PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 4 | ENERO 2010 | *ISSN EN TRÁMITE* | REVISTA BIMESTRAL

Editorial

Una vez más **.Seguridad** es publicada para ofrecer a los lectores un espacio donde se pueden informar sobre asuntos de Seguridad Informática así como fomentar la cultura de la seguridad en cómputo.

En esta edición te damos a conocer los diferentes tipos de ***software* de seguridad** de los cuales puedes hacer uso en tu equipo para mantenerlo protegido. Con ello, es nuestro propósito el ofrecerte herramientas con las cuales puedes defenderte de las amenazas presentes en Internet. Estas herramientas que te presentamos forman un conjunto que te pueden brindar mayor seguridad en tus navegaciones. De esta forma podrás sentirte más seguro al hacer uso de Internet y podrás disfrutar de los beneficios que esta te ofrece.

Esperamos que hagas uso de este *software* y te sea de utilidad.

Rocío del Pilar Soto Astorga
Departamento de Seguridad en Cómputo

Javier Santillán

Imagínese una calle concurrida, edificio tras edificio, gente de todo tipo con diferentes destinos e intenciones. Cuando una de ellas se dispone a entrar a un edificio, se encuentra en la puerta a un oficial el cual verifica que esa persona se dirige hacia las oficinas del tercer piso por lo cual la deja pasar. Segundos después, otra persona intenta entrar diciendo que su destino son las oficinas del quinto piso. Como al oficial le han indicado que no se debe permitir el acceso a aquellos que van al quinto piso, entonces niega el acceso. Este tipo de acciones son las que precisamente hacen los *firewalls* en el mundo de las telecomunicaciones.

Internet es conjunto de redes, millones de ellas conviviendo alrededor del mundo. Debido a muchos factores que se han dado en el desarrollo y evolución de las comunicaciones han surgido amenazas que constantemente acechan a equipos conectados a la red. Incluso sin estar conectados a Internet, con el solo hecho de pertenecer a una red de datos, existen peligros constantes a los que todos los equipos están expuestos. Amenazas como los virus, gusanos, herramientas automatizadas, intrusos, publicidad no deseada, etc., se encuentran en el flujo de las redes de datos.

Pero, ¿cómo defenderse de estas amenazas? *Firewalls* al ataque, o mejor dicho, ¡a la defensiva!

Los *firewalls* (también llamados cortafuegos), son mecanismos de protección utilizados para establecer un control de acceso de los paquetes que entran y salen de una red. Funcionan mediante la definición de políticas, las cuales establecen lo que se va a permitir y lo que será restringido.

Como es de suponerse, existen diversos tipos de *firewalls*, cada uno destinado según el rol del equipo, usuario y tipo de red. En las clasificaciones más importantes, los *firewalls* son divididos en *firewalls* de *software* (lógicos) y *firewalls* de *hardware* (físicos). Existe también otra clasificación según el tipo de funcionamiento (capa de red en la que realizan su función). En cualquier caso, una de las cosas más importantes en un *firewall* es su correcta configuración mediante adecuadas políticas.

Al hablar de políticas nos referimos a un conjunto de reglas que establecerá lo que será permitido y negado. Una política puede ser tan específica como se desee, dependiendo también de las capacidades del *firewall*. Citando el caso de nuestro ejemplo inicial, una política podría definir el origen de la persona, el destino en el edificio, la persona que visita, y la cantidad de veces que puede acceder el visitante. Traduciendo a términos computacionales, significaría que el *firewall*

comprobaría la dirección IP origen del paquete de datos, la dirección destino, el puerto de la aplicación (por ej. Puerto 80 HTTP), y la cantidad de conexiones que puede recibir en un determinado tiempo.

Como se puede ver, mientras más capacidades tenga un *firewall*, las reglas pueden ser más complejas. Lo anterior debe manejarse con mucho cuidado ya que pueden ocasionarse fallas, contradicciones o en su caso omisiones. Pero en términos generales, ¿cuáles son las ventajas y desventajas de un *firewall*?

Ventajas

- Establecen un perímetro de protección de la red
- Mejora el control de acceso de todos los paquetes de datos que entran y salen
- Optimización del flujo de datos en la red

Desventajas

- Demandan conocimientos generales de redes de datos
- Pueden ser muy complejos
- Si no se configuran correctamente, pueden causar problemas en los servicios de la red.

Ahora, ¿cómo podemos identificar la mejor solución de *firewall*?

Esto depende totalmente del esquema de la red en que nos encontremos. Si bien es cierto que sirven para lo mismo, los diferentes tipos de *firewalls* tienen características que en un esquema no se utilizarían y en otro serían insuficientes.

Si somos usuarios caseros, es decir, nuestro equipo se encuentra en nuestra casa, bastará con tener instalado un *firewall* personal. Este tipo de *firewalls* están basados en *software* y tienen las características básicas y algunas adicionales que proporcionarán al equipo de una protección general en contra de las amenazas más comunes. Según los conocimientos del usuario, podrá configurarse para que la interacción del mismo sea mínima, de hecho, muchos *firewalls* de este tipo tienen una característica llamada “modo de aprendizaje” la cual permite que el *firewall* vaya definiendo reglas según se van presentando las situaciones, y según la respuesta del usuario (permitir o denegar), el *firewall* va creando un esquema propio para el funcionamiento de esa máquina.

Por otro lado, si nos encontramos en un esquema institucional en donde la red consiste en una serie de estaciones de trabajo, seguramente la decisión del *firewall* a utilizar no dependerá de nosotros sino del administrador de red. Generalmente, cuando se tiene un ambiente controlado, se cuenta con una administración centralizada con sistemas de monitoreo de tráfico de red y el *firewall* se ubica en un dispositivo principal el cual controla el tráfico de todos los equipos. Este *firewall* es mucho más complejo que los *firewall* personales ya que tiene capacidad para administrar el control de acceso de varios equipos. A través de estos sistemas puede controlarse incluso el tráfico de ciertas aplicaciones o por usuario.

Finalmente, en los ambientes más complejos de las grandes redes donde se encuentran todos los dispositivos de comunicación, están los sistemas *firewall* dedicados, ya sea de *software* o de *hardware*. Estos sistemas están dedicados exclusivamente para tener el rol de *firewall*, control de acceso, filtrado de paquetes, etc., y son monitoreados constantemente por los administradores. Pueden llegar a ser muy costosos y complejos en cuanto a su configuración, sin embargo, la finalidad general es la misma: control del flujo de datos en la red.

Es muy importante mencionar que el tener un *firewall* no es sinónimo de un sistema seguro. Si bien es un mecanismo que incrementa la protección, existen técnicas para evadirlos. Desde la perspectiva de usuario, es buena práctica que se combine la instalación de un *firewall* con otros sistemas como antivirus, *antispyware*, etc., los cuales darán a nuestro sistema puntos extra de protección.

Es totalmente válido el argumento de que en cuestiones de seguridad informática, “nada es 100% seguro”, así que en este caso, los *firewalls* nos ayudan, pero no resuelven los problemas de seguridad.

Antivirus: Una Herramienta Indispensable para Nuestra Seguridad

Miriam J. Padilla Espinosa

Debido a que en la actualidad el intercambio de información y la comunicación entre personas son realizados muy frecuentemente por medios electrónicos, se debe contar con mecanismos de protección para nuestros equipos de cómputo, como una medida de protección de la confidencialidad, la integridad y la disponibilidad de nuestra información.

De las herramientas fundamentales y requeridas para la protección de nuestros equipos encabeza la lista el *software* Antivirus, el cual es un programa de computadora, que mediante un escaneo de archivos tiene como objetivo la detección, identificación y eliminación de ***malware***[1]. El *software* antivirus está formado por tres partes principales, tal como se muestra en la Figura 1:

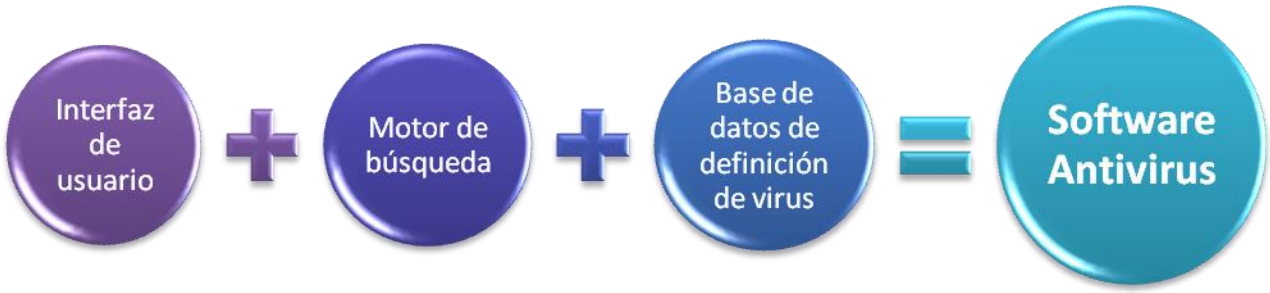

Figura 1. Partes de un *software* antivirus

- **Interfaz de usuario*:*** es el medio por el cual un usuario puede comunicarse e interactuar con el *software* antivirus y realizar configuraciones. (véase Figura 2).
- **Motor de búsqueda:** el motor de búsqueda es el cerebro del *software* antivirus ya que se encarga de la búsqueda y detección de *malware*, utilizando para ello la base de datos de definiciones de virus. Conforme nuevos virus son creados, el motor debe de actualizarse para que pueda realizar la búsqueda en las áreas, los archivos o sistemas que no se hayan revisado antes.
- **Base de datos de definición de virus*:*** contiene los archivos actualizados sobre las firmas del *malware* y es utilizada por el *software* antivirus para lograr su detección. Es esencial que la base de datos de definición de virus esté siempre actualizada para una eficaz y pronta detección que incluya a los virus más recientes.

[1] ***Malware*:** término utilizado para hacer referencia a todo aquel *software* que perjudica a un equipo de cómputo. El origen de esta palabra proviene del término en inglés "malicious software", conocido en español como código malicioso, dentro de esta clasificación están los virus, los caballos de Troya, las puertas traseras, los gusanos de Internet, *bots*, entre otros.

Antivirus: Una Herramienta Indispensable para Nuestra Seguridad

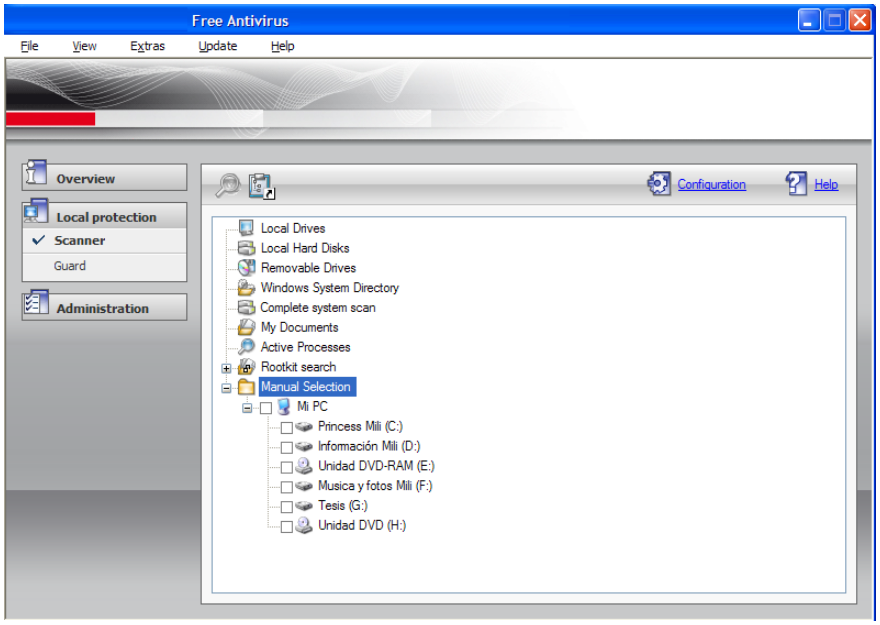

Figura 2. Interfaz de usuario de un *software* antivirus

Existen tres tecnologías utilizadas por los programas antivirus para realizar la detección de *malware*, estas son:

a) **Coincidencia de firmas *(Matching signature):*** Esta tecnología se basa en la búsqueda de coincidencias entre los archivos escaneados y los registros de las firmas de *malware* (contenidos en la base de datos de definición de virus). Una detección ocurre cuando se presenta una coincidencia entre los puntos en comparación. El inconveniente de esta tecnología radica en la necesidad de contar previamente con la firma asociada al *malware* para poder realizar su detección, lo cual requiere que el usuario realice actualizaciones periódicas a la base de datos que contiene las firmas del *malware*.

b) **Heurístico *(Heuristic):*** Esta tecnología consiste en que el *software* antivirus puede realizar la detección de *malware* del que aún no cuente con la firma asociada. Esto es posible mediante el uso de una base de datos de firmas de comportamiento del *malware*. Para llevar a cabo la detección, el *software* antivirus que utiliza esta tecnología, analiza el código para cualquier rutina o subrutina y lo compara con las firmas de comportamiento almacenadas en la base de datos (nivel estático), por otro lado si la tecnología heurística recurre a la ejecución en un máquina virtual que permite analizar el comportamiento del

malware se denomina de nivel dinámico. La desventaja del uso de esta tecnología es que debido a su funcionamiento puede provocar **falsos positivos**.[2]

c) **Verificación de integridad *(Integrity checksum*[3]**): Esta tecnología se fundamenta, en la idea de que un *malware* que desea infectar un sistema, deberá realizar modificaciones en el mismo para cumplir con su objetivo. Un ejemplo de ello podría ser la presencia de un virus que sobrescribe un archivo del sistema, agregando el código malicioso dentro del archivo (principalmente ocurre en este tipo de archivos debido a que se encuentran en áreas reservadas y son accedidos de forma mínima por los usuarios). El método recurre a la obtención de la lista de verificación de los archivos limpios de *malware* y cualquier alteración en este valor indicará que se ha presentado una modificación, lo cual puede indicar presencia de un *malware*. Las desventajas del uso de este método es la generación de falsos positivos, así como su ineficiencia hacia la detección de los macro virus o aquellos virus capaces de insertarse en la memoria y lograr su ejecución sin necesidad de estar almacenados de forma previa dentro de un archivo. Otro punto importantes es el proceso de detección de *malware* esto se realiza mediante dos procedimientos de operación los cuales están definidos en la Tabla 1:

	TIEMPO REAL (*Real Time*)	ESCÁNER BAJO DEMANDA (*on- demand scanner*)
Funcionamiento	Realizan la búsqueda de *malware* cuando se tiene acceso a un archivo o se ejecuta alguna aplicación.	El usuario puede indicar en cualquier momento, la revisión del archivo, carpeta o contenido en busca de *malware*.
Ventajas	Proporciona una protección constante cuando se requiere trabajar con un archivo o dispositivo en particular.	Puede ser programado para realizar comprobaciones en todos los archivos para la búsqueda de código malicioso.

[2] **Falso positivo:** consiste en un error por el cual un *software* antivirus reporta que un archivo, área o sistema está infectado, cuando en realidad está limpio de cualquier *malware*.

[3] **Suma de verificación (*checksum*):** Consiste en una forma para el control de redundancia, así como, para la protección de la integridad de los datos, el proceso consiste en sumar cada uno de los componentes básicos del sistema (cada *byte*) y almacenar el valor del resultado, posteriormente se repite el mismo procedimiento y se compara con el valor previamente obtenido, si los datos no coinciden indica que los datos han sido modificados.

Desventajas	Sólo realiza la revisión cuando se tiene acceso al archivo, en caso de que un archivo infectado esté alojado en el disco duro y no se acceda a él, el *software* antivirus no podrá realizar la detección	Ofrece una buena evaluación del sistema en un único punto en el tiempo (únicamente en el momento en que es invocado).

Tabla 1. Procedimientos de operación

Los criterios de evaluación que los usuarios caseros, las empresas y las instituciones podrían considerar para seleccionar el *software* antivirus adecuado a sus necesidades se presentan en la Tabla 2:

CRITERIO DE EVALUACIÓN	DESCRIPCIÓN
Detección	Dos aspectos importantes dentro de este criterio son: el número de virus que el *software* puede detectar (conocido como velocidad de detección) y bajo qué circunstancias puede realizarla (detección en recursos compartidos de red, a través de correo electrónico o si está ejecutándose en memoria).
Tecnología	Verificar el tipo de tecnologías que incluye el producto (compatibilidad con *software* y *hardware*, proceso de operación --*real time, on Access scanner*--, tecnologías utilizadas para realizar la detección.
Mantenimiento	Debido a la importancia de la actualización de la base de datos de definiciones de virus, es recomendable elegir un antivirus que sea fácil de actualizar y para el cual, las actualizaciones de la base de datos se realicen con mayor frecuencia. Además deberá evaluarse el tiempo en que se lleva a cabo el proceso de actualización.
Desempeño	Impactos que afecten el rendimiento del equipo de cómputo donde fue instalado.

Manejabilidad	En el caso de ambientes empresariales, la importancia de poder centralizar la gestión del *software* antivirus, que permita establecer los periodos de actualización, el establecimiento de políticas, verificar la protección de los clientes y de los servidores.
Soporte técnico	Conocer los diferentes niveles de soporte disponibles (usuario casero, soluciones corporativas), además de los medios para brindar el soporte (en línea, teléfono de contacto). Así como también las alertas sobre malware desconocido y que represente un riesgo alto para los equipos de cómputo.
Revisiones y evaluaciones de terceras partes	Evaluaciones publicadas por terceras partes, que permitan conocer a fondo el desempeño de un *software* antivirus bajo procedimientos particulares de evaluación.
Productos y vulnerabilidades	Identificar las vulnerabilidades detectadas en el *software* antivirus.
Perfil del distribuidor	Investigar información sobre los distribuidores, su posición y reconocimiento en el mercado, así como el tiempo que llevan en él.

Tabla 2. Criterios de evaluación

Es importante que antes de seleccionar un *software* antivirus se lleve a cabo un análisis de las distintas opciones que existen actualmente en el mercado y se consideren criterios que contribuyan a elegir la opción que satisfaga mejor las necesidades de seguridad.
Ya que tengas un antivirus instalado en tu equipo de cómputo, no olvides actualizarlo diariamente y complementarlo con otras herramientas como (*firewall, IDS, antispam, antispyware*).

Referencias:

http://www.sans.org/reading_room/whitepapers/commerical/choosing_your_antivirus_software_784
http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
http://www.antivirusworld.com/articles/antivirus.php
http://www.pcworld.idg.com.au/article/189865/antivirus_software?pp=4

Miriam Valdés Rodríguez

El *antispyware* es una tecnología de seguridad que ayuda a proteger a un equipo contra *spyware* y otro *software* potencialmente no deseado. Este *software* ayuda a reducir los efectos causados por el *spyware* incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada. Permite a los usuarios protegerse contra los programas cuya intención es rastrear la información sobre hábitos de consumo y navegación, o peor aún, obtener contraseñas y otros datos sensibles.

Síntomas de que una computadora está infectado por "spyware":

- Se abren continuamente ventanas emergentes mientras te encuentras en Internet.
- Se te dirige a sitios web que no indicaste.
- Aparecen barras de herramientas sin que tú lo hayas especificado.
- Sin aviso, te es cambiada la página de inicio.

Consideraciones generales para la elección de un *software antispyware*.

Al momento de seleccionar un *antispyware*, es necesario tomar en cuenta que cuente con algún reconocimiento por parte de algún laboratorio de investigación. Además debe de incluir las siguientes características generales:

1. **Bloqueo en tiempo real y monitoreo antes de que el *spyware* se descargue o instale.** Es mucho más fácil prevenir que el *spyware* se instale, en lugar de realizar una limpieza a un sistema afectado.
2. **Actualizaciones automáticas de firmas de *spyware*.** Es importante cerciorarse de que el *antispyware* esté actualizado. Algunas de las herramientas gratis requieren de actualizaciones manuales.
3. **Búsqueda automática que permita fijar el día y hora para las exploraciones automáticas.** Alternativamente, puede indicar al *software* la fecha para ejecutar exploraciones en su computadora.
4. **Capacidad para poder restaurar o revertir, en caso de que algún componente de una aplicación sea borrado inadvertidamente.** Con esta característica, los componentes pueden ser restaurados de la cuarentena para que la aplicación funcione nuevamente.
5. **Descripción del nivel de amenaza y análisis del estado de la máquina en la interfaz.** Permite al usuario tomar buenas decisiones acerca de qué componentes debe de ignorar, colocar en cuarentena o eliminar.
6. **Información, como ayuda en línea, foros, correo electrónico de apoyo y soporte telefónico.** Contar con información en diferentes medios para consultas acerca del *antispyware.*

Ejemplo de un *antispyware* gratuito

Antispyware	***Lavasoft Ad-Aware Anniversary Edition***  **Gratis**
Sistema Operativo	Windows 2000, XP, Vista
Características	• Protección en tiempo real. • Detección y eliminación de *malware*. • Actualizaciones automáticas.
Licencia	**Distribución gratuita**
Ventajas	• Un buen rendimiento en la eliminación de *spyware* • Protección en tiempo real
Desventajas	• No realiza escaneos automáticos.
Página web	http://www.lavasoft.com/

Para más información acerca de las diferentes tecnologías de *antispyware* que existen actualmente, consulta las siguientes direcciones electrónicas:

http://www.firewallguide.com/spyware.htm
2-spyware.com

Hay que tomar en consideración que algunos de los *antispyware* en conjunto con otros programas instalados, por ejemplo con los antivirus, pueden causar tanto problemas como soluciones y es mejor estar informado antes de utilizarlos.

Referencias:

http://www.seguridad.unam.mx/usuario-casero/index.htm
http://productos.arnet.com.ar/popup_antispyware_02.html
http://www.microsoft.com/SPAIN/windowsxp/using/security/expert/honeycutt_spyware.mspx
http://www.firewallguide.com/spyware.htm
http://www.consumersearch.com/anti-spyware-reviews
http://www.2-spyware.com/
http://www.us-cert.gov/cas/tips/ST06-009.html
http://www.vsantivirus.com/mm-antispywares.htm
http://www.pctools.com/es/spyware-doctor/

Mayra Villeda Juárez
Francisco Carlos Martínez Godínez

Sin darnos cuenta, el correo electrónico se ha convertido en una parte fundamental de nuestra forma de comunicación y de nuestro estilo de vida. El correo electrónico permite comunicarnos con gente de todo el mundo de manera prácticamente instantánea, un mismo correo puede ser enviado a varias personas a la vez, además de permitir enviar archivos de todo tipo. Sin embargo, en medio de tanta información, resulta interesante saber cuáles de los correos que recibimos son en realidad confiables y de nuestro interés.

Además de los correos personales, laborales y todos aquellos que responden a una solicitud realizada por nosotros, existen muchos otros de los cuales desconocemos su origen y el modo en que el remitente obtuvo nuestra dirección de correo electrónico. Al correo electrónico no solicitado y enviado masivamente por parte de un tercero, se le denomina *spam*. La vía más utilizada de envío de *spam* es la basada en el correo electrónico pero también puede presentarse por programas de mensajería instantánea o por teléfono celular.

El *spam* es utilizado, por lo general, para el envío de publicidad, aunque también se usa en la propagación de códigos maliciosos como son los virus. Además de los riesgos que representa el *spam* por el envío de contenidos dañinos, y por la molestia que causa al usuario recibir publicidad no deseada; también existen efectos colaterales de su existencia, tales como son la pérdida de productividad que genera en el personal la lectura de correo, y el consumo de recursos (ancho de banda, procesamiento, etc.) que generan este tipo de correos. En el 2008 el *spam* correspondió al 60.56% de incidentes reportados al UNAM-CERT.

Ante este panorama, resultaría útil encontrar alguna medida que nos proteja del envió masivo y malintencionado de correo electrónico. De esta forma se conoce como ***antispam*** a toda aquella aplicación o herramienta informática que se encarga de detectar y eliminar el *spam* y los correos no deseados. El objetivo principal de una herramienta *antispam* es el filtrar el tráfico de correo electrónico, eliminando el correo no deseado a la vez que detecta aquellos mensajes que son de nuestro interés permitiéndoles el paso a nuestra bandeja de entrada.

Las herramientas *antispam* utilizan diversos mecanismos para filtrar el correo no deseado. Algunas técnicas hacen uso de diccionarios, los cuales son consultados por la herramienta *antispam* en nuestro propio sistema y tienen como función el detectar palabras o patrones específicos que suelen aparecer en el correo *spam*. Este diccionario puede ser configurado de manera manual, con palabras y frases que el propio usuario relaciona con correos malintencionados, o puede ser producto de alguna aplicación diseñada para tal fin. Otra técnica es el uso de listas de confianza. De acuerdo con esta clasificación, los tipos más utilizados de listas son negras y blancas. Se definen como listas blancas a todas aquellas listas de direcciones de correo que se consideran de confianza y de las cuales el usuario siempre desea recibir correos. En el otro extremo están las listas negras, dentro de las cuales están identificados remitentes de correo *spam*. De este modo, el *antispam* se

encarga de bloquear el paso de los correos cuya dirección está contenida en alguna lista negra y de permitir el de las direcciones contenidas en las listas blancas.

Las técnicas remotas, a diferencia de las locales, utilizan herramientas que se conectan a servidores remotos, los cuales se encargan de determinar si un correo es *spam* o no. Estos servidores utilizan grandes bases de datos que contienen direcciones de correo electrónico, palabras, frases, entre otros patrones para identificar el correo electrónico no deseado. Existe una gran diversidad de productos que pueden ayudarnos a resolver el problema del *spam*, tanto versiones gratuitas como comerciales.

RECOMENDACIONES

No contribuyas con el envío de correo *spam*, siguiendo las siguientes recomendaciones:

1. **No** envíes mensajes en cadena, ya que estos mismos son generalmente algún tipo de engaño.
2. Si deseas enviar mensajes a muchos destinatarios hazlo **siempre** Con Copia Oculta (CCC), ya que esto evita que un destinatario vea y obtenga la dirección de correo de los demás destinatarios.
3. No publiques tu dirección de correo electrónico privada en sitios webs, foros, conversaciones online, etc. ya que sólo facilita su obtención a las personas que envían *spam*.
4. **Nunca** respondas mensajes de remitentes desconocidos, ya que con esto sólo estas confirmando tu dirección de correo provocando que recibas más correo basura.
5. Es bueno que tengas más de una cuenta de correo (al menos 2 o 3): una cuenta laboral que sólo sea utilizada para este fin, una personal y la otra para contacto público o de distribución masiva.

Referencias:

http://www.eset-la.com/centro-amenazas/amenazas/2178-Spam
http://www.segu-info.com.ar/malware/spam.htm
http://www.alegsa.com.ar/Dic/antispam.php
http://www.eset.com/products/nod32.php
http://www.symantec.com/es/mx/business/brightmail-message-filter
http://www.kaspersky.com/sp/anti-spam
http://home.mcafee.com/Store/
http://www.nominalia.com/email/antivantis_protection.html
http://www.masadelante.com/faqs/programas-anti-spam

Edgar Omar López Hernández

1. ¿Qué es el *software* de seguridad?

El *software* de seguridad es toda aplicación encargada de proteger la información dentro de nuestros equipos de cómputo, esto lo hace mediante la detección, bloqueo, eliminación y/o negación de la entrada de amenazas a la seguridad de la información. Existen herramientas para proteger los diversos aspectos que abarca la seguridad de la información: confidencialidad, integridad, disponibilidad.

2. ¿Existe *software* de seguridad gratuito?

Sí existe *software* de seguridad gratuito. Al obtenerlo, debemos de ser cuidadosos en cuanto a los sitios en donde lo descargamos, ya que algunas veces puede ser peligroso debido a la existencia de sitios web de descarga infectados con *malware*. Una buena opción es buscar si la herramienta cuenta con algún sitio propio para posteriormente realizar la descarga desde esta dirección.

3. ¿Cómo se compara la eficiencia del *software* de seguridad gratuito con el comercial?

La principal diferencia que se puede presentar entre las herramientas gratuitas y las comerciales es que en estas últimas siempre se cuenta con un soporte técnico especializado en caso de alguna falla. Las versiones comerciales suelen tener además, opciones más amplias de protección.

4. ¿Todos los sistemas necesitan *software* de seguridad?

De alguna u otra forma todos los sistemas necesitan *software* de seguridad. Es una opción muy recomendada para mantener protegida a nuestra computadora. Dependiendo el tipo de sistema que utilicemos, es como se va a elegir la herramienta de seguridad adecuada, tomando en cuenta además el uso que se le va a dar al equipo. No es lo mismo que se utilice como estación de trabajo que como servidor en producción. En sistemas Windows es necesario tener por lo menos una herramienta antivirus instalada. Algunas versiones cuentan ya con la instalación de *firewall* y *antispyware* por defecto.

5. ¿Si ya uso algún antivirus, también necesito un *firewall*?

Es recomendable que cada equipo conectado a la red cuente con un *firewall* de *host* (personal), además de los mecanismos de protección que puedan existir en la propia red local. Algunos antivirus ya cuentan con un módulo encargado de hacer la actividad de un *firewall*, es por eso que hay que hacer un estudio minucioso sobre las necesidades de seguridad que se requieren para un determinado equipo, dispositivo, etc., además de los beneficios que nos dan los *software* ya instalados.

6. ¿De qué me debo proteger?

Existen una gran variedad de amenazas a las que se está expuesto como usuario de Internet, como por ejemplo, una infección por virus, caballos de Troya, la posibilidad de caer en sitios web falsos o comprometidos, etc. En general a todo aquello que sea capaz de alterar el funcionamiento de nuestro sistema o comprometer nuestra información, por lo cual debemos tomar las medidas necesarias al momento de estar navegando en Internet mediante el uso de *software* de seguridad. Todo esto para evitar o prevenir, de la mejor forma posible, algún tipo de daño a nuestra computadora.

7. ¿Pueden los teléfonos celulares infectarse de algún virus?

No es tan común, pero sí se han presentado casos en donde los teléfonos celulares han sido infectados por virus que pueden llegar a provocar que el teléfono sea bloqueado o la denegación total del servicio, incluso también pueden ser atacados mediante el envío de mensajes *spam*. Se han reportado vulnerabilidades en la mayoría de los equipos de telefonía móvil, por lo que debemos estar al pendiente. Es recomendable también no dejar el *bluetooth* encendido siempre, esto aparte de que gasta la batería del equipo, también lo expone a algunos ataques como los que se presentan a las redes inalámbricas debido a que intercepta la información. Incluso existen programas con los que un intruso puede adueñarse del control total de tu equipo.

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castros
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

Ma. de Lourdes Velázquez Pastrana
Directora de Telecomunicaciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

M en I. Rocío del Pilar Soto Astorga
Edición

Edgar Omar López Hernández
Francisco Carlos Martínez Godínez
Miriam J. Padilla Espinosa
Javier Ulises Santillán Arenas
Miriam Valdés Rodríguez
Mayra Villeda Juárez
Colaboraciones

Ing. Rubén Aquino Luna
Responsable del Departamento de Seguridad en Cómputo UNAM-CERT

Rocío del Pilar Soto Astorga
Rubén Aquino Luna
Manuel I. Quintero Martínez
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico