Banda ancha

Se conoce como banda ancha en telecomunicaciones a la transmisión de datos simétricos por la cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión. Así se utilizan dos o más canales de datos simultáneos en una única conexión, lo que se denomina multiplexación (ver apartado más abajo).

Algunas de las variantes de los servicios de Fiber To The Home son de banda ancha.

Los routers que operan con velocidades mayores a 100 Mbit/s también son banda ancha, pues obtienen velocidades de transmisión simétricas.

Al concepto de banda ancha hay que atribuirle otras características, además de la velocidad, como son la interactividad, digitalización y conexión o capacidad de acceso (función primordial de la banda ancha).

Patterson ya hablaba de que la conexión de banda ancha depende de la red de comunicaciones, de las prestaciones del servicio.

Ancho de banda

Para la velocidad de la información en sistemas informáticos y de telecomunicaciones, se define como Tasa de transferencia.

La tasa de transferencia se refiere al ancho de banda real medido en un momento concreto del día empleando rutas concretas de internet mientras se transmite un conjunto específico de datos, desafortunadamente, por muchas razones la tasa es con frecuencia menor al ancho de banda máximo del medio que se está empleando.

Los siguientes son algunos de los factores que determinan la tasa de transferencia:

- Dispositivos de Internet-Working
- Tipos de datos que se van a transferir
- Topología de la red

 Número de usuarios en la red

 La computadora del usuario

 El servidor

 Condiciones de la energía

 Congestión

El ancho de banda teórico de la red es una consideración importante en el diseño de la red, porque la tasa de transferencia de la red nunca es mayor que dicho ancho de banda, debido a las limitaciones puestas por el medio y a las tecnologías de red elegidas.

La unidad con que el Sistema Internacional de Unidades expresa el bit rate es el bit por segundo (bit/s, b/s, bps). La b debe escribirse siempre en minúscula, para impedir la confusión con byte por segundo (B/s). Para convertir de bytes/s a bits/s, basta simplemente multiplicar por "8" y viceversa.

Que la unidad utilizada sea el bit/s, no implica que no puedan utilizarse múltiplos del mismo:

 kbit/s o kbps (kb/s, kilobit/s o mil bits por segundo)

 Mbit/s o Mbps(Mb/s, Megabit/s o un millón de bits por segundo)

 Gbit/s o Gbps (Gb/s, Gigabit, mil millones de bits)

 byte/s (B/s u 8 bits por segundo)

 kilobyte/s (kB/s, mil bytes u ocho mil bits por segundo)

 megabyte/s (MB/s, un millón de bytes u 8 millones de bit por segundo)

 gigabyte/s (GB/s, mil millones de bytes u 8 mil millones de bits)

Compartición: Expresión que define el número de usuarios asignados a un determinado canal compartido.

Usuarios: Número de individuos que acceden al servicio.

El servicio de Internet se basa en la necesidad particular de las personas de acceder a información de una manera totalmente aleatoria. Todos tenemos intereses y necesidades

diferentes de consumir la información disponible en Internet. Esto hace que en las conexiones internacionales de internet, los proveedores podemos compartir los canales entre diferentes usuarios.

Así es como nace el concepto de compartición de canal en los proveedores de internet. A fin de poder llevar un control de la compartición se toma en cuenta la capacidad del canal internacional asignada para cierta cantidad de usuarios con determinados anchos de banda contratados.

La relación entre ancho de banda internacional y el ancho de banda total de los usuarios de Internet permite tener comparticiones de 1 a 1, 2 a 1, 4 a 1, etc. Por ejemplo si el ancho de banda en el canal internacional es 2048 Kbps y el proveedor tiene cuatro clientes de 512 Kbps, entonces estos clientes tienen una compartición de 1 a 1. Si el proveedor tiene los mismos 2048 Kbps y tiene 4 clientes de 1024 Kbps entonces decimos que estos clientes tienen una compartición de 2 a 1.

Y un último ejemplo, si el proveedor tiene un ancho de banda de 2048 Kbps y tiene 32 clientes de 512 Kbps cada uno, entonces estos clientes tienen un nivel de compartición de 8 a 1. Cuando un cliente evalúa la necesidad de contratar el servicio de Internet siempre debe consultar con su proveedor que nivel de compartición efectiva le va a entregar. Este concepto de compartición definitivamente va a influir en la tarifa mensual que aplique el proveedor a sus servicios. Los servicios de Internet residenciales por regla general tienen un nivel de compartición de hasta 8 a 1.

Seguridad informática

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello

existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Objetivos

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

 La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas,

robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

 Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

 La información: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Amenazas

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tenidas en cuenta, incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

 Usuarios: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobre dimensionados, no se les han restringido acciones innecesarias, etc.

 Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano,

una bomba lógica, un programa espía o spyware, en general conocidos como malware.

 Errores de programación: La mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.

 Intrusos: persona que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).

 Un siniestro (robo, incendio, inundación): una mala manipulación o una mala intención derivan a la pérdida del material o de los archivos.

 Personal técnico interno: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.

 Fallos electrónicos o lógicos de los sistemas informáticos en general.

 Catástrofes naturales: rayos, terremotos, inundaciones, rayos cósmicos, etc.

Vulnerabilidad del usuario

Existen diferentes tipos de ataques en Internet como virus, troyanos u otros, dichos ataques pueden ser contrarrestados o eliminados pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como “el eslabón más débil”. Dicho ataque es capaz de conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando

autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

Tipos de amenazas

Existen infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de phishing puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma (sin que deje de ser delito en ambos casos, al menos en países con legislación para el caso, como lo es España).

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

 Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

 Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos.

 Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser

exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.

 Amenazas externas: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Amenazas por el efecto

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

 Robo de información.

 Destrucción de información.

 Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.

 Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.

 Robo de dinero, estafas,...

Amenazas por el medio utilizado

Se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

 Virus informático: malware que tiene por objeto alterar el normal funcionamiento de la computadora, 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 un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

 Phishing.

 Ingeniería social.

 Denegación de servicio.

 Spoofing: de DNS, de IP, de DHCP, etc.

Amenaza informática del futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

 Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas".

 Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada

Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

 "La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas", La amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del

capital”.

 Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geoposicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc.

Para no ser presa de esta nueva ola de ataques más sutiles, se recomienda:

 Mantener las soluciones activadas y actualizadas.

 Evitar realizar operaciones comerciales en computadoras de uso público o en redes abiertas.

 Verificar los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

Análisis de riesgos

Artículo principal: Análisis de riesgo informático.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

Elementos de un análisis de riesgo

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras. La fórmula para determinar el riesgo total es:

RT (Riesgo Total) = Probabilidad x Impacto Promedio

A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el riesgo residual.

Análisis de impacto al negocio

Véase también: Economía de seguridad informática.

El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver.

Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: confidencialidad de la información, la integridad (aplicaciones e información) y finalmente la disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor web público pueden poseer la característica de confidencialidad baja (ya que toda la información es pública) pero necesita alta disponibilidad e integridad, para poder

ser confiable. En contraste, un sistema de planificación de recursos empresariales (ERP) es, habitualmente, un sistema que posee alto puntaje en las tres variables.

Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

Puesta en marcha de una política de seguridad

Véanse también: Plan de contingencias y Plan de continuidad del negocio.

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Por ejemplo, en España, la Ley Orgánica de Protección de Datos de carácter personal o también llamada LOPD y su normativa de desarrollo, protege ese tipo de datos estipulando medidas básicas y necesidades que impidan la pérdida de calidad de la información o su robo. También en ese país, el Esquema Nacional de Seguridad establece medidas tecnológicas para permitir que los sistemas informáticos que prestan servicios a los ciudadanos cumplan con una requerimientos de seguridad acordes al tipo de disponibilidad de los servicios que se prestan.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

 Elaborar reglas y procedimientos para cada servicio de la organización.

 Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión

 Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables

jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida.

Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

Técnicas para asegurar el sistema

Dos firewalls permiten crear una DMZ donde alojar los principales servidores que dan servicio a la empresa y la relacionan con Internet. Por ejemplo, los servidores web, los servidores de correo electrónico,... El router es el elemento expuesto directamente a Internet y, por tanto, el más vulnerable.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo.

Cada tipo de ataque y cada sistema requiere de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos)

A continuación se enumeran una serie de medidas que se consideran básicas para asegurar un sistema tipo, si bien para necesidades específicas se requieren medidas extraordinarias y de mayor profundidad:

 Utilizar técnicas de desarrollo que cumplan con los criterios de seguridad al uso para todo el software que se implante en los sistemas, partiendo de estándares y de personal suficientemente formado y concienciado con la seguridad.

 Implantar medidas de seguridad físicas: sistemas antiincendios, vigilancia de los

centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.

 Codificar la información: criptología, criptografía y criptociencia. Esto se debe realizar en todos aquellos trayectos por los que circule la información que se quiere proteger, no solo en aquellos más vulnerables. Por ejemplo, si los datos de una base muy confidencial se han protegido con dos niveles de firewall, se ha cifrado todo el trayecto entre los clientes y los servidores y entre los propios servidores, se utilizan certificados y sin embargo se dejan sin cifrar las impresiones enviadas a la impresora de red, tendríamos un punto de vulnerabilidad.

 Contraseñas difíciles de averiguar que, por ejemplo, no puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad. Las contraseñas, además, deben tener la suficiente complejidad como para que un atacante no pueda deducirla por medio de programas informáticos. El uso de certificados digitales mejora la seguridad frente al simple uso de contraseñas.

 Vigilancia de red. Las redes transportan toda la información, por lo que además de ser el medio habitual de acceso de los atacantes, también son un buen lugar para obtener la información sin tener que acceder a las fuentes de la misma. Por la red no solo circula la información de ficheros informáticos como tal, también se transportan por ella: correo electrónico, conversaciones telefónica (ToIP),

mensajería instantánea, navegación Internet, lecturas y escrituras a bases de datos, etc. Por todo ello, proteger la red es una de las principales tareas para evitar robo de información. Existen medidas que abarcan desde la seguridad física de los puntos de entrada hasta el controld e equipos conectados, por ejemplo 802.1x. En el caso de redes inalámbricas la posibilidad de vulnerar la seguridad es

mayor y deben adoptarse medidas adicionales.

 Redes perimetrales de seguridad, o DMZ, permiten generar reglas de acceso fuertes entre los usuarios y servidores no públicos y los equipos publicados. De esta forma, las reglas más debíles solo permiten el acceso a ciertos equipos y nunca a los datos, que quedarán tras dos niveles de seguridad.

 Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.

 Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

 Copias de seguridad e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.

 Controlar el acceso a la información por medio de permisos centralizados y mantenidos (tipo Active Directory, LDAP, listas de control de acceso, etc.). Los medios para conseguirlo son:

 Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

 Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

 Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

 Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro. y que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

 Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los

sistemas o aplicaciones empleadas.

 Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo, como se ha indicado más arriba, e incluso utilizando programa que ayuden a los usuarios a la gestión de la gran cantidad de contraseñas que tienen gestionar en los entornos actuales, conocidos habitaulmente como gestores de identidad.

 Redundancia y descentralización.

Respaldo de información

Artículo principal: Copia de seguridad.

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups. Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (solo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

 Continuo

El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

 Seguro

Muchos softwares de respaldo incluyen cifrado de datos, lo cual debe ser hecho

localmente en el equipo antes del envío de la información.

 Remoto

Los datos deben quedar alojados en dependencias alejadas de la empresa.

 Mantenimiento de versiones anteriores de los datos

Se debe contar con un sistema que permita la recuperación de, por ejemplo, versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online, servicio de backup remoto, están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información derivando la necesidad del crecimiento de la copia de respaldo a proveedor del servicio.

Protección contra virus

Los virus son uno de los medios más tradiccionales de ataque a los sistemas y a la información que sostienen. Para poder evitar su contagio se deben vigilar los equipos y los medios de acceso a ellos, principalmente la red.

Control del software instalado

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en

caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Control de la red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red solo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

Protección física de acceso a las redes

Independientemente de las medidas que se adopten para proteger a los equipos de una red de área local y el software que reside en ellos, se deben tomar medidas que impidan que usuarios no autorizados puedan acceder. Las medidas habituales dependen del medio físico a proteger.

A continuación se enumeran algunos de los métodos, sin entrar al tema de la protección de la red frente a ataques o intentos de intrusión desde redes externas, tales como Internet.

Redes cableadas

Las rosetas de conexión de los edificios deben estar protegidas y vigiladas. Una medida básica es evitar tener puntos de red conectados a los switches. Aún así siempre puede ser sustituido un equipo por otro no autorizado con lo que hacen falta medidas adicionales: norma de acceso 802.1x, listas de control de acceso por MAC addresses, servidores de DHCP por asignación reservada, etc.

Redes inalámbricas

En este caso el control físico se hace más difícil, si bien se pueden tomar medidas de contención de la emisión electromágnética para circunscribirla a aquellos lugares que consideremos apropiados y seguros. Además se consideran medidas de calidad el uso del cifrado (WEP, WPA, WPA v.2, uso de certificados digitales, etc.), contraseñas compartidas y, también en este caso, los filtros de direcciones MAC, son varias de las

medidas habituales que cuando se aplican conjuntamente aumentan la seguridad de forma considerable frente al uso de un único método.