Seguridad de la Información

Métodos de protección

Fecha revisión: *27/05/2002* Ref: *CE00004*

1. Introducción

¿Está su empresa protegida contra la fuga de información?

¿Es consciente de la pérdida de productividad para su empresa que supone un mal uso de Internet?

¿Tiene sentido en una empresa hacer uso de una herramienta de tan alto riesgo como Internet sin ningún plan previo de seguridad de la información?

¿Sabe que Internet y el correo electrónico son las principales vías de contagio de los nuevos virus como los troyanos que nos provoca un agujero de seguridad siendo su PC controlado desde el exterior por un pirata informático?

Con el auge del ADSL y del cable, ¿es conocedor del riesgo actual de sufrir intrusiones en su ordenador y ser víctima de cualquier internauta malintencionado que con pocos conocimientos informáticos puede fácilmente coger, borrar y modificar la información de su ordenador?

En los últimos años hemos sido testigos de un espectacular crecimiento en la implantación de los accesos a Internet de banda ancha como el ADSL y el cable, enfrentándonos a un gravísimo problema de seguridad, ya que se puede similar “la banda ancha como vivir todos en la misma casa y con las ventanas abiertas”.

Y al mismo tiempo los usuarios durante este período “han bajado la guardia” sobre precauciones en el uso de Internet y se ha pasado de un cierto temor y respeto a una situación actual en la que se realizan conexiones a Internet sin ninguna protección ni medida de seguridad ni asesoramiento por ningún experto en seguridad.

A lo largo de este informe desarrollamos esta **gravísima situación actual de inseguridad en la protección de nuestros sistemas y de la información en ellos contenida**.

2. Evolución del concepto de Seguridad de la Información

La seguridad que hace unos años se limitaba al ámbito del espionaje industrial, en la actualidad y gracias al auge y utilización de Internet, ha hecho que sea parte integrante de la inversión que ha de realizar una empresa para el desempeño de cualquier actividad económica. En un principio la seguridad se centraba en lo que se conoce como seguridad perimetral, es decir, un control estricto de quién y qué entra y sale del área protegida. **En la actualidad y la legislación así lo recoge, las empresas han de garantizar la seguridad y privacidad de los datos personales que poseen**.

Los ataques de los piratas informáticos se están extendiendo con preocupante rapidez gracias al creciente número de ordenadores conectados a Internet y a la popularización de herramientas que permiten a cualquiera introducirse en ordenadores particulares y en redes informáticas.

La seguridad de las redes de la empresa es uno de los temas que más preocupa en la actualidad, como consecuencia de la generalización de Internet y del acceso remoto de los usuarios. Siendo el mejor enfoque para afrontar este desafío de seguridad el entenderlo como algo global, distribuido y completo.

A la hora de abordar la seguridad de las redes, lo primero que constatamos es que la realidad actual es radicalmente distinta a la de hace unos años. Aunque el objetivo último sigue siendo el mismo: minimizar el riesgo protegiendo los sistemas y la información crítica de las compañías de la pérdida o del uso indebido.

Hasta hace no mucho tiempo los sistemas de información eran sistemas eminentemente cerrados. Por un lado, contar con una tecnología propietaria aseguraba el aislamiento exterior. Por otro lado, las diferentes áreas departamentales de las compañías contaban con sistemas de información propios y, a menudo, aislados del resto de los sistemas de la compañía. Y en este entorno el principal problema de seguridad era la pérdida accidental de los datos por fallos de los sistemas, problema que se solventaba a través de sistemas de back-up o sistemas redundantes.

Sin embargo, **actualmente han aparecido nuevos retos de seguridad a los que es necesario enfrentarse**:

- **Nuevos usuarios internos y externos**: las demandas de acceso a los sistemas de información de las compañías están creciendo a pasos agigantados y frecuentemente a través de redes públicas como Internet.
- **Interconexión de áreas departamentales**: hoy en día con las crecientes exigencias de información hace impensable el aislamiento de las diferentes áreas de una compañía. Por tanto, el añadido en seguridad que procedía del aislamiento desaparece.
- **Comercio electrónico**: el comercio electrónico supone que numerosos usuarios entran en los servidores de la compañía a la búsqueda de información, por lo que la empresa se encuentra de nuevo ante un nuevo reto de seguridad.

- **Multiplicación de usuarios y dispositivos**: el número de internautas crece exponencialmente con multitud de dispositivos diferentes que permiten el acceso a Internet, representando todo ello más amenaza para la seguridad.
- **Conectividad permanente**: Internet supone conectividad permanente las 24 horas del día, no se pueden cerrar los servidores y cuando se cierra la oficina alguien desde la otra punta del globo puede comenzar sus ataques.

De forma esquemática las áreas de seguridad a tener en cuenta en las empresas son las siguientes:

- Control de accesos (continente): cortafuegos, antivirus, certificación...
- Confidencialidad de las comunicaciones (contenido): VPN
- Monitorización: gestión, administración y operación de los sistemas y violación de los sistemas

3. Cifras preocupantes sobre seguridad

La *AEDI* (*Asociación Española para la Dirección Informática*) y *Microsoft* han realizado un estudio titulado "Política Empresarial de Seguridad de la Información", de la cual se extrae, como conclusión más significativa, que **el 74% de las empresas españolas son conscientes de que no podrían sobrevivir más de cuatro días sin la información contenida en sus ordenadores**. A pesar de la preocupación que las empresas manifiestan por disponer plenamente de su información, sus políticas de seguridad se centran en los aspectos más tradicionales (control de accesos, antivirus, copias de seguridad...), dejando en segundo orden otros aspectos como las auditorías, procedimientos para la detección de intrusos o políticas de mantenimiento que garanticen la disponibilidad permanente del servicio.

Según *Websense* **durante la jornada laboral: el 40% de la navegación por Internet no está relacionada con actividades comerciales, ocurre el 70% del tráfico de pornografía de Internet, se realizan más del 60% de la compras on-line, los usuarios de la web aprovechan las conexiones a alta velocidad para obtener acceso a sitios de entretenimiento de banda ancha con más frecuencia que cuando están en casa y las palabras más buscadas en Internet son: mp3, sexo y hotmail**.

Gartner, revela en su último estudio que **sólo el 35% de las pymes de todo el mundo poseen un completo plan de recuperación de desastres y que menos del 10% han desarrollado planes de contingencia o de gestión en situaciones de crisis**. Y en otro estudio relativo a los principales problemas de seguridad que tendrán que afrontar las empresas exponen que hasta el 2002 **el 90% de los ataques informáticos aprovecharán vulnerabilidades para las que existe una solución conocida**, además estima que **el 20% de las empresas sufrirán en los próximos tres años un incidente de seguridad serio aparte de los virus**.

Según un estudio presentado por *Landwell* **cuatro de cada cinco problemas relacionados con la seguridad informática se originan desde dentro de la propia empresa** por lo que se pone de manifiesto que una gran parte de los casos de trasgresión de las políticas de seguridad en las empresas se producen desde dentro

de las compañías, aumentando así la vulnerabilidad de las mismas frente a posibles ataques.

La revista *Information Security* acaba de desvelar que el ataque a los servidores web se ha duplicado en 2001 respecto al año anterior. Y es que **el 90% de las compañías consultadas por la publicación reconoce haber recibido la desagradable visita de algún gusano, virus o Caballo de Troya y un 40% recibió un ataque de denegación de servicio**. **El 78% de los consultados han achacado parte de la responsabilidad de los contagios a los empleados, ya que se instalan software ilegal sin autorización previa**. A eso se añade que, a su juicio, **el 60% utiliza ordenadores de la empresa con fines extra-laborales**.

El 90% de las empresas entrevistadas por el *Instituto de Seguridad Informática CIS y el FBI* **declararon haber sufrido una violación de sus sistemas de seguridad informática en los últimos doce meses**, sin embargo, sólo un 34% de ellas denunciaron las intrusiones, principalmente para evitar la publicidad negativa o que la competencia se aprovechase de ello. **Tras los ataques el 77% de las empresas optaron por tapar los agujeros de seguridad descubiertos**.

En un informe de *Ernst & Young* referido a datos mundiales de empresas del año 2002 informan que: sólo **el 40% están seguras de poder detectar un ataque, un 40% no investigan los incidentes de seguridad, un 75% han sufrido caída inesperada de sus sistemas**.

Según un estudio realizado por *Webscreen Technology*, **durante el año 2002 una de cada tres empresas británicas sufrirá un ataque de denegación de servicios distribuido** (Distributed Denial of Service, DDoS). Los ataques de denegación de servicios distribuido son los que se producen cuando un sitio web recibe, de forma simultánea y desde múltiples sitios de Internet un gran número de peticiones que los servidores no pueden soportar y que, por lo tanto, provocan su caída. En la práctica, resulta muy difícil llegar a saber quién realiza estos ataques, ya que se llevan a cabo de forma anónima desde los sistemas de otros usuarios.

4. Conceptos básicos de Internet

Con el auge del ADSL y del cable y la conexión a Internet permanente, normalmente con una dirección IP casi fija, fácil de detectar y que facilita su localización y ataque, nos enfrentamos con un grave problema de seguridad, ya que es preciso considerar una nueva modalidad de **hacker** que, en realidad, no persigue beneficio económico ni popularidad en la consecución de sus acciones, sino simplemente buscan diversión. Los llamados **lammers** les divierte entrar en su PC y destrozarle el sistema o robarle información por el mero hecho de resultarle divertido. Los contratos de las operadoras no suelen advertir al usuario de estas vulnerabilidades que afectarían gravemente a su negocio.

El término **hacker**, se utiliza normalmente para identificar a los que siendo expertos en sistemas informáticos únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daño, pero pueden instalar troyanos que les proporcionen passwords nuevas.

Se denominan puertas traseras (**backdoors**) a aquellos programas que permiten el acceso a un ordenador de forma remota desde otro, siendo los "**Caballos de Troya**", también denominado **troyanos**, aquellos programas maliciosos insertados en un PC sin consentimiento de su dueño que permite el control de ese PC desde el exterior por otra persona. Se pueden considerar un tipo de virus, ya que el PC atacado se infecta con él. Normalmente un troyano se instala en un PC a través de un correo electrónico o a través de un intercambio de ficheros. Un cortafuegos instalado detectaría cualquier intento de conexión a la red y solicitaría nuestra conformidad para permitir el acceso.

Los **crackers** son los hackers fascinados por su capacidad de romper sistemas de protección para obtener beneficios y además el problema radica en que esta rotura es difundida normalmente por Internet para conocimientos de otros.

En cuanto a los **piratas informáticos**, su actividad se centra en la obtención de información confidencial y software de manera ilícita.

Los **lammers** es el grupo más numeroso de miembros con mayor presencia en la red y el más peligroso, lo forman principiantes con pocos conocimientos informáticos que utilizan programas rastreadores de puertos abiertos y programas sniffers que monitorean los paquetes de red que están direccionados al PC donde están instalados para interceptar contraseñas y correos electrónicos con el objetivo de poder entrar en dichos sistemas remotos. A través de dichos programas que están difundidos por la Red escanean los rangos de IP asignados a ADSL y descubren muchísimos ordenadores con el disco duro compartido pudiendo coger, borrar y modificar información en ellos contenida o atacar a terceros desde dichos ordenadores.

Existen dos maneras de obtener el acceso a ADSL: **modem** y **router**. **Actualmente la adopción de modem es la más implantada por la agresivas ofertas de las operadoras, pero es la más insegura al ser el propio PC quien gestiona el acceso**, convirtiéndose en el punto final de la conexión. En el caso del **router** la seguridad es superior, puesto que existe un elemento intermedio al que el PC se conecta. Aunque en el caso de los routers se han planteado ciertos problemas de agujeros de seguridad en determinados modelos, lo que es indudable es que los niveles de seguridad proporcionados por las operadoras no son suficientes.

Para entender de forma clara la problemática de la conexión a Internet debemos de conocer que cuando nos conectamos a Internet, establecemos un tráfico incesante de envío y recepción de pequeñas unidades de datos llamados **paquetes**. Por lo tanto, en Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino y la comunicación que entra y sale de nuestro PC lo hace a través de los llamados **puertos** que explicamos a continuación.

Cuando un PC se conecta a Internet pasa a formar parte de toda la Red y como tal se tiene que comunicar con el resto. Para poder comunicarse lo primero que se necesita es tener una dirección electrónica llamada **dirección IP** para poder identificarse con los demás. Gracias a la **dirección IP se identifica un determinado recurso de forma única para permitir acceder a él**. Pero esto no es suficiente, ya que **en Internet se pueden utilizar muchos y diversos servicios y es necesario poder diferenciarlos y la forma de diferenciarlos es mediante los puertos**.

Por lo que podemos considerar los puertos como los puntos de enganche para la conexión de red que realizamos. El protocolo de comunicaciones identifica los extremos de una conexión por las **direcciones IP** de los dos nodos implicados y el número de los puertos de cada nodo. Existen más de 65.000 puertos diferentes,

usados para las conexiones de Internet, así por ejemplo, un servidor web escucha las peticiones que le hacen por el puerto 80, un servidor FTP lo hace por el puerto 21, etc.

Por lo tanto como hemos dicho anteriormente, cuando un usuario se conecta a Internet ya sea por un **modem** o por una tarjeta **RDSI**, este recibe de su **ISP** (Proveedor de Servicios de Internet) una **dirección IP**. Esta dirección es la que nos permitirá navegar y acceder a otros ordenadores los cuales contienen las páginas web a las que estamos accediendo, ya que estos ordenadores disponen a su vez de su propia **dirección IP**. Por lo que en este momento nuestro ordenador se encuentra conectado a una red, Internet, que es pública en la que nosotros tenemos una **dirección IP** que también es pública, por lo tanto cualquier pirata informático puede tener acceso a nuestro PC. Esta **dirección IP** cuando la conexión la realizamos de forma intermitente puede cambiar en cada conexión pero basta que a nuestro PC hayan accedido una sola vez para que puedan haber instalado un "**Caballo de Troya**" que les permita tomar el control de nuestro PC independientemente de la dirección asignada en cada momento. Como hemos explicado anteriormente el problema se agrava cuando aprovechando las "**tarifas planas**" las conexiones pueden llegar a ser permanentes, de esta forma la **dirección IP** asignada está más tiempo expuesta a Internet y a los posibles ataques que podamos recibir.

Además de la conexión a Internet vía **modem** o tarjeta **RDSI** hemos dicho anteriormente que podemos optar por la opción de instalar un **router**, el cual nos va a permitir una conexión más segura a Internet aislando nuestra red local mediante filtrado de paquetes (Firewall), o bien ocultando las direcciones de los PCs mediante **NAT** (Network Address Traslation). El filtrado de paquetes permite determinar qué paquetes pueden pasar hacia nuestra red. El proceso **NAT** permite ocultar las direcciones de los PCs con una única dirección. Nuestro **ISP** asignará la dirección **IP** al **router** y éste enmascara las direcciones de nuestros PCs con la asignada por el **ISP**, con lo cual desde Internet no sabrán la dirección real del PC que está conectado en ese momento. Por supuesto el **router** es capaz de gestionar la conexión de varios PCs al mismo tiempo, permitiéndonos además un ahorro, ya que usando una sola conexión podemos conectar a la vez varios PCs a Internet. Por otro lado los routers son elementos que requieren una configuración para que se ajuste a las necesidades del usuario y cerrar todos aquellos puertos que no se van a utilizar, cosa que no se suele realizar ya que se instalan los routers por las operadoras con una configuración estándar para todos sus clientes.

Para poder realizar una conexión compartida a Internet también disponemos de la opción de un **Servidor Proxy**, pero esto requiere la utilización de un PC sólo para la conexión a Internet y un software que controle esta conexión con lo cual el coste podría ser más elevado.

Por lo tanto estar conectado a Internet permanentemente no solo proporciona ventajas, sino que también corremos el riesgo de sufrir intrusiones en nuestro ordenador y ser víctimas de cualquier internauta malintencionado. Cualquiera que descubra la **dirección IP** con la que un PC se conecta a Internet podría acceder a dicho PC para realizar cualquier acción, desde acceder a los ficheros, pasando por introducir virus o troyanos o usar dicho PC como plataforma para ataques a otros ordenadores. En este sentido, se recomienda instalar un **cortafuegos** (firewall) que impida las conexiones externas no deseadas, así como contar con un antivirus actualizado, que permita eliminar los troyanos en caso de que se sea victima de uno de ellos.

Según las recomendaciones para usuarios domésticos del *National Infraestructure Protection Center norteamericano*, **el cortafuegos debería ser tan imprescindible como el antivirus**.

Los cortafuegos profesionales son esenciales para proteger la seguridad de las redes corporativas frente a los cortafuegos personales de menos complejidad para dar solución a las vulnerabilidades en el mercado doméstico, protegiéndonos contra intrusiones tales como escaneado de puertos y troyanos, así como evitar el envío de datos personales a sitios web inseguros y bloquear applets Java, controles Actives y cookies de sitios desconocidos.

Una medida básica de seguridad es conocer que puertos tenemos, cuáles están abiertos, porqué están abiertos y de estos últimos los que no utilicemos o que sean fuente de un problema de seguridad. A través de un escaneador de puertos podemos saber qué puertos están abiertos en un PC, dando opción a que el intruso pueda penetrar en nuestro sistema a través de ellos.

Un sistema básico de seguridad, que debemos utilizar para nuestra conexión de Internet, es la instalación de un cortafuegos que es un sistema de defensa que se basa en la instalación de una barrera entre el PC e Internet, por la que circulan los datos. Este tráfico entre Internet y el PC es autorizado o denegado por el cortafuegos filtrando los paquetes conforme a la configuración realizada. La misión de un cortafuegos es la de aceptar o denegar tráfico, pero no el contenido del mismo, en principio deniega tráfico cerrando puertos. En el momento que un determinado servicio o programa intente acceder a Internet o a nuestro PC nos lo comunicará y podremos en ese momento aceptar o denegar dicho tráfico, pudiendo así mismo hacer permanente la respuesta hasta que no cambiemos nuestra política de aceptación. Mediante un cortafuegos se puede cerrar u ocultar puertos evitando intrusiones, se puede recibir cuando detecte algún tipo de escaneo o intento de intrusión, facilitando la IP del atacante y el puerto atacado.

5. Métodos de protección

5.1 Firewall (Cortafuegos)

El **Firewall** nos va a permitir aislar nuestra red de Internet, mediante un filtrado de los paquetes que van tanto desde nuestra red hacia Internet como de Internet hacia nuestra red. Un **Router** actúa como un Firewall, ya que permite filtrar los paquetes en función de unos determinados datos que contienen los mismos, como dirección IP, puerto, etc.

Hay otros tipos de filtrados a un nivel más alto que permiten filtrar a nivel de las aplicaciones que se están utilizando, Navegadores (HTTP), Transferencia de ficheros (FTP), correo electrónico (SMTP y POP3). Para realizar estos filtrados es necesario la utilización de un software específico y un PC que se instala entre la red interna y la conexión a Internet que es el encargado de vigilar todas las transferencias que se realizan.

5.2 Antivirus

Internet y el correo electrónico son las principales vías de contagio de los nuevos virus y el problema de la seguridad se ha convertido en una obsesión para los usuarios, sobre todo si se piensa que existen unos 60.000 virus catalogados y que cada día aparecen veinte nuevos virus.

La inmensa mayoría de las infecciones por virus en la actualidad son debidas a infecciones por **gusanos** (programas que se transmiten a través de Internet) y **troyanos** (programas que ejecutan acciones ocultas e indeseables) en la mayoría de las veces a través del correo electrónico.

Debido a la proliferación de virus del tipo **gusanos**, que se reproducen a sí mismos y a las mutaciones que se van produciendo, la detección de virus es un problema que cada vez se agrava más si no se disponen de las herramientas necesarias.

Para evitar los problemas que pueden ocasionarnos los virus, pérdida de información e incluso averías en nuestro PC les recomendamos una serie de puntos que le ayudaran a controlar mejor la problemática de los virus.

- **Utilizar un buen antivirus y mantenerlo actualizado**. No es conveniente fiarse de los productos gratuitos que podemos conseguir a través de revistas, ya que estos productos pueden estar anticuados o no controlar bien la gran cantidad de virus que existen actualmente. Algunos buenos antivirus pueden estar permanentemente actualizados vía Internet. Aunque esto no es sinónimo de protección absoluta, ya que un virus de muy reciente aparición puede introducirse en nuestro sistema antes de que la vacuna esté lista o hallamos descargado la actualización.
- **Desconfiar de cualquier archivo recibido por correo electrónico**. Aunque el correo recibido venga de algún conocido es conveniente tener en cuenta que las infecciones a través de envío masivo de e-mail se basan en las libretas de direcciones del software de correo, además pueden enmascararse con “asuntos” que pueden engañarnos y tentarnos para ejecutar el contenido del mismo.
- **Chequear cualquier archivo**. Cualquier archivo, venga de donde venga, por el medio que sea, Internet, disquete, cdrom, etc. debe de ser chequeado antes de ser copiado a nuestro PC, después puede ser tarde.
- **Evitar la ejecución de macros**. Estas son opciones que podemos desactivar de nuestros navegadores, con idea de que no se ejecuten programas que puedan venir ocultos en las páginas WEB o en los documentos recibidos, que simplemente al abrir estos documentos se ejecutan.
- **Mantener actualizados el Sistema Operativo y los Programas**. Todos los programas y Sistemas tienen agujeros de seguridad que son descubiertos con posterioridad a su lanzamiento. Por eso es conveniente la actualización de los mismos, ya que evitaremos que puedan atacarnos a través de estos agujeros. Es necesario configurar correctamente nuestros programas, en especial los navegadores, cortafuegos y antivirus y mantener estos dos últimos siempre activados. Ya que si no se han sabido configurar correctamente no están realizando las funciones de protección para lo cual se han instalado.
- **No permitir que personas que no sean de su confianza usen su ordenador**. Puede que estas personas no sigan tan escrupulosamente las

reglas de seguridad anteriores y al final podemos encontrarnos con problemas ocasionados por ellos.
- **Mantenerse informado sobre las últimas alertas motivadas por recientes ataques y contagios colectivos**.
- **Es necesario realizar copias de seguridad frecuentemente** no sólo de documentos, sino de libreta de direcciones, favoritos, correo de entrada, etc. que no se suele realizar habitualmente.

5.3 VPN (Redes Privadas Virtuales)

Hoy en día la utilización de Internet está abaratando los costes de las comunicaciones entre las empresas, ya sea entre distintas empresas como entre delegaciones de una misma empresa. El problema está en que esta comunicación a través de Internet puede ser interceptada por personas de la competencia, Hackers, etc. Para ello debemos asegurarnos que esta comunicación no pueda ser interceptada, o si lo es que esté encriptada para que no pueda ser leída por alguien ajeno a nuestra empresa.

Esto se realiza mediante las **VPN** que **son enlaces que se establecen entre dos puntos en Internet donde los datos viajan de forma segura de un punto a otro gracias a que son encriptados y sólo el receptor dispone de las claves necesarias para desencriptarlos**.

En general, las soluciones basadas en Internet son inherentemente más débiles, aunque válidas para las compañías que estén buscando reducir los gastos de conectividad y expandir sus capacidades, para las cuales las **VPNs** presentan una solución real.

5.4 Filtrado de contenidos

El filtrado de contenidos nos permite que definamos una política de utilización de Internet, evitando páginas web que pudieran resultar peligrosas tanto a nivel de infecciones o de ataques como a nivel de productividad evitando que los usuarios pierdan el tiempo en páginas web que puedan distraerles de su tarea. El filtrado se puede realizar a nivel del contenido de las páginas, a través de un texto que pueda aparecer en la URL o en la página web e incluso podemos permitir el acceso sólo a las páginas definidas en una determinada lista. También es posible el filtrado a nivel de URL Blocking que es una lista de URL organizadas por categorías: “desnudos”, “racial”, y otras. Estas listas son continuamente actualizadas por las organizaciones que las han creado. Las compañías más conocidas como Microsoft, Netscape, IBM, etc. usan la lista CyberNOT de la compañía The Learning Company.

Mecanismo gracias al cual los usuarios no pueden acceder a determinadas páginas de Internet no autorizadas y a la vez se reduce el riesgo de invasión de virus ocultos en páginas cuyo origen y legalidad no están verificadas.

Una solución de filtrado web puede ayudarnos a aumentar la productividad de nuestros empleados y revalorizar el contenido de sus conexiones a Internet. Desgraciadamente las redes corporativas no siempre están llenas de tráfico relacionado con el trabajo, en lugar de esto, nos podemos encontrar con usuarios

navegando plácida y tranquilamente por lugares de ocio o realizando compras on-line. El problema es triple. En primer lugar, la conexión a Internet es más lenta para aquellos trabajadores que sí empleen este recurso con fines productivos. Por otro, los empleados pueden estar descargando contenidos potencialmente ofensivos o ilegales de los cuales nosotros, como administradores, podemos resultar responsables. Por último, existe una pérdida de productividad asociada directamente a este tipo de actividad en el cómputo de horas remuneradas y no trabajadas.

En resumen, una solución de filtrado de web administra, supervisa e informa acerca del uso de Internet por parte de los empleados.

Por lo que está claro que la navegación por la web debería estar restringida en el trabajo y aquí es donde entra en juego las soluciones de filtrado web, que en la mayoría de los casos trabajan restringiendo el acceso en base a URL (Uniform Resource Locator, localizador universal de recursos). En cada solución la lista de direcciones es categorizada y actualizada de forma regular y principalmente controlan el Administrador de reglas y el monitor que guarda toda la actividad de navegación que pasa por nuestra red, además de quien está visitando cada página web.

6. Conclusiones

Como hemos indicado anteriormente **debemos proteger nuestros equipos de Internet, tanto a nivel de virus, como de posibles ataques de hackers**, ya que no importa que tamaño de empresa tengamos, ninguna está libre de que en un momento determinado sea atacada por un hacker, aunque si bien es cierto que la mayoría de los ataques se realizan a grandes corporaciones también desgraciadamente cada vez existen más herramientas en Internet que pueden hacer de cualquier usuario de Internet un potencial hacker que acaba conectándose a nuestro PC y realizando cualquier manipulación, borrado, etc.. de nuestra información. También el problema de los virus no distingue entre empresa grande o pequeña, basta que nuestra dirección de correo-e esté en la libreta de direcciones de algún otro usuario que no sea tan previsor para que seamos blanco de cualquier virus. Por esto debemos estar siempre protegidos ante cualquier problema que pueda aparecer a través de Internet.

Aunque la seguridad total es imposible, se puede controlar todo un conjunto de vulnerabilidades y lo que se necesita no es solamente prevenir un ataque de seguridad, sino ser capaces de detectar y responder a esta agresión mientras ocurre y reaccionar ante la misma. Al no existir un control de seguridad único, las empresas deben de contar con diversas capas de seguridad en todos los niveles de su información para poder así detectar el problema en algunos de estos puntos antes de que llegue a la información crucial.

Lo importante es comprender que si no se toman ciertas medidas mínimas, la información sensible que se encuentre en cualquier ordenador, con el simple hecho de que tenga acceso a Internet o forme parte de una red local donde haya un ordenador conectado a Internet es suficiente para que pueda estar expuesto a ataques de diversa índole.

De todas formas, **el exceso de prudencia es contrario a la innovación** y, por tanto, lo recomendable es adoptar medidas que garanticen una cobertura suficiente, la elaboración de planes de seguridad tanto física como lógica y de las políticas correspondientes y, por último, la mentalización de los usuarios para el correcto uso de los servicios que se prestan. Y sobre todo **entender la seguridad como un proceso y no como un producto**.

En resumen, para una empresa la información es su activo fundamental que debe protegerse de ataques externos e internos, debiendo tener en todo momento un control de todo el tráfico desde y hacia Internet.