ISSN 1390 – 7832

Rev. SINAPSIS, Vol. 5, Nº 2, Diciembre 2014

Estudio de metodologías para defensa contra virus informático que pueden dañar el equipo de cómputo

Metodología para la defensa contra virus

Bory Daniel Chilán Intriago [(1)]
Enrique Javier Macías Arias [(2)]

[(1)]Instituto Tecnológico Superior Portoviejo, Ecuador
[(2)] Instituto Tecnológico Superior Portoviejo, Ecuador

Contacto: **boris25chi@yahoo.com, enriquemacias21@hotmail.com**

Receptado: 03/07/2014 Aceptado: 04/010/2014

Resumen

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico donde se encuentren. En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes. No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información. El objetivo de esta investigación fue dar a conocer los resultados obtenidos sobre los métodos para defensa contra virus informático. En este trabajo se concluyó que el avance de la tecnología tanto en software como en hardware, ha hecho que los antivirus hayan evolucionado hacia mejores programas que no solo buscan detectar virus informáticos si no bloquearlos y desinfectarlos. Para el desarrollo de esta experiencia se realizaron encuestas a 69 Ingenieros en Sistemas y Administradores de centros de cómputo de la ciudad de Portoviejo, Ecuador. Se concluyó que La mayoría de usuarios adquieren los programas de antivirus mediante descargas de la web, o compra de programas piratas, los cuales no protegen totalmente al computador y en vez de volverse una ayuda se convierte en amenazas.

Palabras claves: antivirus, desinfectarlos, vulnerables, virus informáticos, software, hardware, centros de cómputo

Study of methodologies for defense against computer viruses that can damage computer equipment.

Abstract

One of the most striking changes in the world today is the speed of communication. Modern systems allow the flow of knowledge is independent of the physical location where they are. In that sense, no longer surprises transfer or instant real- time and because knowledge is power ; to acquire , companies have joined in large international networks to transfer data, sound and images, and make trade electronically in order to be more efficient. However, joining publicly have become vulnerable, as each computer system involved in the network is a potential target and appealing for information. The objective of this research was to present the results on methods of defense against computer viruses. This paper concluded that the advancement of technology both in software and hardware, has made the best antivirus programs have evolved to not only seek to detect viruses if no block and disinfection. For the development of this experience surveys to 69Ingenieros Systems and datacenter managers of Portoviejo, Ecuador ciudadde. It was concluded that most users purchase antivirus programs via web downloads, or buying pirated programs, which do not fully protect the computer and instead of becoming an aid becomes threats.

Keywords: antivirus, disinfect, vulnerable, computer virus, software, hardware, computer centers

Introducción

En el mundo globalizado, los cambios más sorprendentes es la rapidez de las comunicaciones. Modernos sistemas de información permiten que el flujo de conocimientos sea independiente del lugar físico en que se encuentren. No sorprende la transferencia de información en tiempo real o instantáneo dentro de una red LAN o a través de la nube.

Con mayor frecuencia se encuentran noticias sobre la violación de redes de importantes organizaciones por criminales informáticos desconocidos. A pesar de que la prensa ha destacado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. De manera permanente se reciben reportes de los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada y miles de contraseñas han sido capturadas a usuarios inocentes; por mencionar algunas cuestiones.

"El escenario electrónico actual es que las organizaciones están uniendo sus redes internas a la Internet, la que crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso a las redes de otras organizaciones también unidas." (Bentley, 2002)

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos o que han sido infectadas por virus. A pesar de que la prensa ha publicitado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. A diario se reciben reportes los ataques de virus a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar puertas traseras de entrada, y miles de contraseñas han sido capturadas a usuarios inocentes. (Gonzalez, Virus Informático, 2003)

El objetivo de esta investigación fue determinar las metodologías de defensa contra virus informáticos, que utilizan los Ingenieros en Sistemas Informáticos y Administradores de centro de cómputo.

Virus informáticos

Un virus informático es un malware, el cual significa malicious software, también llamado badware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario hecho maliciosamente por otra persona.

Estos malware tienen finalidades muy diversas ya que en esta categoría, encontramos desde un troyano hasta un spyware, los cuales son los programas de la actualidad que lo conforman.

Un virus informático es un programa de computadora, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Obviamente ahí termina todo su parecido con estos típicos programas que casi todo el mundo tiene instalados en sus computadoras, los virus tienen por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más benignos, que solo se caracterizan por ser molestos.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse.

Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a autorreplicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible. El virus toma el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución.

Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

Los virus informáticos son diseñados para propagarse de un equipo a otro y para interferir en el funcionamiento del equipo, puede dañar o eliminar datos del equipo, usar el programa de correo electrónico para propagarse a otros equipos o incluso borrar todo el7

contenido del disco duro, se propagan más fácilmente mediante datos adjuntos incluidos en mensajes de correo electrónico o de mensajería instantánea.

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción.
- Módulo de Ataque.
- Módulo de Defensa.

El módulo de reproducción se encarga de manejar las rutinas de parasitación de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

Características

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos, estos programas se diseminan por medio de réplicas y copias. Las redes en la actualidad ayudan a dicha propagación cuando éstas no tienen la seguridad adecuada, esto ocasiona pérdida de información, horas de parada productiva, tiempo de reinstalación, entre otros. Hay que tener en cuenta que cada virus plantea una situación diferente.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de booteo, menos comunes son los no residentes que no permanecen en la memoria después que el programa-huesped es cerrado. (Del Pino Gonzalez, 1991)

Los virus pueden llegar a camuflarse y esconderse para evitar la detección y reparación. Como lo hacen:

a. El virus re-orienta la lectura del disco para evitar ser detectado;
b. Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus;
c. Encriptamiento: el virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse DEBE desencriptarse siendo entonces detectable;
d. Polimorfismo: mutan cambiando segmentos del código para parecer distintos en cada "nueva generación", lo que los hace muy difíciles de detectar y destruir;
e. Gatillables: se relaciona con un evento que puede ser el cambio de fecha, una determinada combinación de tecleo; un macro o la apertura de un programa asociado al virus Troyanos.

Aunque clasificar el malware puede resultar agotador y profundo, puede resumirse en:

✓ Virus informáticos, los cuales a su vez se sub clasifican en:

De programas ejecutables:

Estos virus basan su principio en que MS-DOS ejecuta en primer lugar el archivo con extensión COM frente al de extensión EXE, en el caso de existir dos archivos con el mismo nombre pero diferente extensión dentro del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar.

Después ejecuta el nuevo archivo COM, creado por el virus, y cede el control al archivo EXE. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.

Residentes en memoria

También llamados TSR por Terminate and StayResident (Terminar y permanecer residente en la memoria) se cargan en la RAM del ordenador para infectar los archivos ejecutables abiertos por el usuario. Los virus no residentes, una vez ejecutados, infectan programas que se encuentran en el disco duro

De sector de arranque

Utilizan el sector de arranque, el cual contiene la información sobre el tipo de disco, es decir, numero de pistas, sectores, caras, tamaño de la FAT, sector de comienzo, etc. A todo esto hay que sumarle un pequeño programa de arranque que verifica si el disco puede arrancar el sistema operativo. Los virus de Boot utilizan este sector de arranque para ubicarse, guardando el sector original en otra parte del disco. En muchas ocasiones el virus marca los sectores donde guarda el Boot original como defectuosos; de esta forma impiden que sean borrados. En el caso de discos duros pueden utilizar también la tabla de particiones como ubicación. Suelen quedar residentes en memoria al hacer cualquier operación en un disco infectado, a la espera de replicarse. Como ejemplos representativos está el Brain.

Macrovirus o virus de macro

Un macro es una secuencia de órdenes de teclado y mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y no actuarán hasta que el archivo se abra o utilice.

De correo electrónico

Uno de los más importantes medios de comunicación en la actualidad es el correo electrónico. Mediante él podemos enviar información en tiempo real a cualquier destinatario en cualquier lugar del mundo. Eso lo convierte en una poderosa herramienta, y a su vez en un peligro potencial, ya que los virus informáticos se propagan a través del correo electrónico.

Gusanos (worm)

Los Worms o gusanos se registran para correr cuando inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.

Troyanos (trojanhorse)

Troyanos: suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos. Funcionan de modo similar al Caballo de Troya; ayudan al atacante a entrar al sistema

infectado, haciéndose pasar como contenido genuino (salva pantallas, juegos, música). En ocasiones descargan otros virus para agravar la condición del equipo.

Exploits

Es un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs) una de las herramientas más utilizadas para realizar este tipo de ataque informático es el Metasploit que se encuentra en su última versión.

Rootkits

Un rootkit es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos. Existen rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows.

Backdoors

En la informática, una puerta trasera (o en inglés backdoor), es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema.

Estas puertas también pueden ser utilizadas para fines maliciosos y espionaje.

Keyloggers

Un keylogger (deriva del inglés: Key (Tecla) y Logger (Registrador); registrador de teclas) es una herramienta de diagnóstico utilizada en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero y/o enviarlas a través de internet. Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan a cceso a los números de una tarjeta de crédito o a la contraseña de cuentas on line al infiltrarse en un ordenador.

Ransomware

Es un malware generalmente distribuido mediante spam y que mediante distintas técnicas imposibilita al dueño de un documento acceder al mismo. El modo más comúnmente utilizado es cifrar con clave dicho documento y dejar instrucciones al usuario para obtenerla, posterior al pago de "rescate".

Spam

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups y todo tipo de imágenes y textos en la web.

Ciclo de vida de un Virus

El ciclo de vida de un virus empieza cuando se crea y acaba cuando es completamente erradicado. A continuación describimos cada una de las fases,

Creación

Hasta hace poco tiempo, la creación de un virus requería el conocimiento de lenguajes de programación avanzados. Hoy cualquiera con simples conocimientos de programación básica puede crear un virus. Típicamente son individuos con afán de protagonismo los que crean los virus, con el fin de extender al azar el efecto nocivo de su creación.

Réplica

Los virus no suelen ser activos en el momento de su creación, sino que poseen un tiempo de espera (incubación), lo que les permite extenderse ampliamente antes de ser detectados.

Activación

Los virus con rutinas dañinas se activan cuando se dan ciertas condiciones, por ejemplo, en una determinada fecha o cuando el usuario infectado realiza una acción particular. Los virus sin rutinas dañinas no tienen activación, causando de por si el daño, como la ocupación del espacio de almacenaje.

Descubrimiento

Esta fase no siempre sigue a la activación. Cuando se detecta un virus, este se aísla y se envía al ICSA en Washington, D.C., para ser documentado y distribuido a los fabricante de software antivirus. El descubrimiento suele realizarse antes de que el virus pueda convertirse en una amenaza para la comunidad informática.

Asimilación

En este punto, los fabricantes de software antivirus modifican este para que pueda detectar el nuevo virus. Este proceso puede durar de un día a seis meses, dependiendo del fabricante y el tipo del virus.

Erradicación

Si multitud de usuarios instalan un software de protección actualizado, cualquier virus puede eliminarse definitivamente. Aunque hasta ahora ningún virus ha desaparecido por completo, algunos hace tiempo que han dejado de ser una amenaza.

Métodos de prevención de virus informáticos

- ✓ Los virus informáticos pueden evitarse de múltiples maneras, una de ellas es no utilizar software que se tenga duda de su procedencia, otra es evitando el intercambio de información de una computadora a otra, si ésta no es confiable (Interlink, Internet, Red Local, etc.).
- ✓ Evite usar discos de procedencia desconocida sin antes haberlos revisado y que no contengan virus; de hacerlo, se deben verificar éstos previamente con un programa antivirus, esto no asegura la completa limpieza de virus, ya que los programas antivirus sólo revisan a los virus que pueden reconocer, si un virus es más reciente que el programa antivirus este no lo detecta. Además, la mejor recomendación es usar software original.
- ✓ Para evitar la pérdida de información por virus o cualquier otro evento que pueda dañar sus datos, lo recomendable es hacer respaldos periódicos y constantes de su información. No

tener archivos de texto muy grandes, como una tesis o reporte de proyecto de investigación en un solo archivo.

Activos

Antivirus: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección no tificando al usuario de posibles incidencias de seguridad.

Filtros de ficheros: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

Pasivos

- ✓ Evitar introducir a tu equipo medios de almacenamiento removibles que consideres que pudieran estar infectados con algún virus.
- ✓ No instalar software "pirata".
- ✓ Evitar descargar software de Internet.
- ✓ No abrir mensajes provenientes de una dirección electrónica desconocida.
- ✓ No aceptar e-mails de desconocidos.

Antivirus

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada. .

La técnica de scanning fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.

Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades.

Modelo Antivirus

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado de control y el segundo denominado de respuesta. A su vez, cada uno de ellos se divide en varias partes:

a. Módulo de control: posee la técnica verificación de integridad que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

   Otra opción dentro de este módulo es la identificación de virus, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.

   Asimismo, la identificación de código dañino es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.

   Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

b. Módulo de respuesta: la función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Materiales y Métodos

Lugar y períodos de desarrollo del experimento.

La investigación se realizó en la ciudad de Portoviejo, a Ingenieros en Sistemas y Administradores de centros de cómputo.

Muestra.

Para la puesta en marcha de la investigación, se encuestaron a 69 personas, ingeniero en sistemas y administradores de centros de cómputo.

Instrucciones metodológicas.

Podemos decir que la investigación científica se define como la serie de pasos que conducen a la búsqueda de conocimientos mediante la aplicación de métodos y técnicas y para lograr esto nos basamos en los siguientes.

Exploratoria: Son las investigaciones que pretenden darnos una visión general de tipo aproximativo respecto a una determinada realidad.

Todo el proceso fue llevado a cabo mediante el empleo del método de la encuesta, que nos permitió sacar nuestras conclusiones respecto a combatir de manera más segura contra los ataques de los virus informáticos.

Análisis estadístico. El análisis estadístico se desarrolló mediante porcentajes y gráficos estadísticos: los datos se compararon a través de una tabla con los indicadores necesarios y su grafica respectiva.

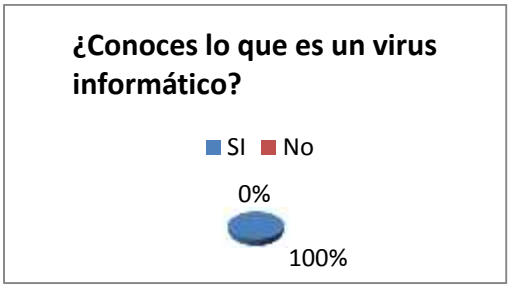
Resultados

¿CONOCES LO QUE ES UN VIRUS INFORMÁTICO?

CUADRO #1

	)	)0%
)		%
)tal	)	)0%

GRAFICO ESTADÍSTICO



RESUMEN

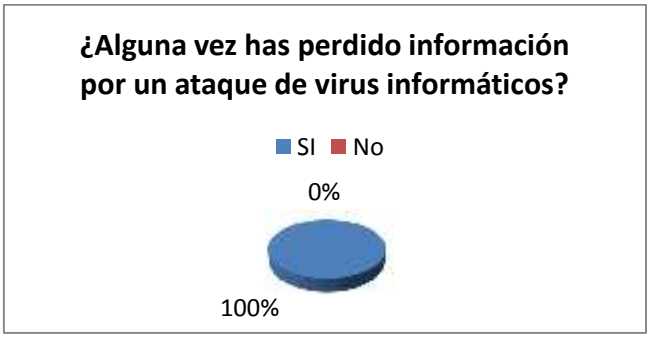
Como es común todo ingeniero en sistemas o administrador de centros de cómputo conocen que es un virus informático, dando un 100% de conocimiento, mientras que el 0 % indica que todos están conscientes de lo que es un virus, así lo muestra la gráfica estadística.

2. ¿ALGUNA VEZ HAS PERDIDO INFORMACIÓN POR UN ATAQUE DE VIRUS INFORMÁTICOS?

CUADRO #2

		0%
		%
tal		0%

GRAFICO ESTADÍSTICO



RESUMEN Como se muestra la gráfica los ingenieros en Sistemas que se entrevistaron dijeron de manera general que si perdieron información por culpa de un virus informático, mientras que el 0% indica que nadie ha pasado problemas con los virus informáticos.

¿TIENES PRECAUCIÓN AL INGRESAR DISPOSITIVOS EN LOS COMPUTADORES?

CUADRO #3

		0%

ɔ		%
ɔtal	)	)0%

GRAFICO ESTADISTICO

RESUMEN

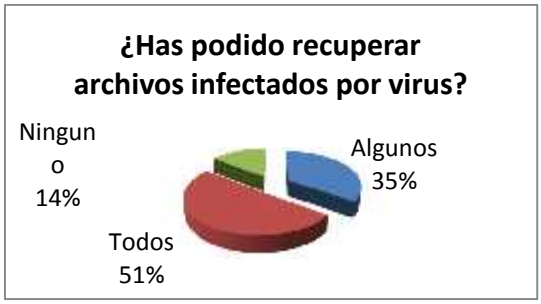
Como se muestra la gráfica los ingenieros en Sistemas que se entrevistaron dijeron de manera general el 100% dijo que tenían precaución al ingresar dispositivos en los computadores.

¿HAS PODIDO RECUPERAR ARCHIVOS INFECTADOS POR VIRUS?

CUADRO #4

ɹgunos	-	ɔ%
ɔdos	ɔ	ɹ%
ɹnguno	)	ɬ5
ɔtal	)	)0%

GRAFICO ESTADISTICO



RESUMEN

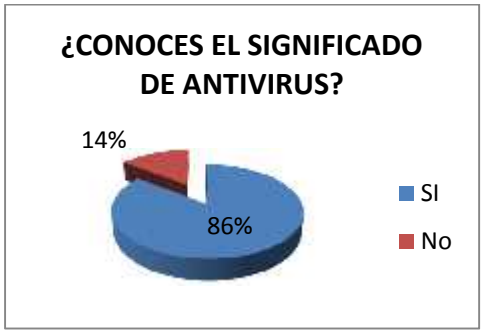
Según la pregunta que si ha podido recuperar información luego de que el virus la ha borrado, los encuetados respondieron que el 35% recupero algunos archivos, el 51% recupero todo mientras que el 14% dijeron que ningún archivo pudo recuperar.

¿CONOCES EL SIGNIFICADO DE ANTIVIRUS?

CUADRO #5

	)	.51%
o	)	.49%
otal	)	0.00%

GRAFICO ESTADISTICO



RESUMEN

Según la pregunta de que si conoce el significado de antivirus, el resultado arrojo que el 69.57% respondió que sí y el 30.43% respondió que no conoce el verdadero significado

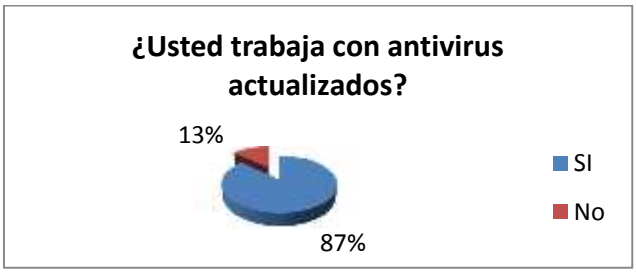
¿Usted trabaja con antivirus actualizados?

CUADRO #6

	)	%

ɔ		%
ɔtal	)	0%

GRAFICO ESTADISTICO



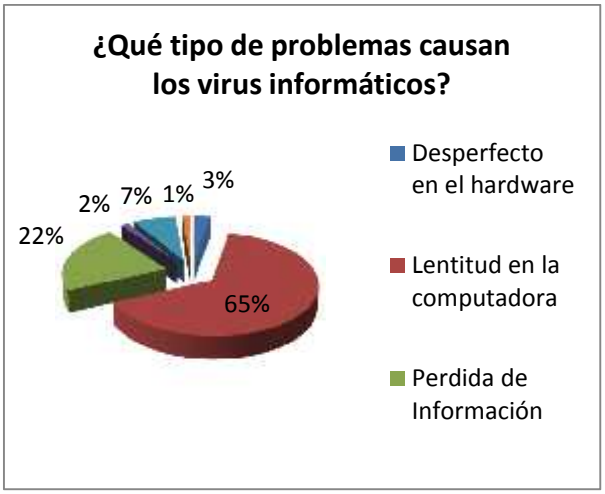
RESUMEN Según la pregunta de que trabaja con antivirus actualizados, el resultado arrojo que el 87% respondió que sí trabaja con antivirus actualizados y el 13% respondió que no trabaja con antivirus actualizados.

¿Qué tipo de problemas causan los virus informáticos?

CUADRO ESTADÍSTICO

esperfecto en el hardware		%
ntitud en la computadora		%
rdida de Información		%
rdida de Unidades		%
rmateo de Unidades		%
raso en la presentación de trabajos		%
	)	0%

GRAFICO ESTADISTICO



RESUMEN

Según la pregunta ¿Qué tipo de problemas causan los virus informáticos?, tenemos los siguientes resultados. Desperfecto de hardware con el 3%, lentitud en la computadora 65%, perdida de información 22%, perdida de unidades 1%, formateo de unidades 7% y el atraso en la presentación de trabajos 1%.

¿Sabes que es un Spyware?

CUADRO ESTADÍSTICO

	)	%)
)	)	%)
otal	)	0%)

GRAFICO ESTADISTICO

RESUMEN

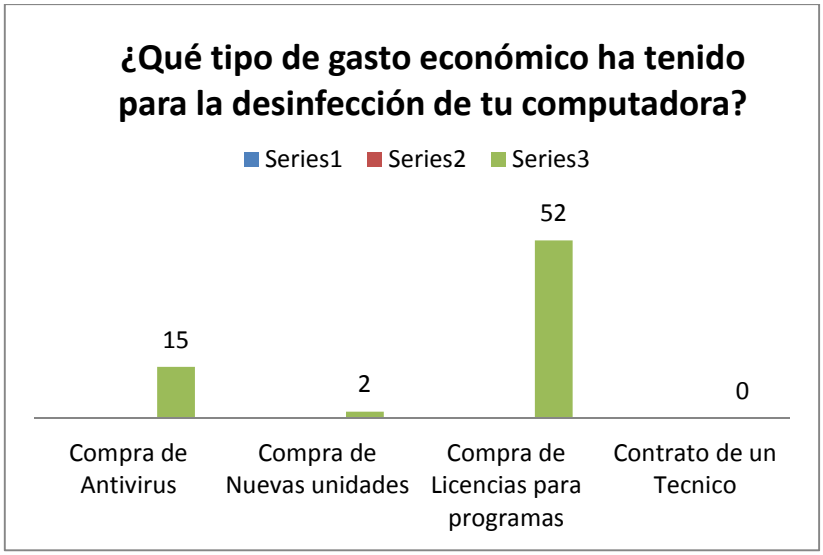
Según la pregunta de que si conoce que es un Spyware, el resultado arrojo que el 58% respondió que sí trabaja con antivirus actualizados y el 42% respondió que no conoce un Spyware.

¿Qué tipo de gasto económico ha tenido para la desinfección de tu computadora?

CUADRO ESTADÍSTICO

ompra de Antivirus		%
ompra de Nuevas unidades		%
ompra de Licencias para ogramas		%
ontrato de un Tecnico		%
otal		0%

GRAFICO ESTADISTICO



RESUMEN Sobre la pregunta de ¿Qué tipo de gasto económico ha tenido para la desinfección de tu computadora?, tenemos los resultados de compra de antivirus 22%, compra de nuevas unidades 3%, compra de licencias para programas 75%, contrato de un técnico 0%.

¿Estás consciente de la importancia de escanear el computador constantemente para evitar infecciones de virus informáticos?

CUADRO ESTADÍSTICO

		0%
ɔ		%
ɔtal		0%

GRAFICO ESTADISTICO

RESUMEN

Según la pregunta de que si ¿Estás consciente de la importancia de escanear el computador constantemente para evitar infecciones de virus informáticos, el resultado arrojo que el 58% respondió que sí trabaja con antivirus actualizados y el 42% respondió que no conoce un Spyware.

Conclusiones y recomendaciones

Es muy importante tener pleno conocimiento de las necesidades de cada organización y de cada usuario; pues de estas necesidades depende el tipo de antivirus que debe estar instalado en los ordenadores debido a que no existen antivirus ni malos ni buenos, el grado de eficiencia de estos depende de las necesidades que deba suplir.

Es indispensable para cualquier usuario de sistemas informáticos contar con una protección antivirus que garantice una seguridad a la hora de enfrentarse a este tipo de ataques maliciosos. Se debe conocer muy bien el funcionamiento de los virus existentes y sus formas de actuar, debido a que de ellos depende la protección a la cual nuestro sistema estará expuesto.

Prever la forma en las que los virus se propagan y los sitios del sistema a los cuales afectara no es algo fácil de saber, por lo que es importante comprender su funcionalidad y generalidades de estos, para llegar a unas medidas de seguridad que garanticen una buena protección antivirus.

Una buena opción para prevenir y controlar gran cantidad de virus es educar a los usuarios de sistemas informáticos, informándoles que deben hacer en el momento en que se enfrente ante ataques sospechosos y así detener y evitar la propagación de virus informáticos

En cuanto a las empresas es de vital importancia implementar políticas de seguridad informática, ya que con estas sería más fácil la identificación del problema pues con el desarrollo de las mismas se podrían hacer análisis de la seguridad en los equipos de cómputo.

Algo más seria hacer auditorias y revisiones de los sistema de seguridad. Es de suma importancia contar con antivirus que actualicen constantemente las firmas de virus existentes en tiempo real, esto hará mucho más efectivo el nivel de protección del sistema

Bibliografía

1. Benitez, J. (2014). Hasta 4 000 virus informáticos amenazan al día al computador. *El Comercio*, pág. 16.

2. Bentley, A. (2002). *La Actitud del Educador.* Buenos Aires: Victor Leru.

3. Del Pino Gonzalez, J. (1991). *Virus Informático.* Madrid: Paraninfo.

4. Gonzalez, D. P. (1991). *Virus Informatico.* Madrid: Paraninfo.

5. Gonzalez, D. P. (2003). *Virus Informático.* Madrid: Paraninfo.

6. Levin, R. (1991). *Virus Informático: Tipos, Protección, Diagnosis, Soluciones.* Madrid: Paraninfo.

7. Levin, R. (1991). *VIRUS INFORMATICOS: TIPOS, PROTECCION, DIAGNOSIS, .* Madrid: Paraninfo.

8. Lopez, A. (2000). *Enciclopedia Interactiva Estudiantil siglo XXI.* Madrid.

9. Pablos Heredero, C. (2002). *Informática y comunicaciones en la empresa.* Madrid: Brosmac.

10. Pons. (1994). *La Tecnlogía.* Madrid.

11. Quesada. (1990). *Técnica y la ciencia.* Mexico.

12.Sarramona. (1994). *Técnicas de Virus.* Madrid.