Educación y Sociedad
UCP "Manuel Ascunce Domenech"
Revista Digital. Año 12 - Número 2. Abr-Jun 2014.

Seguridad informática: un reto para los usuarios de los sistemas informáticos

Informatic security: a challenge for computer system clients

Fecha de recibido: 14 de febrero de 2014. Fecha de aprobado: 27 de marzo de 2014. Resultado de formación académica de maestría del autor.

Autor:

Erlys Durán Rodríguez. Lic. en Educación, especialidad Matemática – Computación. Asistente. Profesor de la Universidad de Ciencias Pedagógicas "Manuel Ascunce Domenech" de Ciego de Ávila. Posee publicaciones en revistas nacionales e internacionales. Ha participado en eventos territoriales y nacionales de seguridad informática. Imparte la asignatura Software Geogebra. erlys@ucp.ca.rimed.cu

Resumen

Sobre la base de las limitaciones en el cumplimiento del objetivo de la seguridad informática, en el presente artículo se ofrecen las posibles amenazas y riesgos sobre los activos y recursos informáticos, se precisan acciones en relación con los tres elementos básicos del sistema informático: hardware, software y los datos; de ahí que el objetivo de este artículo está dirigido a ofrecer acciones que permiten identificar las amenazas y riesgos en los activos y recursos informáticos en la Universidad de Ciencias Pedagógicas "Manuel Ascunce Domenech".

Palabras clave: seguridad informática, riesgos, hardware, software

Abstract

Upon the basis of some limitations dealing with the accomplishment of the security objective, in this paper the objectives, and the possible risks and threats of the informatics devices are given as well as the actions in relation to the three basic elements of the system: hardware, software and data; thus the objective of this article is to give some actions for the identification of risks and threats in the informatics resources at "Manuel Ascunce Domenech" University of Pedagogical Sciences.

Key words: informatic security, risks, hardware, software

Introducción

Hasta la aparición y difusión del uso de los sistemas informáticos toda la información de interés de una organización se preservaba en papel y se almacenaba en grandes cantidades de abultados archivadores; datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesamiento; sin embargo los sistemas informáticos permiten la digitalización de todo el volumen de información, se reduce el espacio, y facilita su análisis y procesamiento; de igual manera se gana en rapidez en el manejo de la información y se mejora la presentación de la misma.

Las tecnologías de la información han sido conceptualizadas como la integración y convergencia de la computación, microelectrónica, las telecomunicaciones y las técnicas para el procesamiento de datos. Se reconocen como sus principales componentes el factor humano, los contenidos de la información, el equipamiento, la infraestructura material, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulaciones, y los recursos financieros.

No obstante de sus ventajas, el amplio desarrollo de las tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas incoherentes y delictivas que se ofrecen la posibilidad de cometer delitos. Es por esta razón que lograr estándares en el mundo altamente tecnificado de hoy es quizás la principal barrera con las que se enfrentan los profesionales para garantizar la seguridad informática; por otra parte, la situación internacional actual exige la concientización de todos de que la información es conocimiento y como tal se le debe atribuir la importancia que merece.

En la sociedad actual se reconoce el papel desempeñado por las tecnologías de la información como núcleo central de la transformación multidimensional que experimenta la economía y la sociedad, por lo que resulta importante el estudio y dominio de las influencias que esa transformación impone al ser humano como ente social porque tiende a modificar no sólo sus hábitos y patrones de conducta, sino su forma de pensar. La seguridad informática juega un papel decisivo en la sociedad cubana, pues en este contexto la seguridad informática es la característica que indica que un sistema está libre de todo peligro, daño o riesgo, dicha información tiene relevancia especial, que en un contexto determinado se debe proteger.

Las necesidades de la seguridad informática están encaminadas a identificar las amenazas y riesgos sobre los activos y recursos informáticos, en precisar qué acciones deben ser tomadas en cuenta, en determinar las responsabilidades, establecer las políticas, medidas y procedimientos para la seguridad de la información.

En correspondencia con lo anteriormente expuesto, en las inspecciones realizadas se constató que existen dificultades en el estricto cumplimiento de la seguridad informática en las redes, por lo que el objetivo de este artículo está dirigido a ofrecer acciones que permiten identificar las amenazas y riesgos sobre los activos y recursos informáticos en la Universidad de Ciencias Pedagógicas "Manuel Ascunce Domenech".

El análisis y estudio de los controles de seguridad informática para el cumplimiento de lo establecido en el código de ética, el plan de seguridad informática de la universidad, y el marco legal vigente en Cuba permitieron obtener los resultados a través de diversos métodos y técnicas como controles al uso de la red por parte de los usuarios, observación directa e indirecta, y encuesta a usuarios de la red.

Desarrollo

Establecer el valor de la información es relativo porque constituye un recurso que, en muchos casos, no se valora adecuadamente como consecuencia de su intangibilidad, premisa que no ocurre con los equipos, las aplicaciones y la documentación.

La información que se conserva a través de los recursos informáticos puede clasificarse según sus características en: clasificada, limitada y ordinaria. A continuación se explicitan sus características.

La información clasificada es aquella cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para el Estado o para su desarrollo político, militar, económico, científico, técnico, cultural, social o de cualquier otro tipo; la información limitada por su importancia para el objeto social de la entidad no resulta conveniente su difusión pública y debe limitarse su acceso a personas determinadas por el jefe de la entidad, y la información ordinaria es la que su conocimiento o divulgación no autorizada no produce daños o riesgos para el funcionamiento de la entidad.

Como consecuencia de la amplia difusión de la tecnología informática, la información puede utilizarse para fines poco éticos, puede divulgarse sin autorización de su propietario, estar sujeta a robos, sabotaje o fraudes y puede ser alterada, destruida y mal utilizada.

A partir de lo anteriormente expuesto en el artículo, a continuación se destacan los objetivos fundamentales que rigen la seguridad informática, entre estos el referido a mantener la protección contra la divulgación no autorizada de la información, la destrucción o alteración no autorizada de la información, y la manipulación no autorizada de los recursos informáticos. La seguridad informática se fundamenta en tres características que debe cumplir todo sistema informático, estas son: la confidencialidad, la integridad, y la disponibilidad.

La confidencialidad se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático; basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, que son aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados. La privacidad o confidencialidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño, volverse obsoleta.

La integridad es la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático; en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio tiene mayor recurrencia en sistemas descentralizados en los que diferentes usuarios, computadores y procesos comparten la misma información.

La integridad de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos o modificación por personas que se infiltran en el sistema.

La disponibilidad se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático; sobre la base de este principio, las

herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, es primordial en los sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente. La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

En correspondencia con lo anteriormente expuesto, existen algunos mecanismos y estrategias a seguir para mantener una adecuada seguridad informática, que se les denominan principios básicos de seguridad informática, estos son:

• Mínimo privilegio: se deben otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran, ni más ni menos de lo solicitado.

• Eslabón más débil: la seguridad de un sistema es tan fuerte como su parte más débil. Un atacante primero analiza cuál es el punto más débil del sistema y concentra sus esfuerzos en ese lugar.

• Proporcionalidad: las medidas de seguridad deben estar en correspondencia con lo que se protege y con el nivel de riesgo existente. No sería lógico proteger con múltiples recursos un activo informático que no posee valor o que la probabilidad de ocurrencia de un ataque sobre el mismo es muy baja.

• Dinamismo: la seguridad informática no es un producto, es un proceso. No se termina con la implementación de los medios tecnológicos, se requiere permanentemente monitoreo y mantenimiento.

• Participación universal: la gestión de la seguridad informática necesita de la participación de todo el personal de una institución. La seguridad que puede ser alcanzada mediante medios técnicos es limitada y debiera ser apoyada por una gestión y procedimientos adecuados que involucren a todos los individuos.

El control sobre la información es cualquier medida de seguridad que se define para manejar algún riesgo, lo que permite asegurar que solo los usuarios autorizados pueden decidir cuándo y

cómo permitir el acceso a la misma. Por otro lado, la autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución; también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Para realizar el análisis de la seguridad informática se deberán conocer las características de lo que se pretende proteger: la información, que constituye una agregación de datos que tiene un significado específico más allá de cada uno de estos, y tendrá un sentido particular según cómo y quién la procese, (Toffler, 1998), definición que se asume en este artículo.

Adicionalmente, se pueden considerar algunos aspectos relacionados con los anteriores, pero que incorporan otros particulares, como son:

- Protección a la réplica: se asegura que una transacción solo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- No repudio: se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- Aislamiento: íntimamente relacionado con la confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- Auditoria: es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.

Las amenazas en el contexto informático son cualquier elemento que comprometa al sistema. A continuación se destacan las amenazas que repercuten negativamente en la seguridad informática, por su origen se clasifican en accidentales o intencionales, dentro de las accidentales están las provocadas por causas naturales, laborales o sociales, y dentro de las intencionales se encuentran las internas y externas.

Entre las amenazas naturales se identifican las tormentas eléctricas, las inundaciones, y los incendios. Entre las causas laborales o sociales están:

1. Fallo de software.

2. Fallo de hardware.

3. Fallo de energía eléctrica.

4. Destrucción de la información.

5. Errores de operación.

6. Fuga de información.

7. Accesos no autorizados.

8. Acceso no autorizado a los bienes informáticos

Las amenazas por causas internas o externas están ataque de virus, gusanos y troyanos, así como hurto, traslado o pérdida de bienes.

No son éstas las únicas amenazas que acechan el sistema informático, pero sí son las que se han identificado con mayor probabilidad de materializarse y producir un impacto negativo; el análisis sistemático de las bitácoras y de los registros de incidencia de la seguridad informática proporciona información suficiente para perfeccionar el estudio de vulnerabilidades.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad del sistema informático.

• La prevención: mecanismo que aumenta la seguridad o fiabilidad de un sistema durante su funcionamiento normal.

• La detección: mecanismo orientado a revelar violaciones en la seguridad, generalmente son programas de auditoria.

• La recuperación: mecanismo que se aplica cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal.

Las preocupaciones que deben tenerse en cuenta ante un problema de seguridad en los sistemas de información, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, solo lo transforma o retrasa. La amenaza o riesgo continúa vigente.

La probabilidad de que se produzca un daño, o que una amenaza conlleve a una vulnerabilidad en el sistema informático se denomina riesgo, que se clasifican en:

1. Proximidad de un daño dentro de este se encuentran:

• Robo de información.

• Pérdida de datos.

• Robo, pérdida de equipos.

• Violación del perímetro de red.

• Virus, troyanos y demás malware.

• Ataque de denegación de servicio, ataques basados en vulnerabilidades.

2. Circunstancias que disminuyen el beneficio:

• Estabilidad de la plataforma software más hardware.

• Desconfiguración, reinstalación de equipos.

• Disminución del rendimiento del usuario.

• Abuso de recursos para uso propio del empleado.

• Aumento del costo total de propiedad del dispositivo.

Por lo que minimizar el riesgo es una tarea de control permanente de la seguridad informática, de ahí que la política más adecuada para controlar el riesgo es la de minimizarlo y minimizar el impacto de la amenaza.

El riesgo puede ser atacado de las siguientes maneras:

• Minimizando la posibilidad de su ocurrencia.

• Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.

• Diseño de métodos para la más rápida recuperación de los daños experimentados.

• Corrección de las medidas de seguridad en función de la experiencia recogida. Luego, el daño es el resultado de la amenaza; aunque esto es sólo la mitad del axioma.

El daño también es el resultado del no accionar, o el accionar de manera incorrecta del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza. De allí que se deriven responsabilidades para la amenaza, y también para la figura del protector. El protector será el encargado de detectar cada una de las vulnerabilidades del sistema que pueden ser explotadas y empleadas, por la amenaza para comprometerlo; también será el encargado de aplicar las contramedidas adecuadas.

La seguridad indicará el índice en que un sistema informático está libre de todo peligro, daño o riesgo, lo que es muy difícil de conseguir, por lo que solo se habla de sistema fiable en vez de sistema seguro. Para garantizar que un sistema sea fiable se deberá conocer qué queremos proteger, de quién queremos protegerlo y cómo se puede lograr esto, para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos.

El conocimiento y la comprensión de la seguridad ayudará a analizar los riesgos, las vulnerabilidades, amenazas y contramedidas, también permite evaluar las ventajas o desventajas de la situación, a decidir medidas técnicas y físicas, e informáticas, sobre la base de las necesidades de seguridad. Todas estas técnicas parten de la premisa de que no existe la seguridad total o deseable en estas circunstancias.

Las funciones que se deben asegurar en un sistema informático son de reconocimiento de cada usuario que deberá identificarse al usar el sistema, y cada operación del mismo será registrada con esta identificación de integridad, sin embargo el aislamiento ocurre cuando los datos utilizados por un usuario deben ser independientes de los de otro, física y lógicamente, y el sistema puede ser auditado, utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones.

El sistema informático debe estar bajo control permanentes, y en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados, lo que permitirá conocer, en todo momento, cualquier suceso de forma tal de mantenerlo actualizado contra nuevas amenazas. Se reconocen tres elementos básicos que se deben proteger en el sistema informático: el hardware, el software y los datos.

Cuando se refiere al hardware, se hace referencia a todas las partes tangibles de un sistema informático donde sus componentes son, electromecánicos y mecánicos, son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado, como puede ser el

conjunto formado por la unidad central de procesamiento, impresoras, CD–ROM, cintas, componentes de comunicación.

La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento, que están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso del ordenador, el microprocesador que controla la computadora y le proporciona la capacidad de cálculo.

Contrariamente, el soporte lógico es intangible y se denomina software, el cual consiste en el conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en la computadora. Las dos categorías primarias del software son: software del sistema el cual incluye los sistemas operativos, que controlan los trabajos del ordenador o computadora, y la otra categoría es software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras. Por lo tanto, el software del sistema procesa tareas tan esenciales, que a menudo son invisibles, como el mantenimiento de los archivos del disco y la administración de la pantalla, mientras que el software de aplicación lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares. http://es.wikipedia.org/wiki/Hardware

Se entiende por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos. De los tres elementos, los datos que maneja el sistema serán los más importantes porque son el resultado del trabajo realizado. Si existiera daño del hardware o software, estos pueden adquirirse nuevamente, pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar, de ahí que se debe hacer obligatoriamente un sistema de copias de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño. http://es.wikipedia.org/wiki/Hardware

Para cualquiera de los elementos descritos existen gran variedad de amenazas y ataques que se pueden clasificar en:

• Ataques pasivos: el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, generalmente se emplean para obtener el origen y destinatario de la comunicación.

• Ataques activos: estos implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos.

Seleccionar las medidas de seguridad para ponerlas en práctica requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la amigabilidad para el usuario; esto significa que la seguridad y la utilidad de una computadora son inversamente proporcionales; al incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

El control de acceso ocupa un importante lugar en el desarrollo de la seguridad informática. Para que el sistema autentique a un usuario hay que disponer y exhibir:

• Algo que se conoce.

• Nombre de usuario y clave de acceso.

• Algo que se posee.

• Algo que se es, una característica personal y única.

Lo ideal es hacer una combinación de dos factores. Es un conjunto de caracteres escrito por el usuario siguiendo una norma preestablecida que lo identificará ante el sistema informático. Debe ser personal, secreta, intransferible, modificable solo por su titular y difícil de descubrir; sin embargo existen riesgos inherentes a la clave, como son la pérdida u olvido de la misma, la sustracción por parte de un tercero, no renovación periódica de la clave, y descuidos en su operación.

Para construir una clave de acceso es necesario tener en cuenta ciertas normas que como son no utilizar palabras comunes ni nombres de fácil deducción por terceros: los nombres de mascota, nombre personal o de un familiar cercano, no vincularlas a una característica personal: teléfono, carné de identidad, licencia de conducción del automóvil, no utilizar terminología técnica conocida: *admin*, *root*, etc.; debe combinar caracteres alfabéticos, mayúsculas y minúsculas, números y caracteres especiales, construirlas utilizando al menos de seis a ocho caracteres, y usar claves distintas para máquinas diferentes o sistemas diferentes.

A continuación se sugieren otras normas que no por ser cotidianas deben tenerse en cuenta para el uso de las claves de acceso, estas pueden ser:

• Evite que no vean su clave cuando la escribe.

• No observe a otros mientras lo hacen.

• No escriba la clave en papeles, ni en archivos sin cifrar.

• No comparta su clave con otros.

• No pida la clave de otro.

• No habilite la opción de recordar claves en los programas que utilice.

• Si por algún motivo tuvo que escribir la clave, no la deje al alcance de terceros debajo del teclado, en un cajón del escritorio, y nunca pegada al monitor.

• Nunca envíe su clave por correo electrónico ni la mencione en una conversación, ni se la entregue a nadie, aunque sea o diga ser el administrador del sistema.

• No mantenga una contraseña indefinidamente. Cámbiela regularmente, aunque las políticas de administración de claves no lo obliguen.

Se hace oportuno mencionar algunas normas mínimas para el administrador de las claves de acceso por lo que no debe existir ninguna cuenta sin contraseña, si es administrador del sistema, revisar periódicamente el sistema de claves y utilizar fechas de vencimiento, no permitir el uso de las contraseñas que, por defecto, genera y adjudica el sistema. Obligar al cambio cuando se da de alta al usuario y periódicamente de acuerdo con las normas vigentes, así como no dudar en cambiar las contraseñas, si se sospecha que alguien puede conocerla.

Las medidas antes mencionadas son de importancia para la protección de los datos y aplicaciones, sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultad en recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Los sistemas informáticos deben ser protegidos de los virus, conocidos como pequeños programas, invisibles para el usuario, no detectables por el sistema operativo, y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas completas de sí mismos, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa, susceptibles de mutar; resultando de dicho proceso la modificación, alteración o destrucción de los programas, información o hardware afectados.

Otro de los objetivos de los virus informáticos es alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario; estos habitualmente reemplazan archivos ejecutables por otros infectados con su código. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, son muy nocivos y algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

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, incluso cuando el programa que lo contenía haya terminado de ejecutarse, el virus toma entonces 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 programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

Algunos virus pueden causar efectos indeseables y otros dañar el hardware, software o archivos, pueden de igual forma modificar el funcionamiento de las computadoras, borrar o arruinar información, consumir memoria, entre otras acciones dañinas. El efecto más negativo de un virus es su auto-reproducción incontrolable que sobrecarga todos los recursos del ordenador. Un virus puede estar alojado en un ordenador y no infectarlo hasta que exista la acción humana, o sea el virus se activa cuando se ejecuta o abre un programa infectado.

La mayoría de los usuarios ante una situación de virus de un ordenador culpan al antivirus y en el peor de los casos al personal informático, cuando es importante señalar que la acción humana juega un papel fundamental en la infección de un ordenador. Las personas ayudan inconscientemente o por falta de conocimiento informático a propagar los virus al compartir archivos infectados, al enviar correos electrónicos con virus en archivos adjuntos, al no desinfectar los medios extraíbles como memoria flash, disco duros externos, entre otros, por lo que no solo basta con mantener actualizado el antivirus sino saber ejecutar las acciones preventivas de seguridad informática.

Al acceder a internet desde la computadora y conectar algún dispositivo extraíble memoria USB, disco duro externo, se corre el riesgo de que el dispositivo quede infectado con algún virus. La internet es considerada como una fuente amplia de gusanos y virus informáticos sin embargo, se puede encontrar un ordenador sin conexión a internet con un nivel fatal de infección por no saber aplicar las medidas de seguridad informática.

Para evitar y mantener seguro los ordenadores libre de virus, los usuarios implicados deben actuar; el usuario debe tener conocimientos básicos, y el informático como experto, debe saber aplicar con eficiencia y eficacia las medidas de seguridad contra los virus.

Para proteger los ordenadores de los virus, se deben tomar las siguientes medidas:.

• Instalar un antivirus y actualizarlo periódicamente.

• Configurarlo correctamente para que pueda monitorizar las acciones, escanear los ficheros que entran por primera vez en el sistema.

• Tener cuidado con los ficheros que se envían por *messenger*.

• No ejecutar de manera inmediata ficheros ejecutables enviados por correo o descargadas de internet, antes verificar en una computadora de cuarentena.

• Desconfiar de correos extraños que no se esperan recibir, que invitan a leer documentos, que hacen abrir en enlaces.

• No suspender la protección del antivirus, para que la computadora no trabaje de manera lenta.

A continuación se hace mención de los diferentes tipos de virus y algunas de sus características que poseen.

1. Worm o gusano informático: reside y se multiplica en la memoria del ordenador, sin la asistencia de un usuario. Consume banda ancha o memoria del sistema.

2. Caballo de Troya: se esconde en un programa legítimo y se activa cuando se ejecuta. Deja indefensa la computadora, capta datos contraseñas y lo envía a otros sitios.

3. Bombas lógicas o de tiempo: permanecen ocultos hasta que se activan tras un hecho puntual fecha específica o combinación de teclas.

4. Hoax: el objetivo de estos falsos virus es que se sobrecargue el flujo de información mediante el e-mail y las redes.

5. De enlace: cambian las direcciones con las que se accede a los archivos de la computadora por aquella en la que residen. Ocasionan la imposibilidad de ubicar los archivos almacenados.

6. De sobre-escritura: este virus genera la pérdida del contenido de los archivos a los que ataca sobre-escribiendo su interior.

7. Residente: este virus permanece en la memoria y espera a que el usuario ejecute algún archivo o programa para poder infectarlo.

Para contrarrestar la proliferación de programas malignos o virus surgieron los antivirus cuya finalidad es detectar, erradicar o prevenir las infecciones virales. De forma general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer con el aumento de los ordenadores y las capacidades de comunicación.

En correspondencia con lo anteriormente expresado, se hace necesaria la preparación ante cualquier eventualidad de este tipo, y de esta manera poder identificar las amenazas y riesgos sobre los recursos informáticos para minimizar los trastornos que éste pudiera ocasionar.

Conclusiones

De lo anteriormente expresado se infiere que la seguridad informática constituye un reto para los usuarios de los sistemas informáticos, pues el conocimiento de sus objetivos, así como el desarrollo de acciones para la identificación de riesgos y amenazas sobre los activos y recursos informáticos constituye una prioridad para los profesores y estudiantes de la Universidad de Ciencias Pedagógicas "Manuel Ascunce Domenech".

El acelerado desarrollo que han alcanzado las tecnologías de la informática y las comunicaciones ha propiciado que se hayan ido introduciendo en las actividades diarias servicios cada vez más especializados, que a la vez evidencian una alta dependencia de la información digitalizada y de los sistemas informáticos, por lo que la seguridad informática constituye un factor esencial para evitar pérdidas de la información.

Los conocimientos teóricos y el desarrollo de habilidades en el manejo de la seguridad informática hacen posible que los usuarios de los servicios informáticos logren un mayor dominio de las tecnologías de la información y las comunicaciones.

Bibliografía

ALDEGANI, GUSTAVO. MIGUEL. Seguridad Informática. MP Ediciones. 1° Edición. ISBN 987–9131–26–6. Uruguay. 1997.

ARDITA, JULIO CÉSAR. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal en instalaciones de Cybsec S.A. http://www.cybsec.com, enero de 2001.

GONZÁLEZ, J.; GÓMEZ, A. I. Y TORO: Modelo para la producción y evaluación de materiales instruccionales basados en la computadora. Evento internacional Pedagogía ´95, La Habana, 1995.

GONZÁLEZ, J.; et:al. Tecnología interactiva. Desarrollo y consecuencias para la escuela. Centro de Estudios de Software para la Enseñanza (CESoftE), ISPEJV, La Habana, 1994.

HUERTA, ANTONIO VILLALÓN: Seguridad en Unix y Redes Versión 2.1,Julio, 2000.

HUERTA, ANTONIO VILLALÓN. Seguridad en Unix y Redes. Digital – Open Publication License v.10

HOWARD, JOHN D. THESIS: An Analysis of security on the Internet 1989–1995.

LEVIN, RICARDO. Virus Informáticos. Mc Graw Hill. ISBN 007–881647–5. España. 1992.

LEVIN, RICARDO. Virus Informáticos. Mc Graw Hill. ISBN 007–881647–5. España. 1992.

LIZAMA MENDOZA J, Y FARIAS-ELINOS, M. Analfabetismo digital y sus implicaciones en la Seguridad Informática. Facultad de Ciencias Políticas, Universidad Nacional Autónoma de México, 2003

Ministerio de Educación: Programa Rector para el Desarrollo de la Informática Educativa durante el período 1996-2000. La Habana, 1996.

Ministerio de la Informática y las Comunicaciones Adiestramiento "Introducción a la Seguridad en Redes". Empresa SEGURMATICA del, noviembre 2010.

Ministerio del Poder Popular para la Educación. "Manual de consulta. Módulo I. Las Tecnologías de la Información y la Comunicación" 2008.

NOMBELLA, Juan José. Seguridad Informática. Editorial Paraninfo. ISBN 84–283–2341–0. España. 1996.

RODRÍGUEZ CUERVO, A MIGUEL. Libro digital Elementos Básicos de Seguridad Informática, IPLAC 2010.

Revista Virus Reports. Ediciones Ubik Número 16–Página 2 http://es.wikipedia.org/wiki/Hardware

http://www.ecured.cu/index.php/Seguridad_Inform%C3%A1tica#Riesgo_para_los_activos_cr.C3.ADticos

http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

http://www.giron.co.cu/es/noticia/ciencia-y-t%C3%A9cnica/la-seguridad-inform%C3%A1tica-virus-vs-antivirus