse (probablemente sin llegar a ningún acuerdo como ocurre en estas cuestiones) en el tema de la instalación de filtros en forma masiva en lugares públicos, queríamos enfocar su importancia a nivel empresarial. Son muchas la experiencias que ponen de manifiesto su utilidad a la hora de mejorar la productividad y concentración de los empleados si se restringen ciertos temas que no son laborales.

Tenemos experiencias en nuestro país de compañeros que trabajando en grandes empresas y teniendo en sus manos la responsabilidad de administración de recursos (ancho de banda, horas de trabajo, tráfico en la red interna, dispositivos de hardware entre otros) optaron primeramente por una política de “libertad absoluta” para todos los empleados en el uso de la red, viendo que los recursos no eran bien aprovechados tuvieron que implantar algún sistema de filtrado y restricciones de acceso.

Con los ejemplos y estadísticas descritas a lo largo del trabajo queríamos poner en conocimiento de todos justamente la importancia de los filtros, es decir no solo su relevancia estrictamente moral de lo que se “debe o no mirar” sino también su utilidad en niveles de rendimiento laboral y también educativo.

XI. Bibliografía

- Asociación Española de Usuarios de Internet: www.aui.es
- Asociación de Internautas: www.internautas.org
- Cyberpatrol- Software para el control de acceso a la Red: www.cyberpatrol.com
- Edunet servicio español para evitar accesos a páginas no deseadas: www.edunet.es
- Guardianserver: www.guardianserver.com.
- Netnanny - Software que controla el acceso a contenidos X y violentos: www.netnanny.com
- Surfwatch- software para el filtrado de contenidos: www.surfwatch.com
- Asociación de Clasificación de Contenidos en Internet : http://www.Icra.Org www.rsac.org
- Guardone www.guardone.com
- 3W Consortium: www.3w.org
- Empresas nacionales: www.redetica.com www.netvision.com.py
- Filtros por Squid: http://www.squid-cache.org http://squidguard.org/ http://dansguardian.org/ http://www.nxp.net/netfilter_prod.asp
- Asociaciones de padres y colegios: http://www.entelchile.net/entelcorp/internet/planes/familia/legal.htm www.sat.lib.tx.us/inetuse_esp.htm www.albanet.com.mx/articulos/FILTROS.htm www.unidosaqui.com/content/es0055D322.html www.soltel.com.uy/ids.html
- Otros links utilizados http://www.hypermedia.com.py/num01.htm http://www.yagua.com http://lat.3com.com/lat/products/firewalls/index.html http://www.ciberestrella.com/010202/articulos/china.htm http://ar.news.yahoo.com/75141528/010714/559998.html http://www.unesco.org/courier/2001_03/sp/education.htm http://www.arnal.es/free/noticias/2_25/filtros.html http://www.intellicom.net/espanol/spkids_faq.htm http://www.consulintel.es/Html/Productos/Cacheflow/filtrado.htm http://ar.news.yahoo.com/75141528/010714/559998.html http://www.arrakis.es/~dlevis/diecom/netescuea.htm http://www.ucm.es/info/dinforma/activi/libro/21.html www.microasist.com www.xav.com www.websense.com www.N2H2.com

Índice