Auditoría de Sistema y políticas de Seguridad Informática

1. **AUDITORIA INFORMATICA (AUD).**

a. Generalidades

En primer lugar es importante definir el término de Auditoría, ya que el mismo se ha usado principalmente para referirse a una revisión cuyo único fin es detectar errores, fraudes, señalar fallas y como consecuencia recomendar el despido o remoción del personal, no obstante, la Auditoría es un concepto mucho más amplio que The American Accounting Association lo define claramente como **"El proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionada con informes sobre actividades económicas y otros acontecimientos relacionados". El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando los principios establecidos para el caso".** Para Hernández García toda auditoría y cualquier tipo de auditoria **"es una actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas."**

Hasta hace poco tiempo, la comprobación de la gestión y control de la actividad económica y financiera de las organizaciones, se hacía solamente por medio de la Auditoría Financiera, sin embargo, por el grado de informatización de las empresas, la misma no era suficiente y se hizo necesario conocer qué ocurría dentro de los sistemas de información, ya que la Auditoría Financiera podía llegar a conocer la información de entrada al sistema y el resultado obtenido, pero no podía determinar lo que sucedía entre el momento de entrada de la información y los resultados o salida de la misma, es decir se conocían los **"inputs"** y los **"outputs"** pero no desconocía cómo se habían generado estos últimos y si habían sido objeto o no de alguna manipulación. El examen de lo que acontece realmente en los Sistemas de Información, se puede realizar gracias a la Auditoría Informática.

Pero, ¿Qué es la Auditoría Informática?. No existen definiciones oficiales sobre la misma, y algunas de las que aparecen en libros o se dan en cursos y seminarios tienen la influencia y criterio personal de su autor, no obstante, a continuación mencionamos las que consideramos más importantes:

Una definición podría ser la siguiente: **"Se entiende por Auditoría Informática una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa".**

Ramos González propone la siguiente definición: **"La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos".**

Para Fernando Catacora Carpio, Especialista en Sistemas de Información Gerencial y profesor de esta cátedra en la Universidad Católica Andrés Bello de Caracas, Venezuela **"La Auditoría Informática es aquella que tiene como objetivo principal la evaluación de los controles internos en el área de PED (Procesamiento Electrónico de Datos).**

Otra definición nos indica que la Auditoría Informática es aquella que tiene como objetivos evaluar los controles de la función informática, analizar la eficiencia de lo sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente. El auditor informático debe velar por la correcta utilización de los recursos que la empresa dispone para lograr un eficiente y eficaz Sistema d Información.

Finalmente, de forma sencilla y gráfica podemos decir que la Auditoría Informática es el proceso de recolección y evaluación de evidencia para determinar sí u sistema automatizado:

Salvaguarda activos	{	**Daños** **Destrucción** **Uso no autorizado** **Robo**
		Oportuna

Mantiene la Integridad de los datos	{	**Precisa** **Confiable** **Completa**
Alcanza Metas Organizacionales	{	**Contribución de la función Informática**
Consume recursos eficientemente	{	**Utiliza los recursos adecuadamente en el procesamiento de la información**

Fuente:

Así pues, debemos reafirmar que la Auditoría Informática, también conocida en nuestro medio como Auditoría de Sistemas, surge debido a que la información se convierte en uno de los activos más importante de las empresas, lo cual se puede confirmar si consideramos el hecho de que si se queman las instalaciones físicas de cualquier organización, sin que sufran daños los ordenadores, servidores o equipo de cómputo, la entidad podría retomar su operación normal en un menor tiempo, qu si ocurre lo contrario. A raíz de esto, la información adquiere gran importancia en la empresa moderna debido a su poder estratégico y a que se invierten grandes sum de dinero y tiempo en la creación de sistemas de información con el fin de obtener una mayor productividad.

Otro factor que influyó grandemente en el nacimiento de la Auditoría Informática fue el uso de la tecnología y sistemas computarizados para el procesamiento de la información, lo cual ha tenido una importante repercusión sobre la disciplina contable, pues la mayoría de las operaciones financieras han recibido la influencia de la informática.

b. Alcance de la Auditoría Informática

El alcance de la Auditoría Informática no es nada más que la precisión con que se define el entorno y los límites en que va a desarrollarse la misma y se complementa con los objetivos establecidos para la revisión. El alcance de la Auditoría Informática deberá definirse de forma clara en el Informe Final, detallando no solamente los temas que fueron examinados, sino también indicando cuales se omitieron.

c. Importancia de la Auditoría Informática

A pesar de ser una disciplina cuya práctica ha aumentado en nuestro país durante los últimos años, la Auditoría Informática, es importante en las organizaciones por l siguientes razones:

- Se pueden difundir y utilizar resultados o información errónea si la calidad de datos de entrada es inexacta o los mismos son manipulados, lo cual abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.
- Las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.
- La continuidad de las operaciones, la administración y organización de la empresa no deben descansar en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.
- La vigencia de la Ley de Derecho de Autor, la piratería de softwares y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problema en plazos razonables, es decir, el usuario percibe que está abandonado y desatendido permanentemente.
- En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas, personal subalterno, horas de trabajo pagadas, programas, aplicaciones, servicios de correo, internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos personales, alejados totalmente de las operacion de la empresa o de las labores para las cuales fue contratado.
- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de aut y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

d. Tipos de Auditoría Informática

El Departamento de Informática o Sistemas desarrolla diversas actividades y sobre la base de estas se han establecido las principales divisiones de la Auditoría Informática, las cuales son: de Explotación u Operación, Desarrollo de Proyectos, de Sistemas, de Comunicaciones y Redes y de Seguridad. A continuación repasaremos brevemente cada una.

d.1. Auditoría Informática de Producción o Explotación

En algunos casos también conocida como de Explotación o Operación, se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

La producción, operación o explotación informática dispone de una materia prima, los datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas y obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Auditar la producción, operación o explotación consiste en revisar las secciones que la componen y sus interrelaciones, las cuales generalmente son: planificación, producción y soporte técnico.

d.2. Auditoría Informática de Desarrollo de Proyectos

La función de desarrollo es una evolución del llamado análisis y programación de sistemas, y abarca muchas áreas, como lo son: prerequisitos del usuario y del entorno, análisis funcional, diseño, análisis orgánico (preprogramación y programación), pruebas entrega a explotación o producción y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, ya que en caso contrario, los costos pueden excederse, puede producirse la insatisfacción del usuario.

La auditoría en este caso deberá principalmente comprobar la seguridad de los programas en el sentido de garantizar que lo ejecutado por la máquina sea exactamente lo previsto o lo solicitado inicialmente.

d.3. Auditoría Informática de Sistemas

Se ocupa de analizar y revisar los controles y efectividad de la actividad que se conoce como técnicas de sistemas en todas sus facetas y se enfoca principalmente en e entorno general de sistemas, el cual incluye sistemas operativos, softwares básicos, aplicaciones, administración de base de datos, etc.

d.4. Auditoría Informática de Comunicaciones y Redes

Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores, etc. Así pues, la Auditoría Informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de auditoría se requiere un equipo de especialistas y expertos en comunicaciones y redes.

El auditor informático deberá inquirir sobre los índices de utilización de las líneas contratadas, solicitar información sobre tiempos de desuso; deberá proveerse de la topología de la red de comunicaciones actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. Por otro lado, será necesario qu obtenga información sobre la cantidad de líneas existentes, cómo son y donde están instaladas, sin embargo, las debilidades más frecuentes o importantes se encuentra en las disfunciones organizativas, pues la contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras, impresoras, etc.).

d.5. Auditoría de la Seguridad Informática

La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Por su parte, la seguridad lógica se refiere a la seguridad en el uso de softwares, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.

d.6. Auditoría Informática para Aplicaciones en Internet.

En este tipo de revisiones, se enfoca principalmente en verificar los siguientes aspectos, los cuales no puede pasar por alto el auditor informático:

- Evaluación de los riesgos de internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y la arquitectura de seguridad implementada.
- Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

e. Metodología de Trabajo de Auditoría Informática

- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.

1. **POLÍTICAS DE SEGURIDAD INFORMÁTICA (SEG)**

a. Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse través de redes, ha abierto nuevos horizontes ha las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

b. Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Po tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

c. Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empres para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia d los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización

la empresa, cambio o diversificación del área de negocios, etc.

d. Parámetros para Establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

e. Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: **"más dinero para juguetes del Departamento de Sistemas"**.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

1. **PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS (PRIV)**

3.1. Privacidad en la Red

a. Generalidades

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Por tal razón, es necesario que las organizaciones m*antengan sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos*.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

b. Definición de Privacidad de las Redes

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.).

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos, computadoras personales, teléfonos móviles, etc.).

Así pues, las redes en las empresas, son los medios que permiten la comunicación de diversos equipos y usuarios, pero también están propensas a ser controladas o accesadas por personas no autorizadas. Cuando nos referimos a la privacidad de la red, se evoca al cuidado o medidas establecidas para que la información de los sistemas como puede ser datos de clientes, servicios contratados, reportes financieros y administrativos, estrategias de mercado, etc., no sea consultada por intrusos.

c. Requisitos para Mantener la Privacidad de las Redes

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más seguras ante las posibilidades de intrusión.

1. **Disponibilidad**: significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la empresa.
2. **Autenticación**: confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, la autenticación de los sitios web, etc.
3. **Integridad**: confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica
4. **Confidencialidad**: protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que pueden amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

d. Riesgos o Amenazas a la Privacidad de las Redes

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

2. **Interceptación de las Comunicaciones**: la comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, pinchando la línea, o controlando las transmisiones.

3. **Acceso no Autorizado a Ordenadores y Redes de Ordenadores**: el acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma mal intencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: explotación de información interna, ataques aprovechando la tendencia de la gente a utilizar contraseñas previsibles, aprovechar la tendencia de la gente a desvelar informació a personas en apariencia fiables e interceptación de contraseñas.
4. **Perturbación de las Redes**: actualmente las redes se encuentran ampliamente digitalizadas y controladas por ordenadores, pero en el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos se concretan a los puntos débiles y más vulnerables de los componentes de las redes como son sistemas operativos, encaminadores, conmutadores, servidores de nombres de dominio, etc.
5. **Ejecución de Programas que Modifican y Destruyen los Datos**: los ordenadores funcionan con programas informáticos, pero lamentablemente, los programas pueden usarse también para desactivar un ordenador y para borrar o modificar los datos. Cuando esto ocurre en un ordenador que forma parte de un red, los efectos de estas alteraciones pueden tener un alcance considerable. Por ejemplo, un virus es un programa informático mal intencionado que reproduce su propio código que se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código del virus.
6. **Declaración Falsa**: a la hora de efectuar una conexión a la red o de recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función del contexto de la comunicación. Para la red, el mayor riesgo de ataque procede de la gente que conoce el contexto. Por tal razón, las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos. como pueden ser transmitir datos confidenciales a personas no autorizadas, rechazo de un contrato, etc.
7. **Accidentes no Provocados**: numerosos problemas de seguridad se deben a accidentes imprevistos o no provocados como: son tormentas, inundaciones, incendios, terremotos, interrupción del servicio por obras de construcción, defectos de programas y errores humanos o deficiencias de la gestión del operador, proveedor de servicio o el usuario.

3.2. DETECCIÓN DE INTRUSOS

a. Generalidades

Los sistemas computarizados y aplicaciones están en permanente evolución, por tal razón pueden surgir nuevos puntos vulnerables. A pesar de los avances en los sistemas de seguridad, los usuarios no autorizados con herramientas muy sofisticadas tienen grandes posibilidades de accesar las redes, sistemas o sitios de las organizaciones e interrumpir sus operaciones.

Actualmente, existen más de 30.000 sitios en internet orientados a la piratería o intrusión de redes, los cuales ofrecen programas de fácil descarga y acceso que han dejados las puertas abiertas para nuevos ataques.

Entre los primeros intrusos o piratas informáticos famosos están Steve Wozniak, Bill Gates y Linus Torvalds, quienes ahora son reconocidos creadores de muchas de las tecnologías informáticas que utilizamos en la actualidad. Estos primeros intrusos de redes amaban la tecnología, sentían la imperiosa necesidad de saber como funcionaba todo y su objetivo era impulsar los programas que trascendieran el objetivo para el cual fueron diseñados. En ese entonces, la palabra intruso o pirata informático no tenía la connotación negativa que tiene hoy, ya que ha desaparecido la ética original que provenía de la simple curiosidad y la necesidad de afrontar desafíos.

Los objetivos de los primeros intrusos informáticos no podrían estar más ajenos a los objetivos de los piratas actuales. Lo que motiva a esta nueva generación no parece ser la curiosidad o el afán del conocimiento, como solía ser, al contrario, los motiva la codicia, el poder, la venganza y otras intenciones maliciosas.

b. Factores que Propician el Acceso de Intrusos a la Redes y Sistemas

Los ataques a la seguridad han sobrepasando las estimaciones esperadas, y además del crecimiento de los sitios de internet relacionados con piratería, también hay otros aspectos que propician esta situación:

- Los sistemas operativos y las aplicaciones nunca estarán protegidos. Incluso si se protege el sistema nuevas vulnerabildades aparecerán en el entorno todos los días, como las que actualmente representan los teléfonos, equipos inalámbricos y dispositivos de red.
- En las empresas las redes internas son más o menos confiables, ya que los empleados se conectan a la red desde la casa, otras oficinas u hoteles fuera de la empresa, lo cual genera nuevos riesgos.
- Falta de seguridad física en algunas empresas y falta de políticas de seguridad informática. Por ejemplo, muchos empleados se ausentan y dejan desprotegida su computadora.
- Los empleados no siempre siguen y reconocen la importancia de las políticas de seguridad: La capacitación y entrenamiento que se les brinde a los empleados n cuenta mucho si ignoran las advertencias sobre los peligros de abrir los archivos adjuntos sospechosos del correo electrónico.
- Requerimientos cada vez mayores de disponibilidad de redes y acceso a ellas.

c. Medidas para Controlar el Acceso de Intrusos

Algunas medidas que se pueden poner en práctica para controlar los accesos de intrusos pueden ser las siguientes:

- Utilizar un firewall, que no es más que un dispositivo localizado entre la computadora anfitriona y una red, con el objeto de bloquear el tráfico no deseado de la red mientras permite el cruce de otro tráfico.
- Utilización y actualización de antivirus.
- Actualizar todos los sistemas, servidores y aplicaciones, ya que los intrusos por lo general a través de agujeros conocidos de seguridad.
- Desactivar los servicios innecesarios de redes.
- Eliminar todos los programas innecesarios.
- Analizar la red en busca de servicios comunes de acceso furtivo y utilizar sistemas de detección de intrusos los cuales permiten detectar ataques que pasan inadvertidos a un firewall y avisar antes o justo después de que se produzcan, y
- Finalmente, establecer la práctica de crear respaldos o backups.

Hay muchos dispositivos de seguridad que pueden utilizar las empresas para contrarrestar las amenazas a las que están expuestas, por eso, con frecuencia muchas terminan utilizando soluciones como los firewalls, sistemas de detección de intrusos, redes virtuales, etc. para obtener la protección total que necesitan en materia de seguridad. Debido al incremento de las amenazas y la naturaleza dinámica de los ataques, es necesario adoptar prácticas eficientes e implementar políticas de seguridad que nos permitan manejar eficientemente este tipo de ataques.

d. Principales Actividades de los Intrusos o Piratas Informáticos

Los comportamientos de los intrusos o piratas informáticos han tomado matices preocupantes. A continuación enumeramos algunas de estas actividades:

- Desfiguramiento de los sitios web: esto ocurre cuando se entra al servidor web y se altera o reemplaza la página principal. Los desfiguramientos de los sitios we es una práctica común, pues se lleva a cabo simplemente descargando de internet un programa que está diseñado para aprovecharse de las vulnerabilidades de l sistemas.
- Hurto de la información de las tarjetas de crédito: La información de la tarjeta de crédito puede ser hurtada por medio de las mismas herramientas de ataque que están tras los desfiguramientos de los sitios web. Una vez los piratas informáticos tienen acceso a la red, pueden analizar las bases de datos en busca de archivos que puedan tener información valiosa, como archivos de clientes. Todo archivo que sea interesante para el intruso puede ser descargado a su computadora.
- Ataque a los programas instructores del servidor: Los programas instructores del servidor permiten las comunicaciones bidireccionales entre los servidores y usuarios web. Las instrucciones del servidor también es un objetivo común de los intrusos y lo hacen ejecutando comandos, leyendo los archivos del sistema o modificando los mismos.
- Ataques de negación de servicio: la negación de servicio se produce cuando alguien o algo impide que se realice una tarea u operación deseada. Los intrusos o

piratas logran esto principalmente con el consumo del ancho de banda, inundando la red con datos, agotando los recursos del sistema, fallas de programación, etc.

1. Ataques de negación distribuida de servicio: se refiere cuando muchas computadoras se asaltan y se les ordena inundar un sitio determinado con paquetes o solicitud de información, negando así el servicio a usuarios legítimos.

1. **VIRUS Y ANTIVIRUS (V/A)**

4.1. Virus

a. Generalidades

Antes de profundizar en este tema, debemos aclarar que los virus de computadoras son simplemente programas, y como tales hechos por programadores. Son programas que debido a sus características particulares son especiales. Para hacer un virus de computadora no se requiere capacitación especial, ni una genialidad significativa, sino conocomientos de lenguajes de programación para el público en general y algunos conocimientos puntuales sobre el ambiente de programación y arquitectura de las PC's.

Nuestro trabajo capta el problema del virus, desde el punto de vista funcional. En la vida diaria, cuando un programa invade inadvertidamente el sistema, se replica si conocimiento del usuario y produce daños, pérdida de información o fallas del sistema, reconocemos que existe un virus. Los virus actúan enmarcados por "debajo" d sistema operativo, como regla general, y para actuar sobre los periféricos del sistema, tales como disco rígido, disketteras, ZIP's CD-R's, hacen uso de sus propias rutinas aunque no exclusivamente. Un programa normal, por llamarlo así, utiliza las rutinas del sistema operativo para acceder al control de los periféricos del sistema y eso hace que el usuario sepa exactamente las operaciones que realiza, teniendo control sobre ellas. Los virus, por el contrario, para ocultarse a los ojos del usuario, tienen sus propias rutinas para conectarse con los periféricos de la computadora, lo que les garantiza cierto grado de inmunidad a los ojos del usuario, que no advierte su presencia, ya que el sistema operativo no refleja su actividad en la PC. Una de las principales bases del poder destructivo de estos programas radica en el uso de funciones de manera "sigilosa", oculta a los ojos del usuario común.

El virus, por tratarse de un programa, para su activación debe ser ejecutado y funcionar dentro del sistema al menos una vez. Demás esta decir, que los virus no surgen de las computadoras espontáneamente, sino que ingresan al sistema inadvertidamente para el usuario, y al ser ejecutados, se activan y actúan con la computadora huésped.

b. Definiciones

1. "Un virus es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistem y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco."
2. Un virus es una porción de código ejecutable, que tiene la habilidad única de reproducirse. Se adhieren a cualquier tipo de archivo y se diseminan con los archivos que se copian y envían de persona a persona.

Además de reproducirse, algunos virus informáticos tienen algo en común: una rutina dañina, que el virus descarga como una bomba, mientras que las descargas pueden ser simples mensajes o imágenes, éstas también pueden borrar archivos, reformatear el disco duro o causar otro tipo de daño. Si el virus no contiene una rutina dañina, aún puede causar problemas, como tomar espacio libre del disco y de la memoria, y también disminuir el rendimiento de la computadora.

Los virus de las computadoras no son más que programas; y estos virus casi siempre los acarrean las copias ilegales o piratas. Provocan desde la pérdida de datos o archivos en los medios de almacenamiento de información (diskette, disco duro, cinta), hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo.

c. Características

Hay que recordar que un virus no puede ejecutarse por sí solo, pues necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse en un programa portador, el virus precisa modificar la estructura de aquél, posibilitando que durante su ejecución pueda realizar una llamada al código del virus

Las particularidades de los virus:

- Son muy pequeños.
- Casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha de creación.
- Se reproducen a sí mismo.
- Toman el control o modifican otros programas.
- **Es dañino**: El daño es implícito, busca destruir o alterar, como el consumo de memoria principal y tiempo de procesador.
- **Es autorreproductor**: A nuestro parecer la característica más importante de este tipo de programas es la de crear copias de sí mismo.
- **Es subrepticio:** Esto significa que utilizará varias técnicas para evitar que el usuario se de cuenta de su presencia.

d. ¿Quiénes hacen los virus?

Los virus informáticos son hechos por personas con conocimiento de programación, pero que no son necesariamente genios de las computadoras. Tienen conocimient de lenguaje ensamblador y de cómo funciona internamente la computadora. A diferencia de los virus que causan resfriados y enfermedades en humanos, los virus computacionales no ocurren de forma natural, cada uno es programado. No existen virus benéficos. Algunas veces son escritos como una broma, desplegando un mensaje humorístico. En estos casos, el virus no es más que una molestia. Muchas veces son creados por personas que se sienten aburridas, con coraje, como reto intelectual; cualquiera que sea el motivo, los efectos pueden ser devastadores.

e. Síntomas Más Comunes de Virus

La mejor forma de detectar un virus es, obviamente un antivirus, pero en ocasiones los antivirus pueden fallar en la detección. Puede ser que el escaneo no detecte nad y sí el análisis huerístico. Puede ser que no detectemos nada y aún seguir con problemas. En estos casos debemos notar algunos síntomas posibles:

- Los programas comienzan a ocupar más espacio de lo habitual. Se reduce el espacio libre en la memoria RAM. El virus al entrar en el sistema, se sitúa en al memoria RAM, ocupando una porción de ella. El tamaño útil y operativo de la memoria se reduce en la misma cuantía que tiene el código del virus. Siempre en el análisis de una posible infección es muy valioso contar con parámetros de comparación antes y después de la posible infección. Por razones prácticas casi nadie analiza detalladamente su PC en condiciones normales y por ello casi nunca se cuentan con patrones antes de una infección, pero sí es posible analizar estos patrones al arrancar una PC en la posible infección y analizar la memoria arrancando el sistema desde un disco libre de infección.
- Aparecen o desaparecen archivos. En mayor o menor medida, todos los virus, al igual que programas residentes comunes, tienen una tendencia a "colisionar" con otras aplicaciones, lo que provoca también aparición de mensajes de error no comunes.
- Cambia el tamaño de un programa o un objeto. Programas que normalmente funcionaban bien, comienzan a fallar y generar errores durante la sesión.
- Aparecen mensajes u objetos extraños en la pantalla. El código viral, ocupa parte de la RAM y debe quedar "colgado" de la memoria para activarse cuando sea necesario. Esa porción de código que queda en RAM, se llama residente y con algún utilitario que analice el RAM puede ser descubierto.
- El disco trabaja más de lo necesario. Tiempos de cargas mayores y es debido al enlenticimiento global del sistema, en el cual todas las operaciones se demoran más de lo habitual.
- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados. Las operaciones se realizan con más lentitud, ya que los virus son programas como tales requieren de recursos del sistema para funcionar y su ejecución al ser repetitiva, lleva a un enlentecimiento y distorsión global en las operaciones.
- Se modifican sin razón aparente el nombre de los ficheros.
- No se puede acceder al disco duro.

f. Clasificación

A continuación esbozamos una clasificación que tiende a catalogar los virus actuales, sin intentar crear una clasificación académica, sino una orientación en cuanto a funcionalidad de los virus:

- **Virus de Macros/Código Fuente:** Se adjuntan a los programas fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hoja de Cálculo (Excell, Quattro, Lotus).
- **Virus Mutantes:** Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (NATAS o SATÁN, Miguel Angel, por mencionar algunos).
- **Gusanos:** Son programas que se reproducen a sí mismo y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa qu los transporte. Los gusanos se cargan en la memoria y se posesionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, así sucesivamente. Esto hace que queden borradas los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdidas de datos.
- **Caballos de Troya:** Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
- **Bomba de Tiempo:** Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.
- **Autorreplicables:** Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se autoreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programadas o cada determinado tiempo, contado a partir de su última ejecución, o simplemente a "sentir" que se les trata de detectar. Un ejemplo de estos es el virus del viernes 13, que se ejecuta en esa fecha o se borra (junto con los programas infectados), evitando así ser detectado.
- **Infectores del área de carga inicial:** Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciend la computadora y lo conservan todo el tiempo.
- **Infectores del sistema:** Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).
- **Infectores de programas ejecutables:** Estos son los virus más peligrosos porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras). La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posesiona en la memoria de la computadora y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos.

Todos estos programas tienen en común la creación de efectos perniciosos, sin embargo, no todos pueden ser considerados como virus propiamente dichos. La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno de varios de estos programas.

g. Ciclo de Infección

Como mencionamos con anterioridad, para que un virus se active en memoria, se debe ejecutar el programa infectado en primer término, para que el virus inicie sus actividades dentro de nuestro sistema. En este caso, no es necesario arrancar ningún programa, sino simplemente abrir un archivo de Word o Excel infectado.

El ciclo completo de infección de un Macro Virus sería así:

- Se abre el archivo infectado, con lo cual se activa en memoria.
- Infecta sin que el usuario se dé cuanta al NORMAL.DOT, con eso se asegura que el usuario sea un reproductor del virus sin sospecharlo.
- Si está programado para eso, busca dentro de la PC los archivos de Word, Excel, etc. que puedan ser infectados y los infecta.
- Si está programado, verifica un evento de activación, que puede ser una fecha, y genera el problema dentro de la pc (borrar archivos, destruir información, etc.)
- Ahora bien, en el caso de mails vía internet. Los mails no son programas. Algunos no poseen macros (los que sí poseen macros son los mails de Microsoft Outlook). Aquellos que no tienen lenguaje de macros (NO PUEDEN CONTENER VIRUS).
- Los archivos adjuntos asociados al mail pueden llevar virus (siempre que sean susceptibles de ser infectados). Bajen el adjunto, y verifíquenlo. Asegúrense que el antivirus chequee los zipeados o comprimidos si lo adjuntado es un archivo de ese tipo. Si el adjunto es un documento que puede tener macros, desactiven las macros del programa Word antes de abrirlo. Si el adjunto es un archivo de texto plano, pueden quedarse tranquilos.

h. Medidas de Protección Efectivas

Obviamente, la mejor y más efectiva medida es adquirir un antivirus, mantenerlo actualizado y tratar de mantenerse informado sobre las nuevas técnicas de protección y programación de virus. Gracias a internet es posible mantenerse al tanto a través de servicios gratuitos y pagos de información y seguridad. Hay innumerables boletines electrónicos de alerta y seguridad que advierten sobre posibles infecciones de mejor o menor calidad. Existen herramientas indispensables para aquellos que tienen conexiones prolongadas a internet, que tienden a proteger al usuario no sólo detectando posibles intrusos dentro del sistema, sino chequeando constantemente e sistema, a modo de verdaderos escudos de protección.

4.2. Antivirus

a. Generalidades

El programa de antivirus debe ser completo, preciso y rápido. Si no es así, usted simplemente no lo utilizará, y dejará a un lado esta actividad, lo cual es muy peligros Por ejemplo, en cualquier mes determinado hay de 200 a 300 virus circulando por el mundo. Esa cifra proviene de la WildList, una lista mensual reconocida internacionalmente, que tiene los virus que se dispersan en el mundo "en estado salvaje".

El método principal de un analizador de antivirus para atrapar los virus es comparar un código sospechoso con las bases de datos de conocidas firmas de virus. Estas bases de datos incluyen nombres actuales o anteriores en la WildList, así como decenas de miles "zoovirus", que en su mayoría existen en laboratorios, pero que utilizan trucos que pueden ser empleados por futuros virus.

Con el propósito de adquirir un buen antivirus, lo primero es verificar el tipo de tecnología aplicada en su desarrollo, actualmente los antivirus utilizan dos técnicas de verificación:

- La conocida técnica de escaneo, consistente en tener una gran base de datos con fragmentos víricos para comparar los archivos con esa inmensa biblioteca del wildlist.
- La tecnología heurística es fundamental en estos momentos, y en mi opinión, los antivirus han de ofrecer como alternativa al escaneo común (aún necesario) la búsqueda heurística. Esta técnica permite detectar virus que aún no estén en la base de datos scaning, y es muy útil cuando padecemos la infección de un virus que aún no ha sido estudiado ni incorporado a los programas antivirus.

b. Definición de Antivirus

- Es el programa que se encarga de analizar el contenido de los ficheros y, en caso

de detectar un virus en su interior, proceder a su desinfección. También realizan búsquedas heurísticas, esto es, buscar funciones que puedan resultar nocivas para tu ordenador, sin que sean virus reconocidos.

- Es una aplicación o programa dedicada a detectar y eliminar virus informáticos. La forma en que protege es la siguiente, el sistema de protección del Antivirus depende del sistema operativo en que se esté trabajando. En DOS se utiliza TSR (Terminate and Stay Resident, programas que terminan y se quedan residentes en memoria), en Windows 95/98 VxD (Virtual Driver) y en NT drivers en modo Kernel. Por término general se puede pensar en un programa que vigila todos y cada uno de los accesos que se realizan a ficheros y discos y antes de autorizarlos avisa de la existencia virus y, en su caso, desinfecta el fichero en cuestión.

Si eres muy cuidadoso con los programas que utilizas, la información que introduces a tu computadora y con los lugares que visitas en el Internet, así como intercambiar tus discos en el trabajo o discos de amigos (duda procedencia) es muy posible que nunca tengas problemas con virus, lo que sí, es indispensable que tengas instalado un buen Antivirus.

c. Los Antivirus Más Buscados

Actualmente, los virus no sólo son más potentes que sus predecesores, sino que se propagan más rápido. En los años 80, los virus del sector de arranque se multiplicaban a través del intercambio de discos flexibles. A finales de los 90, el correo electrónico era quien transportaba virus de macros que venían en documentos anexos de Microsoft Word.

Ahora el peligro viene principalmente de los gusanos de envíos masivos, se autoreplican y son capaces de secuestrar los libros de direcciones de correo electrónico y autoenviarse a múltiples destinatarios. Por ejemplo, LoveLetter era un virus de guión en Visual Basic. Hoy, la mayoría de los gusanos de correo masivo son programa Win32 independientes, como en el caso de SirCam y Klez. Estos programas son lo peor de todas las infecciones de virus.

Por su parte, los virus de los macros están en un distante segundo lugar y los de guión vienen pegados en un tercer lugar. Ahora los virus del sector arranque sólo representan cerca del 1% de las infecciones.

Al elegir un antivirus, tomamos en cuenta tres aspectos fundamentales: facilidad de adquisición de las actualizaciones, menor costo posible y facilidad de uso. Atendiendo a estos tres requisitos, recomendamos en el mismo orden Scan de McAffee que es un producto gratuito y se puede conseguir fácilmente en el internet o Norton Antivirus para el cual tendrá que invertir algunos dólares.

d. Antivirus al Rescate

A juzgar por la evaluación de siete productos que llevan a cabo, los fabricantes de antivirus, los mismos han respondido bastante bien ante las amenazas: Estos productos son: Etrust EZ Antivirus 5.4, de Computer Associates; Anti-Virus Personal Por 4, de Kaspersky Lab; McAfee Virus Scan 6.02, de Network Associates; Virus Control 5.2, de Norman; Antivirus Platinum 6.25, de Panda; Norton AntiVirus 2002, de Symantec; y PC-cillin 2002, de Trend Micro. Los productos de Norton, Kaspersky y McAfee fueron los que mejor erradicaron los virus, pero Norton se llevó el premio a la mejor compra gracias a su interfaz intuitiva.

Además de la clase de virus que el analizador descubre, también es importante la ubicación de éste, por ejemplo, el protector antivirus debe ser capaz de meterse bien dentro de los archivos zip y otros archivos comprimidos, incluso hasta en los archivos zip que estén ubicados dentro de otros archivos zip. También debe revisar los anexos al correo electrónico, y donde quiera que descubra una infección, debe eliminarla sin destruir archivos valiosos.

Kaspersky, McAfee, Norton, Panda y PC-cillin interceptan y analizan los anexos al correo electrónico antes de que lleguen a la unidad de disco duro. Pero Norton y PC-cillin sólo funcionan con programas de correo electrónico que cumplan con los requisitos de POP3, mientras que Kaspersky sólo funciona con los clientes de Outlook, Outlook Express y Exchange, de Microsoft, Panda, a su vez, analiza anexos de POP3, Exchange e incluso de AOL.

Cuando estos productos encontraron un virus, la mayoría realizó un buen trabajo al quitarles sin dañar archivos, pero Norton fue el único que lo hizo a la perfección.

e. Conozca Bien su Antivirus

Debido a que en todo momento aparecen nuevos virus, es necesario actualizar con facilidad las definiciones. Todos los programas probados, excepto Etrust, ofrecen actualizaciones automáticas programadas. Sin embargo, nuestro tanto a favor es para Norton, que revisa si hay actualizaciones de manera prefijada, al momento de se instalado y después, cada 4 horas. Norton también gana puntos por tener la interfaz más lógica, de fácil dominio.

En virtud de lo anterior, al hacer una evaluación es importante tratar de verificar hasta que punto los diversos antivirus cumplen con las siguientes características:

1. Deben actualizar los patrones o firmas, por lo menos una vez por semana.
2. La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.
3. Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.
4. Se deben poder adaptar a las necesidades de diferentes usuarios.
5. Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
6. Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.
7. Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.
8. Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.
9. No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.
10. El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible.
11. Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.
12. Deben de tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

En base a estos parámetros, uno mismo puede poner a prueba los distintos productos que hay en el mercado y de acuerdo a nuestras prioridades sacar conclusiones.

f. Importancia del Antivirus

Actualmente, no es difícil suponer que cada vez hay mas personas que están conscientes de la necesidad de hacer uso de algún antivirus como medida de protección básica.

- Desde el punto de vista del administrador, este desea primordialmente tener resultados al problema de administración centralizada. Es decir, desea que un antivirus posea una consola que permita la instalación remota tanto en una red LAN como en una WAN y no verse obligado a instalar el producto a pie en cada una de las estaciones de trabajo.
- Desde el punto de vista del usuario final, a quien le interesa no infectarse por ningún motivo y que la protección en memoria del producto sea de lo más eficaz, tanto para detectar y remover cualquier virus que pueda presentarse.

Basados en estas necesidades, podemos darles los siguientes tips:

f.1. Controles

- Control de acceso físico a los equipos.
- Control de entradas a los programas de la computadora a través de claves de acceso (passwords).
- Registro, verificación y control de los diskettes, cd's que se introducen a la computadora.
- Se recomienda algún programa de tipo menú que restrinja los programas que se pueden ejecutar a sólo los autorizados a cada usuario.

f.2. Bloqueos

- Cerradura para floppies "drive lock"
- Uso del candado o llave de encendido, si la computadora lo tiene.
- Deshabilitar el arranque desde la unidad de diskette.
- Deshabilitar completamente las unidades de diskette.
- Habilitación de la facilidad de palabra clave (password).
- Activar la protección anti-virus en BIOS.

f.3. Diskettes

Estos son puntos muy importantes, ¡prácticamente todos los virus se introducen a una computadora por medio de diskettes! Y en caso de un desastre, las copias de respaldo en diskette serán la salvación de nuestros datos.

- Verificar contra virus todos los diskettes que se introduzcan en la computadora, aunque sólo sean de datos.
- No ejecutar programas de origen dudoso.
- No meter diskettes extraños.
- Nunca arranque desde diskette en la operación normal de su computadora.
- Nunca dejar puestos diskettes al apagar la computadora.
- Tenga un diskette de arranque que esté libre de virus y protegido contra escritura.
- Si es necesario arrancar desde diskette, utilice únicamente este diskette.
- Proteja contra escritura sus discos del sistema, así como sus discos de programas de aplicación.
- Que los usuarios sólo manejen diskettes de datos y nunca de programas.
- Instalar nuevos paquetes en una máquina que sirva de conejillo de Indias y que esté un tiempo en observación.
- Mantener copias respaldo, tanto de los programas, como de los datos.
- Hacer por separado los respaldos de datos y de programas.

f.4. Vacunas Antivirus

- Tener varios programas antivirus, preferentemente con diferentes enfoques.
- Utilizar o activar las diversas opciones de protección.
- Comprar las versiones actualizadas de las vacunas.
- Leer la documentación y manuales de los antivirus.

f.5. Servicios en Línea

- Verificar contra virus todo programa que se transfiera.
- Verificar contra virus todo archivo autodescomprimible (aunque sea de datos).

f.6. OTROS

- Capacitar a los usuarios en protección contra virus.
- Desarrollar un plan de emergencia contra virus que prevea procedimientos o máquinas alternas para el proceso de los datos.
- Mantenerse informado, o sea leer sobre el tema.

1. **SEGURIDAD**

a. Generalidades

Cuando hablamos de realizar una evaluación de la seguridad es importante conocer como desarrollar y ejecutar la implantación de un sistema de seguridad.

Desarrollar un sistema de seguridad significa "**planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa**".

Las consideraciones de un sistema integral de seguridad debe contemplar:

- Definir elementos administrativos
- Definir políticas de seguridad
  - A nivel departamental
  - A nivel institucional
- Organizar y dividir las responsabilidades
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Definir prácticas de seguridad para el personal.
- Plan de emergencia, plan de evacuación, uso de recursos de emergencia como extinguidores.
- Definir el tipo de pólizas de seguros.
- Definir elementos técnicos de procedimientos.
- Definir las necesidades de sistemas de seguridad para hardware y software
- Flujo de energía.
- Cableados locales y externos
- Aplicación de los sistemas de seguridad incluyendo datos y archivos.
- Planificación de los papeles de los auditores internos y externos.
- Planificación de programas de desastre y sus pruebas (simulación).
- Planificación de equipos de contingencia con carácter periódico.
- Control de desechos de los nodos importantes del sistema.
- Política de destrucción de basura, copias, fotocopias, etc.

Para dotar de medios necesarios al elaborar su sistema de seguridad se debe considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos y ambientales.
- Elaborar un plan para un programa de seguridad.

b. Seguridad de su Corre "e"

Cada día son más las organizaciones que utilizan el correo electrónico como herramienta fundamental de sus negocios, por ende, es indispensable que se cuente con soluciones confiables y escalables que permitan que las comunicaciones, utilizando este tipo de medio, se realicen de forma segura y confiable. La nueva versión del programa de administración de listas de correo electrónico LISTSERV, viene a satisfacer esta demanda, pues está repleta de nuevas y mejoradas características, está dotada de protección contra virus y de una mayor facilidad de uso.

LISTSERV trabajo bajo una interfaz rediseñada tipo Web que facilita la administración de la lista. Incluye un Experto de Tarea, que guía al administrador de la lista con instrucciones detalladas paso a paso.

Asimismo, con la proliferación de los virus a través del correo electrónico, L-Soft ha integrado a su lista el programa de protección contra virus de F-Secure para inspeccionar el correo electrónico.

c. ¿Cómo Puede Elaborar un Protocolo de Seguridad Antivirus?

La forma más segura, eficiente y efectiva de evitar virus, consiste en elaborar un protocolo de seguridad para sus sistemas PC's. Un protocolo de seguridad consiste en una serie de pasos que deberá seguir con el fin de crear un hábito al operar normalmente con programas y archivos en sus computadoras. Un buen protocolo es aquel que le inculca buenos hábitos de conducta y le permite operar con seguridad su computadora, aún cuando momentáneamente esté desactivado o desactualizado su antivirus.

Este protocolo establece ciertos requisitos para que pueda ser cumplido por el operador en primer término y efectivo en segundo lugar. Le aseguramos que un protocolo puede ser muy efectivo pero si es COMPLICADO, no será puesto en funcionamiento nunca por el operador.

El protocolo de seguridad antivirus consiste en:

1. Instalar el antivirus y asegurar cada 15 días su actualización.
2. Chequear los CD-Rom's ingresados en nuestra PC sólo una vez, al comprarlos o adquirirlos y marcarlos con un fibrón o marcador para certificar el chequeo. Esto solo es válido en el caso de que nuestros CD's no sean procesados en otras PC y sean regrabables.
3. Formatear todo diskette virgen que compremos, sin importar si son formateados de fábrica, ya que pueden colarse virus aún desde el proceso del fabricante.
4. Revisar todo diskette que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido ingresado en la desketera de otra PC.
5. Si nos entregan un diskette y nos dicen que está revisado, NO CONFIAR NUNCA en los procedimientos de otras personas que no seamos nosotros mismos. Nunca sabemos si esa persona sabe operar correctamente su antivirus. Puede haber revisado sólo un tipo de virus y dejar otros sin controlar durante su escaneo o puede tener un módulo residente que es menos efectivo que nuestro antivirus.
6. Para bajar páginas de internet, archivos ejecutables, etc., definir siempre en nuestra PC una carpeta o directorio para recibir el material. De ese modo sabemos que todo lo que bajemos de internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.
7. Nunca abrir un adjunto de un e.mail sin antes chequearlo con nuestro antivirus. Si el adjunto es de un desconocido que no nos avisó previamente del envío del material, directamente borrarlo sin abrir.
8. Al actualizar el antivirus, verificar nuestra PC completamente. En caso de detectar un virus, proceder a verificar todos nuestros soportes (diskettes, CD's, ZIP's etc.)
9. Si por nuestras actividades generamos grandes bibliotecas de diskettes conteniendo información, al guardar los diskettes en la biblioteca, verificarlos por último vez, protegerlos contra escritura y fecharlos para saber cuándo fue el último escaneo.
10. Haga el backup periódico de sus archivos. Una vez cada 15 días es lo mínimo recomendado para un usuario doméstico. Si usa con fines profesionales su PC, debe hacer backup parcial de archivos cada 48 horas como mínimo. Backup parcial de archivos es la copia en diskette de los documentos que graba.

d. Etapas para Implantar un Sistema de Seguridad

Para que su plan de seguridad entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguientes 8 pasos:

1. Introducir el tema de seguridad en la visión de la empresa.
2. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
3. Capacitar a los gerentes y directivos, contemplando el enfoque global.
4. Designar y capacitar supervisores de área.
5. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
6. Mejorar las comunicaciones internas.
7. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
8. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

e. Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

f. Disposiciones que Acompañan la Seguridad

Desde el punto de vista de seguridad, se debe contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo, a saber:

- Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- Medidas en caso de desastre como perdida total de datos, abuso y los planes necesarios para cada caso.
- Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- Verificar el tipo de acceso que tiene las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación y viceversa.
- Que los operadores no sean los únicos en resolver los problemas que se presentan.

Direcciones de Internet Revisadas

http://cache.fdo-may.ubiobio.cl/decom/doc/VIRUS2.htm

http://www.geocities.com/diana_m_alvarez/principal.htm

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

http://dmi.uib.es/~bbuades/auditoria/auditoria.PPT

http://www.delitosinformaticos.com/propiedadindustrial/auditoria.shtml

http://www.monografias.com/trabajos5/audi/audi.shtml

http://www.monografías.com/trabajos11/breverres/breverres.shtml

http://www.monografías.com/trabajos/seguinfo/seguinfo/shtml

http://www.geocities.com/Athens/Olympus/7428/virus1.html

http://ciberconta.unizar.es/LECCION/SEGURO/101.HTM

http://www.criptored.upm.es/guiateoria/gt_m142a.htm

http://www.google.com/search?hl=es&ie=UTF-8&oe=UTF-8&q=%22politicas+de+seguridad+informatica%22&btnG=B%C3%BAsqueda+en+Google&lr=lang_es

http://www.notariado.org/noticias/escriturapublica/16%20escriturapublica/la[arroba]2.htm

http://pp.terra.com.mx/ hugalde/virussoy.html

http://www.belt.es/articulos/articulo.asp?id=65

http://www.ctv.es/USERS/mpq/estrado/estrado004.html

http://web.bemarnet.es/seguridad.html

http://www.filetopia.org/es/politics.htm

http://www.ispjae.edu.cu/eventos/citel/articulos/seguridad.htm

http://216.239.53.100/search?q=cache:X69gAEDxg5QC:europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_es.pdf+%22seguridad+de+redes%22&hl=es&lr=lang_es&ie=UTF-8

LIBROS

Revista PC WORLD. Los Secretos del nuevo Office. Edición julio 2001 Panamá, año 8 número 101.

Revista PC WORLD. Proteja su PC, como evitar ataque de virus. Edición julio 2002. Panamá, año 10, número 112.

INTEGRANTES:

ANGELICA COITE

HUGO ROMERO

Comentarios

Para dejar un comentario, regístrese gratis o si ya está registrado, inicie sesión.

Trabajos relacionados

Actividades en la planeación de sistemas de información.
Hallazgos de los hechos. Herramientas para documentar procesos y decisiones. Árboles de decisión. Tablas de decisión. Es...

Computadores CuánticosA lo largo del último medio siglo, las computadoras han ido duplicando su velocidad cada dos años, al tiempo que el tama...

Comunicación de datos Aplicaciones de las comunicaciones de datos en los negocios. Intercambio electrónico de datos (EDI). Hardware para el so...

Ver mas trabajos de General