EJE N° 1: SEGURIDAD INFORMÁTICA

La creciente globalización de la economía en el mundo ha incrementado la necesidad en las organizaciones a abrir sus puertas al entorno que las rodea y disponer de información íntegra y confiable en el momento adecuado. Debido al incremento en la complejidad de las operaciones de las organizaciones y a la disminución en los tiempos de respuesta requeridos, la única forma de disponer del recurso de la información es teniendo sistemas de información confiables que permitan a la Organización estar en la vanguardia tecnológica y responder oportunamente a las exigencias de un mercado cada vez más competitivo.

La integridad, confidencialidad, confiabilidad y disponibilidad de la información solo puede ser garantizada adoptando los mecanismos adecuados de seguridad en la organización. El aumento de la competencia incrementa la necesidad de establecer políticas y procedimientos de seguridad efectivas que disminuyan los riesgos de que se produzca un escape, alteración o destrucción de datos que sean de vital importancia para la organización.

Un sistema de información dentro de una organización juega el papel análogo al del sistema nervioso de un animal. Incluido en el sistema están los componentes que ejecutan funciones tales como la percepción, clasificación, transmisión, almacenamiento, recuperación, Transformación. Su propósito primordial es proporcionar información (en el momento en que se le solicite) para la toma de decisiones y la coordinación. En el sentido más amplio el sistema de información incluye todos los componentes envueltos en la toma de decisiones, coordinación y advertencia tanto humanos como automáticos. Es así como dada la importancia que tiene este hoy en día para la continuidad del negocio de la organización, que se debe enfrentar el tema de la seguridad de la información como un tema en el que está en juego todos los componentes de la organización.

El objetivo principal de la Seguridad Informática es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora y los datos. Todo esto enmarcado en un metaobjetivo que es el de mantener la **continuidad de los procesos** organizacionales que soportan los sistemas de información.

La Seguridad es un elemento importante de cualquier Servicio y Sistema Informático, aunque a menudo esta es postergada, basta tan sólo una brecha en la seguridad para crear graves daños. Por esto, el papel de la Seguridad Informática es cada vez más importante y no podrá ser ignorado, especialmente por el aumento de la exposición al riesgo que implica la cada vez mayor integración y globalización de los Sistemas Informáticos.

Una Primera Aproximación

El tema de seguridad es complejo y hay varias razones para ello: La gran cantidad de información que manejan las empresas, la conectividad entre sistemas y equipos, pero por sobre todo, la falta de políticas globales al interior de la empresa para enfrentarlo en forma clara y con las herramientas apropiadas.

A continuación se presenta los resultados de encuestas hechas por la Sentry Market Research a 945 directivos de empresa con un nivel tecnológico medio-alto, el 80% está planeando implementar mayores medidas de seguridad en los próximos dos años, y el 29% ya implementó sistemas y software de seguridad.

Un estudio realizado por Intrusión Detección Inc. a 32.250 usuarios de medianas y grandes empresas, extraía las siguientes conclusiones en cuanto a los principales problemas relacionados con la seguridad detectados en la empresa:

- Los usuarios no cambian los passwords con suficiente frecuencia
- El acceso a los archivos es demasiado libre
- La aplicación de normas de seguridad para nuevos usuarios es inconsistente
- Los passwords son fácilmente identificables

- Los identificadores de usuarios están inactivados

Obstáculos para incorporar estrategia de Seguridad en la empresa.

- Falta de herramientas y soluciones de seguridad
- Falta de administración
- Falta de presupuesto
- Falta de recursos humanos

Muchas organizaciones sufren pérdidas financieras apreciables por asuntos relacionados con la seguridad de la información. Así, el 54 % de los encuestados para la realización de este estudio afirmó que sus compañías habían sufrido pérdidas durante los dos años anteriores debido a la seguridad de la información y a la recuperación tras el desastre. Si además se incluyen las pérdidas causadas por los virus informáticos, este porcentaje aumenta hasta alcanzar un 78 %.

Problemas de seguridad que han supuesto pérdidas Financieras

- Virus
- Errores accidentales
- Tiempo de inactividad que no ha causado desastres
- Daños intencionados llevados a cabo por los empleados
- Desastres naturales
- Daños provocados desde el exterior
- Espionaje industrial

Las pérdidas de capital sufridas por las empresas consultadas fueron substanciales, aunque no cuantificables en algunos casos: cerca del 70 % de los encuestados no pudo calcular cuánto había perdido su empresa. Entre aquellas que sí conocían el alcance de las pérdidas, más del 25% las situaba hasta 250.000 dólares, y algunas incluso en más de un millón de dólares.

Definir los límites de seguridad en las empresas es casi imposible porque involucra a **toda la organización**. No solo se trata de protegerla del ambiente externo, sino que también del mal manejo que se puede producir en su interior. Y cada día se está haciendo más común escuchar de firewalls, autentificación de usuarios, control de acceso, firmas digitales, etc. A nivel nacional estamos en una primera etapa, donde las grandes empresas han sido muy sensibles al tema (firewalls) lo que se debe en gran medida, a los temores que existen sobre la inseguridad de la internet tradicional, pero en el resto de las áreas se ha hecho muy poco. Es así como además el desarrollo de la seguridad de los SI/TI en las empresas está en directa relación con la evolución de estas en ellas mismas, las pequeñas y medianas empresas (Pymes), en donde los SI/TI tienen poco tiempo de vida, son las que se encuentran más vulnerables.

SEGURIDAD DE SI/TI

¿Qué es la seguridad informática?

En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen en ella y su corta vida aun. Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, planes, políticas, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

Existe una medida cualitativa para la Seguridad que dice "Un sistema es seguro si se comporta como los usuarios esperan que lo haga" (Dr. Eugene Spafford).

Objetivos que persigue

Como ya se mencionaba en la introducción los objetivos que persigue la seguridad de los SI/TI es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora y los datos. Todo esto enmarcado en un metaobjetivo que es el de mantener la **continuidad de los procesos**

organizacionales que soportan los sistemas de información.
Como es sabido en todas las empresas existen **procesos críticos** que constituyen la medula espinal para que funcione el negocio y muchos de estos procesos críticos son apoyados por los sistemas de información, es por esto que la seguridad de estos resulta de vital importancia para que la empresa pueda mantenerse y continuar en su negocio.

La seguridad como problema cultural

Una de las paradojas es que a pesar de que cada vez se destinan mayores recursos para el área informática y que esta se ha vuelto esencial para la gestión de negocios de las empresas, el presupuesto asignado específicamente al tema de seguridad, no ha crecido en la misma Proporción. Por esto es fundamental crea **conciencia** al interior de las organizaciones para que puedan dimensionar en su justa medida la relevancia del problema, porque si se miran los presupuestos de informática dentro de las empresas, vemos que han crecido notablemente, pero no ha ocurrido lo mismo con los presupuestos asignados a las áreas de seguridad. Mientras más tecnología se incorpora, más se agranda la brecha en lo que son debilidades de seguridad. Actualmente hay empresas que basan sus procesos en de negocios en TI y eso provoca que la empresa este **dependiendo** cada vez mas de estas herramientas tecnológicas y paralelamente van creciendo los temas relacionados con la seguridad. Por esto es fundamental la creación de conciencia en las empresas.
Una de las razones por las cuales no ha despegado fuertemente el comercio electrónico en el país es que ante la decisión de las empresas de abrirse a este tema, que va a requerir el Desarrollo de mecanismo de seguridad, prefieren postergarla y si a este le sumamos la precaria condición de la legislación con respecto al tema la opción queda desechada. La tecnología disponible hoy en día hace posible una transferencia electrónica en forma segura, el problema es que la que la gente no sabe cómo hacerlo y tiene como consecuencia que el país se está quedando atrás no por un problema tecnológico, si no por un problema de **mentalidad.**
Sin duda como vemos la seguridad es fundamental no solo para evitar desastres o perdidas irrecuperables que afecten el funcionamiento de las organizaciones, sino que también para potenciar nuevas áreas de negocios que permitan el crecimiento de los diferentes actores del mercado.

La seguridad como proceso

Uno de los puntos de consenso en el tema es que la seguridad es un proceso y no actividad particular que desarrolla la empresa, un proceso que barre todas las unidades funcionales de Esta. Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no solo implica una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar **confiabilidad** a la información, lo que en ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.
El problema hay que enfrentarlo con tecnología, pero también debe involucrar a los tomadores de decisiones, que son finalmente quienes deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

Propiedades de la Información que protege la Seguridad Informática.

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

- **Confidencialidad** : Se define como la "condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados". La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. A menudo se la relaciona con la Intimidad o Privacidad, cuando esa Información se refiere a personas físicas.
- **Integridad:** Se define como la "condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado". La integridad está vinculada a la **fiabilidad funcional** del sistema de

información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél). La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

- **Disponibilidad**: Se define como el "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable". Se asocia a menudo a la **fiabilidad técnica** (tasa de fallos) de los componentes del sistema de información. La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o "tirar" el servidor.
- **Autentificacion o no repudio:** Se define como "el mecanismo que permite conocer si la persona que está accediendo a un sistema, es realmente quien debe acceder y no un extraño". El no repudio se refiere a los que se hacen sobre en temas de correo electrónico para garantizar la autenticidad del remitente (un mecanismo son las firmas Digitales).

Factores que afectan a los sistemas de Información

Los principales factores que se ciernen sobre los sistemas Informáticos tienen orígenes diversos. Así, si consideramos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, terremotos, sabotajes,... Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos intensos y frecuentemente, por errores de operación. Las líneas de comunicación pueden ser interferidas, etc.

Otros tipos de amenazas provienen de usuarios o empleados infieles. Así, los primeros pueden usurpar la personalidad de usuarios autorizados y acceder indebidamente a datos para su consulta o borrado, o aunque algo más complicado, modificar en su provecho programas de aplicación.

Otras amenazas más sutiles provienen de inadecuados controles de programación. Así, el problema de residuos, es decir, de la permanencia de información en memoria principal cuando ésta es liberada por un usuario o, en el caso de dispositivos externos cuando ésta es incorrectamente borrada.

Una técnica fraudulenta muy usada consiste en transferir información de un programa a otro mediante canales ilícitos y no convencionales (canales ocultos).

Factores que afecta la integridad de los datos

- **Desastres naturales:** Inundaciones, incendios, tormentas, terremotos etc.
- **Fallas de Hardware:** Discos, controladores, energía, memoria, dispositivos etc.
- **Fallas Humanas:** Accidentes, inexperiencias, estrés, problemas de comunicación, venganza, interés personal.
- **Fallas en la red:** Controladores, tarjetas, componentes, radiación
- **Problemas de SW o lógicos:** Requerimientos mal definidos, corrupción de archivos, errores de programas o aplicaciones, problemas de almacenamiento, errores de SO.

Factores que afectan a la seguridad de los datos

- **Autentificación :** La forma en que se hace el proceso de acceso a los sistemas, passwords, perfiles de usuario.
- **Basados en cables:** Todos los cables son "pinchables" es decir se acceder fácilmente a los datos que circulan de un nodo a otro en una red , para esto se utilizan las técnicas de encriptación.
- **Físicas:** averías en los componentes físicos, robo, espionaje industrial etc.
- **Programación:** Aplicaciones mal construidas, los bugs en el software de la industria que necesita de parches para reducir el riesgo de perder los datos
- **Puertas Falsas:** En la mayoría de los software existen puertas falsas que permiten alterar o manipular los datos con los cuales estos trabajan (ej.: manipulación de tablas en las base de datos).

En Resumen

La información y los sistemas que la soportan constituyen recursos valiosos e importantes para la Organización. Su seguridad suele ser imprescindible para mantener valores esenciales, sean propios del sector público (servicio, seguridad procedimental, imagen), propios del sector privado (competitividad, rentabilidad) o comunes a ambos (permanencia del funcionamiento, cumplimiento de la legalidad). Dicha seguridad consiste al final en un depósito de confianza suficiente en la capacidad de dicha información y sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la Organización. Cualquier amenaza que se materialice contra el flujo normal de la información en una Organización, pone de relieve la dependencia y la vulnerabilidad de toda la Organización (en un grado que es consecuente con la gravedad de la amenaza, como es lógico).

El crecimiento de las redes y la consecuente conectividad entre sistemas representa nuevas oportunidades, no sólo positivas, sino también negativas al facilitar por ejemplo los accesos no autorizados y al reducir las facilidades de control centralizado y especializado de los sistemas de información.

Los sistemas de información de cualquier Organización están sometidos a *amenazas* más o menos destructivas (como ampliamente difunden los medios de comunicación incluso los no especializados). Amenazas que van desde fallos técnicos y accidentes no intencionados (pero no menos peligrosos), hasta acciones intencionadas, más o menos lucrativas, de curiosidad, espionaje, sabotaje, vandalismo, chantaje o fraude. Todas las opiniones aseguran que las amenazas a la seguridad de los sistemas de información y a la información misma serán cada vez más ambiciosas y sofisticadas.

El objeto o propósito de la seguridad de los sistemas de información consiste sobre todo en mantener la *continuidad de los procesos* organizacionales que soportan dichos sistemas. Asimismo intentar minimizar tanto el *costo global* de la ejecución de dichos procesos como las *pérdidas* de los recursos asignados a su funcionamiento.

El sujeto global de la seguridad se determina como un Dominio del conjunto de la Organización, que suele considerarse compuesto por Activos (como sujetos elementales de la seguridad), estructurados metódicamente de forma jerarquizada.

La seguridad siempre es barata a largo plazo (y lo es también cada vez más a corto plazo). El ahorro y la eficacia que proporciona son relativos, pues dependen de su costo propio y su implantación inteligente; pero siempre son muy superiores si los requerimientos y especificaciones de seguridad se incorporan en el propio desarrollo de los sistemas y los servicios de información. *Cuanto más temprano se actúe para dar seguridad a los sistemas de información, más sencilla y económica resultará ésta a la Organización.*

Estrategias de seguridad informática

Cuando se habla de la función informática generalmente se tiende a hablar de nuevas tecnologías, de nuevas aplicaciones, nuevos dispositivos, etc.

Sin embargo, se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la ***Información***.

La información es un bien económico, por lo cual requiere normas de protección.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información, lo que constituye un delito informático.

¿Qué es un delito informático?

Maniobra dolosa que opera sobre un sistema de información alterando la integridad, confidencialidad o disponibilidad de la información procesada.

Los sistemas informáticos necesitan mantener seguridad en distintos aspectos de la información, estos son:

Confidencialidad: El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado, información personal e información comercial patentada.

Integridad: El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales.

Disponibilidad: El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes.

Los administradores de seguridad deben desarrollar distintas estrategias de seguridad decidiendo el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles apropiados.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas y deben ser actualizadas permanentemente.

Norma ISO 17799

ISO es una Federación de organismos de normalización, con sede en Ginebra, formada por un solo representante por país.

Dentro de las normas ISO nos encontramos con la Norma ISO 17799, que trata sobre la seguridad informática

ISO 17799

ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes. Así, la norma discute la necesidad de contar con firewall, pero no profundiza sobre los tipos de firewall.

Objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información escrita, hablada y almacenada en las computadoras.

Desarrollar un **sistema de seguridad** significa : "planificar, 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"

La seguridad informática abarca varios aspectos, a saber:

- Seguridad informática física, como los controles de acceso físico.
- Seguridad de la red (por ejemplo, las referentes al correo electrónico y a Internet, accesos remotos, etc.).
- Seguridad de los datos (control de acceso y controles de integridad).

Virus informático

Un virus es un malware que tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un *software*, son muy nocivos y algunos contienen además una carga dañina (*payload*) 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 ejecutar. 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.

El primer virus atacó a una máquina IBM Serie 360 (y reconocido como tal). Fue llamado Creeper, (ENMS) creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» («¡Soy una enredadera... agárrame si puedes!»). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (cortadora).

Métodos de propagación

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*, o, más comúnmente: *Haz 2 clics y gana 2 tonos para móvil gratis*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software modificado o de dudosa procedencia.

Métodos de protección

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

Antivirus

- **Antivirus:** Son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Por ejemplo, al verse que se crea un archivo llamado *Win32.EXE.vbs* en la carpeta *C:\Windows\%System32%* en segundo plano, ve que es comportamiento sospechoso, salta y avisa al usuario.

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

- Actualización automática: Consiste en descargar e instalar las actualizaciones que el fabricante del sistema operativo lanza para corregir fallos de seguridad y mejorar el desempeño. Dependiendo de la configuración el proceso puede ser completamente automático o dejar que el usuario decida cuándo instalar las actualizaciones.

Pasivos

- No instalar software de dudosa procedencia.
- No abrir correos electrónicos de desconocidos ni adjuntos que no se reconozcan.
- Usar un bloqueador de elementos emergentes en el navegador.
- Usar la configuración de privacidad del navegador.
- Activar el Control de cuentas de usuario.
- Borrar la memoria caché de Internet y el historial del navegador.
- No abrir documentos sin asegurarnos del tipo de archivo. Puede ser un ejecutable o incorporar macros en su interior.

Tipos de virus

Existen diversos tipos de virus, varían según su función o la manera en que este se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- Recycler: consiste en crear un acceso directo de un programa y eliminar su aplicación original, además al infectar un pendrive convierte a toda la información en acceso directo y (Se cambia la palabra "elimina" por "oculta") oculta el original de modo que los archivos no puedan ser vistos(Se cambió "no son recuperables" por "no pueden ser vistos"), pero con la creación de un archivo "batch" que modifique los atributos de los archivos contenidos en el pendrive, estos podrían ser recuperados.
- Troyano: Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.
- Gusano: Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
- Bombas lógicas o de tiempo: Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.
- *Hoax*: Los *hoax* no son virus ni tienen capacidad de reproducirse por sí solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.
- Joke: Al igual que los *hoax*, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga

Otros tipos por distintas características son los que se relacionan a continuación:

- **Virus residentes:**

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el

sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados. Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

- **Virus de acción directa:**

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

- **Virus de sobreescritura**:

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

- **Virus de boot (bot_kill) o de arranque:**

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco o unidad de almacenamiento CD, DVD, memorias USB, etc. En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los dispositivos de almacenamiento. Cuando un ordenador se pone en marcha con un dispositivo de almacenamiento, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los dispositivos de almacenamiento contra escritura y no arrancar nunca el ordenador con uno de estos dispositivos desconocido en el ordenador.

Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

- **Virus de enlace o directorio:**

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Los virus de enlace o directorio alteran las direcciones que indican donde se almacenan los ficheros. De este modo, al intentar ejecutar un programa (fichero con extensión EXE o COM) infectado por un virus de enlace, lo que se hace en realidad es ejecutar el virus, ya que éste habrá modificado la dirección donde se encontraba originalmente el programa, colocándose en su lugar.

Una vez producida la infección, resulta imposible localizar y trabajar con los ficheros originales.

- **Virus cifrados:**

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

- Virus polimórficos:

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartitos

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus del fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

- Virus de FAT:

La tabla de asignación de ficheros o FAT (del inglés *File Allocation Table*) es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador.

- Virus hijackers:

Son programas que secuestran navegadores de internet principalmente el Explorer. Los hijackers alteran las páginas iniciales del navegador e impide que el usuario pueda cambiarla, muestra publicidad en pops ups. Instala nuevas herramientas en la barra del navegador y a veces impiden al usuario acceder a ciertas páginas web. Un ejemplo puede ser no poder acceder a una página de antivirus.

- Virus Zombie:

Es cuando la computadora que es infectada es controlada por terceros. Se utiliza para diseminar virus, keyloggers y procedimientos invasivos en general. Esto puede ocurrir cuando la computadora tiene el firewall y su sistema operativo desactualizado.

- Virus Keylogger:

Este virus se encarga de registrar cada tecla que sea pulsada, en algunos casos también registran los clics. Son virus que quedan escondidos en el sistema operativo de manera que la víctima no tiene como saber que está siendo monitorizada. Los keyloggers se utilizan para usualmente para robar contraseñas de cuentas bancarias, obtener contraseñas personales como las del E-mail, Facebook, etc.