Políticas de seguridad para una red local en plataforma NT

Autor: Miledi del Rocío Moreno García

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarrra

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

No. DE ACUERDO 952006 CLAVE 16PSU0014Q

"POLÍTICAS DE SEGURIDAD PARA UNA RED LOCAL EN PLATAFORMA NT "

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

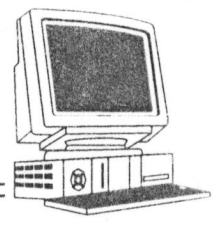
PRESENTA

Miledi del Rocío Moreno García

ASESOR DE TESINA

M.A. Ing. Sergio Francisco Barraza Ibarra

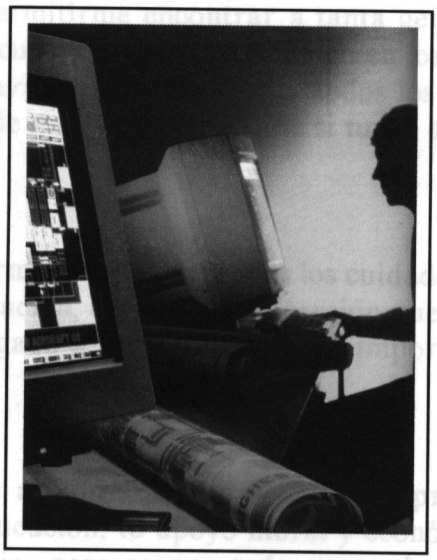
MORELIA, MICH., MÉXICO SEPTIEMBRE 2004



UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

No. DE ACUERDO 952006 **CLAVE 16PSU0014Q**



"POLÍTICAS DE SEGURIDAD PARA UNA RED LOCAL EN PLATAFORMA NT"

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:

MILEDI DEL ROCÍO MORENO GARCÍA

ASESOR DE TESINA:

M.A. ING. SERGIO FRANCISCO BARRAZA IBARRA

MORELIA, MICH., MEXICO **SEPTIEMBRE 2004**

AGRADECIMIENTOS

En primer lugar le agradezco a **DIOS** por darme la familia que tengo: mis padres, hermanos, sobrinos, por permitirme encontrar a tanta gente con la que he convivido a lo largo de toda mi vida y las cuales han estado conmigo en los momentos difíciles. **GRACIAS DIOS** por la vida tan maravillosa que tengo, por todos los bienes y todas las cosas buenas que me has dado a través de mis padres, por que si tu no quisieras yo no estaría aquí y no seria lo que soy.

GRACIAS MAMA, por darme la vida, por todos los cuidados que me diste cuando era niña y te necesitaba, por la educación, cariño y comprensión que me has brindado siempre, si no fuera por ti no hubiera llegado a este momento tan importante en mi vida, esta tesina es dedicada para ti. Te quiero.

GRACIAS PAPA, por que al igual que mi Mamá siempre estuviste conmigo cuando te necesite, te agradezco la educación, tu apoyo moral y económico, se que las metas que uno tiene cuestan mucho trabajo, pero se que todo se puede alcanzar porque tu me lo has enseñado y eres mi ejemplo a seguir, este trabajo también es dedicado para ti. Te quiero

GRACIAS HERMANOS, José Luis, Elizabeth, Jannet y Carlitos, les agradezco a todos el estar conmigo a lo largo de mi vida, ustedes son mi familia y siempre van a estar primero que todos, porque con ustedes crecí, gracias por sus consejos, por su cariño y comprensión. Gracias Angeles y Paco, ustedes también ya son parte de la familia. A todos los quiero mucho

GRACIAS SOBRINITOS, José Luis y Fernanda Mariel, por que hacen que mi vida sea mas feliz. Son mis amores

GRACIAS MAU, porque estuviste conmigo en los momentos difíciles de mi carrera, porque siempre me ayudaste con tus consejos a seguir adelante y a no vencerme por las situaciones difíciles, porque cuando me sentía sola siempre estuviste conmigo. Te quiero mucho

GRACIAS EUGENIA, por ser mi mejor amiga, porque nunca me dejaste sola cuando tuve problemas, porque siempre me ayudaste en toda la carrera y juntas salimos adelante, porque sin ti no hubiera sido tan divertida mi estancia en la escuela, porque me estuviste presionando para que terminara la Tesina y por lo tanto va dedicada también para ti. T.Q.M

GRACIAS NESTOR, por ser mi mejor amigo, porque me ayudaste para lograr esta meta, porque siempre me apoyaste y nunca me dejaste sola, porque se que en ocasiones tenias cosas que hacer pero sin embargo nunca me diste la espalda, te agradezco el haber estado conmigo siempre, sin ti no lo hubiera logrado. T.Q.M

GRACIAS JULIO, por ser mi amigo, porque me apoyaste mucho para lograr esto, por tus consejos, por tu tiempo y por tu ayuda incondicional, estoy muy agradecida contigo por todo. T.Q.M.

GRACIAS A MIS AMIGOS DE LA UVAQ, porque aunque hubo momentos dificiles siempre alguien sonreía y hacia mas placentero el estudiar, y que después de todo pasamos momentos muy padres juntos. (Katia, Alicia, Mary, Hass, Uli, Fok, Dono, Fer, Moi, Jorge) Los quiero

GRACIAS A TODOS MIS AMIGOS, por estar siempre conmigo (Diana,Yoana, America, Paula, Enrique, Maghe, Jorge y Gaby) Los quiero mucho.

GRACIAS ING. BARRAZA, por ser mi asesor de esta Tesina y por todas sus enseñanzas.

INDICE

ANTECEDENTES

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que confrontan las empresas hoy día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos.

Las políticas de seguridad son orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos.

Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales.

Por otro lado las políticas son de jerarquía superior a las normas, estándares y procedimientos que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementacion y otros aspectos en detalle. Además las políticas deberían durar muchos años, mientras que las normas y procedimientos duran menos tiempo.

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos.

Las políticas son distintas y de un nivel superior a los procedimientos, que son los pasos operacionales específicos que deben llevarse a cabo para lograr una cierta meta. Como ejemplo, hay procedimientos específicos para realizar copias de seguridad de la información contenida en los discos duros de los servidores.

Una declaración sobre políticas describe sólo la forma general de manejar un problema específico, pero no debe ser demasiado detallada o extensa, en cuyo caso se convertiría en un procedimiento.

Las políticas también son diferentes de las medidas de seguridad o de los mecanismos de control. Un ejemplo de esto último sería un sistema de cifrado para las comunicaciones o para los datos confidenciales guardados en discos y cintas. En muchos casos las políticas definen metas ó objetivos generales que luego se alcanzan por medio de medidas de seguridad.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles sobre cómo aplicar esta política. Por ejemplo, la metodología a usar para probar el software.

Un documento sobre políticas de seguridad contiene, entre muchos aspectos: definición de seguridad para los activos de información, responsabilidad de gestión de contraseñas, sistema de control de acceso, respaldo de datos, manejo de virus e intrusos. También puede incluir la forma de comprobar el cumplimiento y las eventuales medidas disciplinarias.

INTRODUCCIÓN

Antes de embarcarse en un esfuerzo de elaborar las políticas de seguridad, es aconsejable aclarar quién es responsable de promulgarlas y aplicarlas, si se ignora este paso importante, se corre el riesgo de posteriores objeciones, críticas y malentendidos, que pueden significar problemas y grandes retrasos.

Otro requisito previo necesario para tener éxito involucra la perspectiva de la Junta Directiva y la alta gerencia. Sólo después de que sus miembros tomen conciencia de que los activos de información son un factor vital para el éxito de la organización, es que la seguridad informática es apreciada como un asunto serio que merece atención. En caso contrario probablemente no apoyen la idea de establecer políticas de seguridad.

La alta gerencia debe darse cuenta que hay problemas serios de seguridad y que se requiere de políticas para afrontarlos. Si bien esto puede parecer obvio, muchos intentos de desarrollar e implantar las políticas no ha llegado a ninguna parte a consecuencia de esto. El trabajo previo incluye a menudo una breve presentación a la alta gerencia para sensibilizarla sobre la necesidad de la seguridad informática.

Idealmente, el desarrollo de políticas de seguridad debe comenzarse después de una evaluación a fondo de las vulnerabilidades, amenazas y riesgos. Esta evaluación debería indicar, quizás sólo a grandes rasgos, el valor de la información en cuestión, los riesgos a los cuales esa información se sujeta, y las vulnerabilidades asociadas a la manera actual de manejar la información. También pueden ser incluidos en la declaración de las políticas, los tipos generales de riesgos enfrentados por la organización, así como cualquier otra información útil obtenida a partir del análisis de riesgos.

Un buen momento para desarrollar un conjunto de políticas de seguridad es cuando se está preparando el manual de seguridad para los activos de información. Debido a que ese manual va a ser distribuido a lo largo de toda la organización, representa un medio excelente para incluir también las políticas de seguridad. También pueden publicitarse las políticas en material tal como video, carteles o artículos en un periódico interno.

Otro bueno momento es después de que haya ocurrido una falla grave en seguridad, por ejemplo una intrusión de hackers, un fraude informático, un accidente sin poder recuperar los datos, un incendio y en general algún tipo de daño o perjuicio que haya recibido la atención de la alta gerencia. En este caso habrá un alto interés en que se apliquen las políticas de seguridad y que se implanten medidas más efectivas. Hay que actuar rápidamente para desarrollar las políticas, ya que el nivel de preocupación de los gerentes y de los empleados tiende a decrecer luego que ha pasado el incidente.

Un buen objetivo cuando se redactan las políticas, es que ellas deberían durar varios años, por ejemplo cinco años. En realidad, se harán modificaciones más a menudo, pero para evitar que se vuelvan obsoletas rápidamente, deben elaborarse para que sean independientes de productos comerciales específicos, estructuras organizativas específicas, así como las leyes específicas y regulaciones.

Las cosas se mueven muy rápidamente en el campo de la tecnología, incluyendo la seguridad informática. Por ejemplo, hace apenas algunos años la mayoría de las organizaciones no creían que era necesaria una política de seguridad para Internet, pero hoy en día es muy importante.

Las políticas deben revisarse en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables. Este esfuerzo también ayudará a mejorar la credibilidad de las actividades de seguridad informática dentro de la organización. Los empleados apreciarán que el personal de seguridad informática no está allí para crear más burocracia, sino para realmente ocuparse de las medidas de seguridad requeridas para proteger los recursos.

Con lo anterior, el presente documento pretende ser una guía o manual para establecer las políticas de seguridad informática dentro de una Red de Área Local (LAN).

Tomando como base que en toda Institución donde se cuente con una LAN, se maneja información que es importante o confidencial y debido a la importancia de la misma esta debe estar protegida. Esta protección se puede dar desde programas de software, así como desde dispositivos de hardware. En el contenido de este documento se explicara como implementar Políticas de Seguridad a través de la administración del Sistema Operativo (SO) Windows NT Server, así como de la implementación de herramientas de seguridad que nos ayuden a restringir el acceso a nuestra LAN.

Definiremos a una política de seguridad de la siguiente forma:

Una POLITICA DE SEGURIDAD INFORMÁTICA es un conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad y disponibilidad, tanto de forma accidental como intencionada.

Como se puede notar en la definición toda información debe de mantener estas tres propiedades para que los usuarios puedan hacer uso de ella de una forma segura, estas propiedades son:

Confidencial: La información sólo puede ser accedida por los usuarios que tengan los derechos necesarios para poder consultarla. Ya que en caso de que esto no se cumpla, la información puede ser manipulada y con esto el uso de la misma ya no tendrá el valor esperado.

Integra: Toda información debe ser presentada a los usuarios autorizados tal como fue procesada por las aplicaciones (base de datos), ya que si la información pierde esta propiedad, los usuarios estarán consultando o utilizando información errónea.

Disponible: En toda Institución se trabaja porque la información tenga un 100% de disponibilidad, esto es una premisa dentro de las Instituciones y si no llega a cumplirse, traerá como consecuencia que los usuarios no puedan realizar sus labores de una forma eficiente.

OBJETIVO GENERAL

Tener una guía para la implementación de políticas de seguridad para una LAN, tomando como base operacional el sistema operativo Windows NT Server. Teniendo como objetivo general la protección de los recursos y la información con que se cuenta en la LAN, a través de procedimientos, normas y lineamientos de operación basados en una política de seguridad, así como las herramientas con las que cuenta WNT para la protección de información y también haciendo uso de software o aplicaciones externas que ayuden a la protección de la información que circula dentro de la LAN. Todo esto con el fin de definir los límites entre lo que está permitido a los usuarios dentro de una empresa, así como la protección de las operaciones ilegales que traten de llevarse acabo dentro o fuera de la LAN.

OBJETIVOS ESPECIFICOS

- Para empezar a definir los objetivos específicos, se tomara como base que en la actualidad el arma más importante para toda empresa es la información con la que cuenta, ya que con el buen uso de esta va a sobresalir en el mercado en el que compite. Es por esto que es de suma importancia que la mantenga segura ante los posibles ataques internos o externos a los que esta expuesta. Y las empresas no deben escatimar en costos para mantenerla lo más segura que se pueda.

- Como primer objetivo se tratara de dar a entender la importancia de las Políticas de Seguridad, ya que las posibles amenazas y riesgos están muy latentes en la actualidad. Para evitar este tipo de riesgos o amenazas se dará una explicación del porque es importante asegurar las aplicaciones, la selección de productos de seguridad, entre otras.

- Otro de los objetivos será el de dar una guía de como crear Políticas de Seguridad efectivas, así como un ejemplo que podrá servir como base para la implementación de las mismas en las empresas.

- Dar una explicación más amplia de la forma de implementar Políticas de Seguridad, con el uso del Sistema Operativo Windows NT Server, a través de la administración de usuarios, perfiles y herramientas de seguridad.

- Explicar las diferentes herramientas de seguridad con los que se cuenta en la actualidad para proteger nuestra LAN de los hackers o crackers, así como de los virus que en la actualidad son cada días más poderosos para poder infiltrarse en los Sistemas de Cómputo. Entre las herramientas se explicara el uso de Firewall, Proxy, entre otros.

- Por último se mostrara un modelo de red segura, con el fin de que sirva como base para la implementación dentro de las empresas. Este modelo se implementa desde la protección que vamos a tener de las conexiones de Internet hasta las forma en que los usuarios deben definir sus contraseñas.

POLITICAS DE SEGURIDAD PARA UNA RED LOCAL

Importancia de políticas de Seguridad

a) Aseguran la aplicación correcta de las medidas de seguridad

Con la ilusión de resolver los problemas de seguridad, en muchas organizaciones simplemente se compran uno o más productos de seguridad, en estos casos, a menudo se piensa que nuevos productos (ya sea en hardware, software, o servicios), es todo lo que se necesita. Luego que se instalan los productos, se genera una gran desilusión al darse cuenta que los resultados esperados no se han materializado. En un número grande de casos, esta situación puede atribuirse al hecho de que no se ha creado una infraestructura organizativa adecuada para la seguridad informática.

Un ejemplo puede ayudar a aclarar este punto esencial. Supóngase que una organización ha adquirido recientemente un producto de control de acceso para una red de computadoras. La sola instalación del sistema hará poco para mejorar la seguridad. Sea debe primero decidir cuáles usuarios deben tener acceso a qué recursos de información, preferiblemente definiendo cómo incorporar estos criterios en las políticas de seguridad. También deben establecerse los procedimientos para que el personal técnico implante el control de acceso de una manera acorde con estas decisiones. Además debe definir la manera de revisar las bitácoras (logs) y otros registros generados por el sistema. Éstas y otras medidas constituyen parte de la infraestructura organizativa necesaria para que los productos y servicios de seguridad sean efectivos.

Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad.

Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada, es decir, son los aspectos esenciales desde donde se derivan los demás.

Continuando con el mismo ejemplo anterior de control de acceso, se debería primero llevar a cabo un análisis de riesgo de los sistemas de información. Esta evaluación de los riesgos también ayudará a definir la naturaleza de las amenazas a los distintos recursos, así como las contramedidas pertinentes. Luego pueden establecerse las políticas a fin de tener una guía para la aplicación de tales medidas.

b) Guían el proceso de selección e implantación de los productos de seguridad

La mayoría de las organizaciones no tiene los recursos para diseñar e implantar medidas de control desde cero. Por tal razón a menudo escogen soluciones proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la organización.

Esto se realiza a menudo sin conocer o entender suficientemente los objetivos y las metas de seguridad. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización.
Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere. De manera que tales políticas pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando los sistemas de seguridad.

c) Demuestran el apoyo de la Presidencia y de la Junta Directiva

La mayoría de las personas no está consciente de la gravedad de los riesgos relativos a la seguridad y por eso no se toma el tiempo para analizar estos riesgos a fondo. Además, como no tiene la experiencia suficiente, no es capaz de evaluar la necesidad de ciertas medidas de seguridad. Las políticas son una manera clara y definitiva para que la alta gerencia pueda mostrar que:

1. La seguridad de los activos de información es importante
2. El personal debe prestar la atención debida a la seguridad.

Las políticas pueden entonces propiciar las condiciones para proteger los activos de información. Un ejemplo muy frecuente involucra a los gerentes a nivel medio que se resisten a asignar dinero para la seguridad en sus presupuestos, pero si las políticas han sido emitidas por la Junta Directiva o la alta gerencia, entonces los gerentes a nivel medio no podrán continuar ignorando las medidas de seguridad.

d) Para lograr una mejor seguridad

Uno de los problemas más importantes en el campo de seguridad informática lo representan los esfuerzos fragmentados e incoherentes. A menudo un departamento estará a favor de las medidas de seguridad, mientras que otro dentro de la misma organización se opondrá o será indiferente. Si ambos departamentos comparten recursos informáticos (por ejemplo una LAN o un servidor), el departamento que se opone pondrá en riesgo la seguridad del otro departamento y de la organización completa. Aunque no es ni factible ni deseable que todas las personas en una organización se familiaricen con las complejidades de la seguridad informática, es importante que todas ellas se comprometan con mantener algún nivel mínimo de protección. Las políticas pueden usarse para definir el nivel de esta protección mínima, a veces llamada línea de base.

Elaboración de Políticas de Seguridad

a) Recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las necesidades de seguridad actuales de la organización, antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención. Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de la organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

c) Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos para redactar las políticas, para lo cual pueden servir de ayuda el ejemplo que se encuentra más adelante.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporciona mucho más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Este comité debería tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar las políticas según su viabilidad, análisis costo/beneficio y sus implicaciones. Las preguntas que debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables? ¿Son estas políticas claras e inequívocas?

Es muy importante que la Junta Directiva apruebe las políticas, en el caso frecuente que ciertos empleados objeten o piensen que ellos no necesitan obedecer.

Además es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

La aplicación de nuevas políticas es a menudo más eficaz si los empleados han sido informados de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.

Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Allí, por ejemplo, se explicaría que la información interna es la propiedad de organización, y que no puede ser copiada, modificada, anulada o usada para otros propósitos sin la aprobación de la gerencia.

Longitud del documento sobre las políticas

Las políticas de seguridad deben diseñarse de acuerdo a las necesidades específicas en una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas.

El personal de seguridad puede opinar que es necesario que todo esté absolutamente claro y explícito sobre los asuntos de seguridad informática. En estos casos puede que se requiere un conjunto de políticas. Otros serán renuentes a tener tantas políticas, prefiriendo enfatizar la confianza en buen juicio y buen comportamiento de los empleados.

Aunque un documento conciso será leído y asimilado con más probabilidad, hay mucho a favor de un conjunto completo y extenso de políticas de seguridad. Un principio general es que se deben promulgar sólo aquellas políticas que sean absolutamente necesarias. Esto es debido a que las personas son inherentemente muy diferentes entre sí, como también son diferentes los grupos a que pertenecen. El imponer un único conjunto de reglas para todos puede llevar a resistencia y a pobres resultados. En cambio, al tener sólo aquellas políticas que son estrictamente necesarias, se favorece la iniciativa personal y la creatividad. Además tantas políticas de seguridad van a impedir que el trabajo se haga a tiempo.

En todo caso, en vez de emprender un trabajo a fondo, es mejor empezar primero ocupándose de los aspectos esenciales, para luego ir ampliando con políticas adicionales. Este procedimiento toma a menudo la forma de declaraciones separadas donde se tratan las áreas problemáticas, por ejemplo PCs, LANs e Internet. De esta manera es también más fácil conseguir la aprobación de la alta gerencia así como de los propios empleados. Por otro lado las políticas nunca pueden tomar en cuenta todas las circunstancias y un conjunto extenso y minucioso de políticas puede generar críticas, disgusto y rechazo.

La extensión y el grado de detalle de las políticas es una función de tipo de audiencia y puede haber distintos documentos según el caso. Por ejemplo, podría haber documentos para los usuarios, la gerencia y el personal de informática. Muchas de las políticas en cada uno de estos documentos serían iguales, aunque el grado de detalle, las palabras técnicas utilizadas, y el número de ejemplos puede variar de un documento a otro. Para los usuarios finales, el documento debe limitarse a unas cuantas páginas. Para la gerencia habrá consideraciones adicionales, tal como los aspectos legales, y es probable que esto extienda el documento. Para el personal técnico será todavía más largo y más detallado.

Otro factor que afecta es el grado de seguridad requerido en la organización. En general, cuánto mayor es el uso de la información para las actividades de una organización, mayor es la necesidad de seguridad. Por ejemplo, un banco tendrá muchas y extensas políticas, mientras que una cadena de tiendas por departamentos tendrá menos políticas. Por supuesto que actividades especialmente delicadas, tal como salud y defensa, requieren de políticas muy detalladas.

Adicionalmente al número de políticas, hay que plantearse cuán larga debe ser la definición de cada política. Las definiciones concisas, de unas cuantas frases, son más aceptadas por los empleados ya que son más fácilmente leídas y entendidas. En todo caso deben ser suficientemente específicas para ser entendidas e interpretadas sin error, pero no deben ser tan específicas que impidan adaptarlas a las condiciones particulares de un sitio o departamento. Por ejemplo, se puede promulgar una política la cual especifica que todos los usuarios deben usar contraseñas difíciles de adivinar. Esta política da la flexibilidad a un gerente local para determinar su longitud mínima o un sistema automático que cheque si realmente una contraseña es difícil de adivinar.

Para ayudar a aclarar qué son las políticas, se pueden incluir ejemplos específicos. Como ilustración, una política que prohíbe el uso de los recursos computacionales para fines personales podría incluir ejemplos sobre Internet Chat Relay (IRC) o juegos por computadora.

Si se opta por elaborar un conjunto muy completo de políticas de seguridad, se aconseja hacerlo en dos etapas. El primer paso involucra el obtener la aprobación de la Junta Directiva para un conjunto genérico de políticas, mientras que el segundo paso involucra la aprobación para un conjunto más específico de políticas. El conjunto genérico podría incluir de 10 a 20 políticas, y el juego específico podría incluir otras 50-100.

De hecho, si el conjunto inicial de políticas es demasiado largo o severo, la Junta Directiva puede rechazarlo. Así que se aconseja elaborar un primer conjunto de políticas corto y relativamente fácil de cumplir por parte del personal.

Después, cuando haya sido implantado y asimilado a lo largo de la organización, se puede preparar una lista más completa y más estricta. Es mucho mejor proceder de forma relativamente lenta, con una serie pasos en el desarrollo de políticas, y así lograr credibilidad y apoyo, que preparar de una vez un solo documento extenso con todas las políticas, el cual se rechaza porque fue percibido como excesivamente severo.

Ejemplos de Políticas de Seguridad

1. Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia.

Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas gerencias de la Compañía están en el deber y en la responsabilidad de dedicar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva que muestre el estado actual de la Compañía en cuanto a seguridad informática y los progresos que se han logrado.

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe señalarse claramente que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

2. Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Compañía:

El Comité de Seguridad Informática está compuesto por los representantes de los distintos departamentos de la Compañía, así como por el Gerente de Informática, el Gerente de Telecomunicaciones, y el abogado o representante legal de la Compañía.

Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra. El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

No divulgar información confidencial de la Compañía a personas no autorizadas.

No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.

No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.

Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

Reportar inmediatamente a su jefe inmediato o a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

3. Políticas de seguridad para computadoras

Las computadoras de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática

No se permite fumar, comer o beber mientras se está usando un PC.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

Cualquier falla en las computadoras o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

Si una PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

4. Políticas de seguridad para las comunicaciones

Propiedad de la información

Con el fin de mejorar la productividad, la Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax.

Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación

Los sistemas de comunicación de la Compañía generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Compañía.

Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad

Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifradas. Para tal fin debe utilizarse Outlook, Outlook Express u otros productos previamente aprobados por la Gerencia de Informática.

Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

Es política de la Compañía no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

De manera consistente con prácticas generalmente aceptadas, la Compañía procesa datos estadísticos sobre el uso de los sistemas de comunicación.

Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

5. Políticas de seguridad para redes

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

Aspectos generales

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en la central telefónica, en los servidores y equipos de red de la Compañía, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia.
Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios

Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una nueva cuenta o el cambio de privilegios debe solicitarse por escrito y debe ser debidamente aprobada.

No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo. Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas o tarjetas inteligentes.

Se prohíbe el uso de cuentas anónimas o de invitado (guess) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas y el control de acceso

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas o tarjetas inteligentes.

Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causa de despido.

Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Los archivos de bitácora (logs) y los registros de auditoria que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

Los servidores de red y los equipos de comunicación, deben estar ubicados en locales apropiados, protegidos contra daños y robo.
Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

WINDOWS NT

Windows NT es un sistema operativo de red multiusuario, por eso es necesario realizar lo que se llama una administración de usuarios. En ella, el Administrador del sistema definirá las autorizaciones para acceder al Dominio y a los recursos. Además sirve para que cada usuario pueda tener un entorno de trabajo personalizado.

ADMINISTRACIÓN DE GRUPOS

Un grupo es un conjunto de cuentas de usuario. La asignación de una cuenta de usuario a un grupo concede a éste todos los derechos y permisos concedidos al grupo. Los grupos simplifican la administración al proporcionar un método fácil para conceder derechos comunes a múltiples usuarios simultáneamente.

La administración de grupos se realiza con la herramienta administrativa: *Administrador de Usuarios para Dominios* (o *Administrador de Usuarios*, si se trata de Windows NT Workstation o de un Servidor Independiente). Microsoft distingue entre dos tipos de grupos: locales y globales.

Grupos Locales

Los grupos locales se utilizan para conceder a los usuarios permisos de acceso a un recurso de la red. Recordemos que los permisos son normas que regulan qué usuarios pueden emplear un recurso como, por ejemplo, una carpeta, un archivo o una impresora.

Los grupos locales también se utilizan para proporcionar a los usuarios los derechos para realizar tareas del sistema tales como el cambio de hora de un equipo o la copia de seguridad y la restauración de archivos.

Windows NT incluye varios grupos locales ya creados, diseñados especialmente para asignar derechos a los usuarios. Los grupos incorporados con Windows NT son grupos "predefinidos" que tienen un conjunto predeterminado de derechos de usuario.

Grupos Globales

Los grupos globales se utilizan para organizar cuentas de usuario del dominio, normalmente por función o ubicación geográfica. Se suelen usar, en redes con múltiples dominios.

Cuando los usuarios de un dominio necesitan tener acceso a los recursos existentes en otro dominio, se agregarán a un grupo local del otro dominio para conceder derechos a sus miembros. Se tienen que crear en un controlador del dominio en el que residen las cuentas de los usuarios.

RESUMEN DE LAS CARACTERÍSTICAS DE LOS GRUPOS LOCALES Y GLOBALES	
Grupos locales	**Grupos globales**
Proporcionan a los usuarios permisos o derechos.	Organizan los usuarios del dominio.
Pueden incluir (de cualquier dominio): –Cuentas de usuario – Grupos globales	Sólo pueden incluir cuentas de usuario del dominio en el que residen.
No pueden incluir ningún otro local.	No pueden contener ningún grupo local ni global.
Tienen asignados permisos y derechos en el dominio local.	Se agregan a un grupo local para conceder derechos y permisos a sus miembros.
En Windows NT Workstation o en servidores miembro, sólo se pueden asignar derechos y permisos a recursos locales.	No se asignan a recursos locales.
En un PDC, pueden tener asignados recursos de cualquier controlador del dominio.	Es necesario crearlos en el PDC del dominio donde residen las cuentas.

Diseño de una estrategia de Grupos

Para crear grupos, es recomendable seguir las siguientes directrices:

- Organizar los usuarios del dominio según sus necesidades comunes. Por ejemplo, si el personal de ventas necesita tener acceso a una impresora en color y todos los directores necesitan acceder a un archivo de registros de empleados, organice los usuarios por personal de ventas y por directores.

- En todos los dominios en los que residan cuentas de usuario, crear un grupo global para cada grupo lógico de usuarios. A continuación, agregar las cuentas de usuario adecuadas a los grupos globales correspondientes.

- Crear grupos locales tomando como base sus necesidades de acceso a recursos. Por ejemplo, si los Comerciales necesitan tener acceso al directorio ListaPrecios (sólo para consultar precios) y el Director necesita control total sobre los archivos de dicho directorio, crearemos un grupo local para los Comerciales y otro para el Director (o Directores).

- Asignar los permisos apropiados a los grupos locales.

- Agregar los grupos globales a los grupos locales.

Para agregar grupos globales de un dominio a grupos locales de otro dominio, es imprescindible que se haya establecido la relación de confianza apropiada.

Implementación de Grupos Incorporados

Los grupos incorporados son grupos predefinidos que tienen un conjunto predeterminado de derechos de usuario. Recordemos que los derechos de usuario determinan las tareas del sistema que puede realizar un usuario o un miembro de un grupo. Los equipos que ejecutan Windows NT tienen tres tipos de grupos incorporados:

Los grupos locales incorporados ofrecen a los usuarios derechos para realizar tareas del sistema como la copia de seguridad y la restauración de archivos, el cambio de la hora del sistema y la administración de los recursos del sistema. Los grupos locales incorporados se encuentran en todos los equipos que ejecutan Windows NT.

Los grupos globales incorporados ofrecen a los administradores una forma sencilla de controlar todos los usuarios de un dominio, se encuentran solamente en los controladores de dominio. Los grupos del sistema organizan automáticamente a los usuarios para uso del sistema. Los administradores no asignan usuarios a dichos grupos. En su lugar, los usuarios son miembros de forma predeterminada o se convierten en miembros durante la actividad de la red.

Los grupos del sistema se encuentran en todos los equipos que ejecutan Windows NT.

Los grupos incorporados no pueden eliminarse ni cambiarse.

Grupos incorporados en todos los equipos NT

Grupos locales incorporados que residen en todos los equipos que ejecutan Windows NT:

Usuarios: permite realizar tareas para las que han recibido derechos y tener acceso a los recursos para los que tienen permisos. Se suele utilizar para dar permisos generales a todos los usuarios de nuestro sistema.

Administradores: Los administradores poseen la mayoría de los derechos sobre nuestra máquina (Dominio local). Pueden realizar todas las tareas administrativas en el equipo local. La cuenta Administrador no se debe borrar (puesto que tiene privilegios que cualquier otro usuario del grupo Administradores no consigue tener) y resulta conveniente, por motivos de seguridad cambiarle el nombre y crearse una segunda cuenta de administrador. Los derechos del Administrador vienen restringidos a un solo dominio (en el que se creó), por lo que si se quiere que un solo administrador administre varios dominios, debe incorporar a éste al grupo de Administradores de los demás dominios.
A pesar de que se puede tener tantos administradores como deseemos, no es recomendable que sean muchos puesto que con ello ponemos en peligro la seguridad del sistema, ya que a mayor número de administradores, mayor posibilidad de que se descubra la contraseña de alguno de ellos.

Invitados: permite realizar tareas para las que se les hayan concedido derechos y tener acceso a recursos para los que tengan permiso. Un miembro de este grupo es la cuenta de usuario Invitado, que se suele utilizar para dar acceso a la red a usuarios eventuales a los cuales no queremos asignar una cuenta de usuario. Es recomendable eliminar (o, en su defecto, proteger con contraseña) al usuario invitado como medida de seguridad, evitando así la posibilidad de encontrarnos con alguna conexión sin identificar.

Operadores de Copia: permite usar el programa de "copias de seguridad" de Windows NT, para realizar copias de seguridad.

Duplicadores: Los equipos que ejecutan Windows NT Server pueden sincronizar algunas carpetas (como por ejemplo las de los Script) con otros servidores. Uno de ellos se comporta como el exportador (el que tiene la copia maestra de los archivos) y los otros importan esos datos. De esta manera, podemos tener carpetas en diferentes servidores con el mismo contenido, lo que nos puede servir como medida de seguridad para proteger ciertos archivos críticos. El grupo Duplicadores nos permite utilizar el servicio de "Duplicador de Directorios", que es el que permite que se realice la duplicación.

Usuarios Avanzados: sólo reside en servidores miembro y Windows NT Workstation. Los miembros de este grupo pueden crear y modificar cuentas, así como compartir recursos.

Grupos incorporados sólo en controladores de Dominio

Grupos locales incorporados sólo en controladores de dominio:

Operadores de Cuentas: pueden crear, eliminar y modificar usuarios, grupos globales y grupos locales. No pueden modificar los grupos Administradores ni Operadores de Servidores. No hay miembros iniciales en este grupo.

Operadores de Servidores: pueden compartir los recursos del disco y realizar copias de seguridad. No hay miembros iniciales en este grupo.

Operadores de impresión: pueden configurar y administrar las impresoras de red. No hay miembros iniciales en este grupo.

Grupos globales incorporados sólo en controladores de dominio

Cuando se instala un Windows NT Server como controlador de dominio, se crean tres grupos globales en la base de datos de directorio del dominio:

Usuarios del Dominio: usuarios que tienen acceso al dominio. Se agrega al grupo local de "Usuarios". Cuando se crea una cuenta de usuario del dominio, éste se convierte automáticamente en miembro de este grupo. El Administrador es miembro por defecto.

Administradores del Domino: usuarios que tienen derechos de administración en el dominio. Se agrega al grupo local de "Administradores" para así poder realizar tareas administrativas en el equipo local. El Administrador es miembro por defecto.

Invitados del Dominio: permite realizar tareas para las que se hayan concedido derechos y tener acceso a recursos para los que tengan permiso del dominio. Se agrega al grupo local de "Invitados". Un miembro es el usuario Invitado.

Grupos incorporados del Sistema

Además de los grupos incorporados locales y globales existe un tercer tipo de grupos, llamados Grupos del Sistema que organizan automáticamente a los usuarios para uso del sistema. Los administradores no asignan usuarios o dichos grupos. En su lugar, los usuarios son miembros de forma predeterminada o se convierten en miembros durante la actividad de la red (no se puede modificar la relación de miembro de dichos grupos). Los grupos del sistema se encuentran en cualquier equipo que ejecute Windows NT.

Grupos del sistema que se utilizan para la administración de la red

Todos (Everyone): Contiene todos los usuarios locales y remotos que tienen acceso al equipo.

Creator Owner: Incluye al usuario que creó o tomó posesión de un recurso.

Grupos del sistema que no se utilizan para la administración de la red

Network: Incluye a cualquier usuario que esté actualmente conectado desde otro equipo de la red a un recurso compartido.

Interactive: Incluye automáticamente al usuario que inicia localmente una sesión en el equipo. Los miembros interactivos tienen acceso a los recursos de su equipo.

ADMINISTRACIÓN Y PERFILES DE USUARIO

Cuentas de Usuario

Se trata de las credenciales únicas de un usuario en un dominio, ofreciéndole la posibilidad de iniciar sesión en el Dominio para tener acceso a los recursos de la red o de iniciar la sesión local en un equipo para tener acceso a los recursos locales. Cada persona que utilice la red regularmente debe tener una cuenta.

Las cuentas de usuario se utilizan para controlar cómo un usuario tiene acceso al Dominio o a un equipo. Por ejemplo, puede limitar el número de horas en as que un usuario puede iniciar una sesión en el dominio, impresoras de red que pueden utilizar, etc.

Es decir, gracias a las cuentas de usuario el Administrador puede controlar todo lo que un usuario puede hacer en un dominio, a través de las restricciones de su cuenta y la configuración de derechos de usuario.

Tipos de cuentas de usuario

Existen dos tipos de cuentas de usuario:

Cuentas creadas por nosotros como administradores del dominio: Estas cuentas contienen información acerca del usuario, incluyendo el nombre y la contraseña del usuario, permiten que el usuario inicie una sesión en la red y, con los permisos apropiados, tenga acceso a los recursos de la red.

Cuentas predefinidas o incorporadas: Se trata de cuentas creadas durante la instalación de Windows NT. Estas cuentas son:

Invitado (Guess): La cuenta incorporada Invitado se utiliza para ofrecer a los usuarios ocasionales la posibilidad de iniciar sesiones y tener acceso a los recursos del dominio o equipo local. Por ejemplo, un empleado que necesite tener acceso al equipo durante un periodo breve de tiempo. La cuenta Invitado está deshabilitada de forma predeterminada. No se debe habilitar esta cuenta en una red de alta seguridad. Para mayor seguridad, cambie el nombre de esta cuenta y asígnele una contraseña.

Administrador (Administrator): La cuenta incorporada Administrador se utiliza para administrar la configuración global del equipo y del dominio. El Administrador puede realizar todas las tareas, como la creación o modificación de cuentas de usuario y de grupo, la administración de las directivas de seguridad, la creación de impresoras, y la asignación de permisos y derechos a las cuentas de usuario para que tengan acceso a los recursos.

Otras cuentas: Dependiendo de las aplicaciones instaladas pueden aparecer más cuentas predefinidas.

Para conseguir un mayor grado de seguridad, cree una cuenta de usuario normal que pueda utilizar para realizar las tareas no administrativas, cambie el nombre de la cuenta Administrador y sólo inicie una sesión como Administrador para realizar tareas administrativas.

Diseño de Cuentas de usuario

Para diseñar cuentas de usuario lo primero que tendremos que tener en cuenta es establecer una convención de nombres.

La convención de nombres establece cómo se identificará a los usuarios en la red. Una convención de nombres coherente hará que el administrador y los usuarios puedan recordar más fácilmente los nombres de los usuarios y encontrarlos en listas. Para determinar una convención de nombres, tendremos en cuenta lo siguiente:

1.- Los nombres de usuario deben ser únicos. Si existe un gran número de usuarios, el diseño debe contar con la posibilidad de empleados con nombres duplicados, habrá que determinar un criterio a seguir para no asignar el mismo nombre de cuenta a dichos usuarios. Por ejemplo: José Fernández, JoseF y JoseFdz.

2.- Los nombres de usuario pueden contener cualquier carácter en mayúsculas o minúsculas excepto los siguientes caracteres: " / \ [ ] : ; =, + * ? < >. Podemos utilizar una combinación de caracteres especiales y alfanuméricos en la convención de nombres de usuario para facilitar la identificación de los usuarios.

Administración de cuentas

Existen procedimientos y herramientas que un administrador puede utilizar para realizar sus tareas diarias de forma eficiente y mantener la red en perfecto funcionamiento. Estos son algunos de esos procedimientos y herramientas:

- Crear plantillas para agregar nuevas cuentas de usuario.
- Realizar cambios simultáneamente en varias cuentas de usuario.
- Diseñar e implementar un plan de cuentas para proteger la red.
- Mantener los controladores de dominio de forma que las cuentas de usuario se puedan validar siempre y sin problemas.
- Solucionar los problemas que puedan tener los usuarios con sus cuentas, suelen ser problemas de inicio de sesión.
- Distribuir algunas de las tareas administrativas mediante la creación de un Administrador adicional o un Operador de cuentas:

- Los miembros del grupo Administradores tienen todas las capacidades administrativas. Son responsables del diseño y el mantenimiento de la seguridad de la red.

- Los miembros del grupo Operadores de cuentas pueden crear, eliminar y modificar cuentas de usuario, grupos globales y grupos locales. No obstante, no pueden modificar los grupos Administradores y Operadores de servidores.

Administración del entorno de trabajo de un usuario

Como administradores podemos definir el entorno de trabajo de un usuario para restringir o personalizar lo que un usuario ve y tiene disponible cuando inicia una sesión. Por ejemplo, podemos establecer los colores de la pantalla, la configuración del ratón, y que las conexiones de red y de impresoras sean siempre las mismas cuando un usuario inicie una sesión. Para administrar los entornos de trabajo de los usuarios se utilizan las siguientes herramientas:

Perfiles de usuario

Contienen todas las configuraciones definibles por el usuario para el entorno de trabajo de un equipo que ejecute Windows NT, incluyendo la configuración de la pantalla y las conexiones de red. Los perfiles de usuario ofrecen las siguientes posibilidades:

- Personalizar el entorno de trabajo de un usuario de forma que éste vea siempre el mismo entorno de trabajo cuando inicie una sesión desde cualquier equipo que ejecute Windows NT.
- Ofrecer a los usuarios que comparten un mismo equipo sus propios perfiles de usuario.
- Ofrecer a todos los usuarios el mismo perfil de usuario y evitar que los usuarios lo modifiquen.
- Ofrecer a todos los usuarios el mismo perfil de usuario inicial, pero permitir que los usuarios lo modifiquen.

Archivo de comandos de inicio de sesión

Se trata de un archivo de proceso por lotes (.bat o .cmd) o un archivo ejecutable (.exe) que se ejecuta automáticamente cuando un usuario inicia una sesión en cualquier tipo de estación de trabajo de la red. El archivo de comandos puede contener comandos del sistema operativo, como los comandos para establecer conexiones de red o Iniciar aplicaciones.

Los archivos de comandos de inicio de sesión son los precursores de los perfiles de usuario y proporcionan compatibilidad con versiones anteriores de clientes LAN Manager; no se pueden utilizar para configurar la pantalla.

Perfiles de usuario móviles

Se puede especificar un perfil de usuario móvil para una cuenta de usuario. Los perfiles de usuario móviles proporcionan al usuario el mismo entorno de trabajo, sin importar el equipo con Windows NT en el que el usuario inicie la sesión.

Perfil de usuario móvil obligatorio: es un perfil de usuario preconfigurado que él no puede cambiar. Un perfil obligatorio puede asignarse a varios usuarios. Esto significa que modificando un perfil, el administrador puede cambiar varios entornos de escritorio. Este tipo de perfil se utiliza para proporcionar configuraciones comunes a los usuarios. Por ejemplo, cuando tiene varios usuarios que requieren una configuración idéntica del escritorio para hacer entradas de pedidos.

Perfil de usuario móvil personal: es un perfil de usuario que un usuario puede cambiar; esto significa que cuando el usuario termina la sesión, el perfil de usuario se actualiza para incluir los cambios efectuados por el usuario. Cuando el mismo usuario vuelve a iniciar una sesión, el perfil se carga como se guardó por última vez.

Derechos

Determinan las tareas del sistema que puede realizar un usuario o un miembro de un grupo con el sistema operativo Windows NT. Por ejemplo: iniciar sesión en local, acceder al equipo a través de la red....

Permisos

Son normas que regulan qué usuarios pueden utilizar un determinado recurso compartido del sistema, esto incluye archivos, carpetas, impresoras...

HERRAMIENTAS DE SEGURIDAD

Copia de Seguridad

El programa "Copia de seguridad" de Microsoft Windows NT es una herramienta gráfica que podemos usar para efectuar una copia de seguridad de los datos en cinta. Podemos copiar y restaurar archivos importantes de los volúmenes NTFS o FAT, además de realizar copias de seguridad manualmente o programar una copia de seguridad desatendida.

Los requisitos del programa "Copia de seguridad" de Windows NT son:

- Sólo admite la copia en cintas. Es necesario, por tanto, un dispositivo de unidad de cinta incluida en la lista de configuración de hardware y cintas de copia de seguridad.

- El usuario debe contar con los derechos de usuario apropiado:
  - Todos los usuarios pueden realizar una copia de seguridad de cualquier archivo y carpeta para los que tengan permiso Lectura.
  - Para copiar archivos y carpetas con el programa "Copia de seguridad" de Windows NT, un usuario debe tener el derecho de Copia de seguridad de archivos y directorios. Los miembros de los grupos Operadores de copia, Operadores de servidores y Administradores tienen este derecho.
  - Para restaurar los archivos y carpetas, el usuario debe tener el derecho Restaurar archivos y carpetas. Los miembros de los grupos Operadores de copia, Operadores de servidores y Administradores tienen este derecho.

Diseño de una estrategia de copias de seguridad

Antes de comenzar a copiar los datos, necesitamos desarrollar una estrategia de copia de seguridad que satisfaga las necesidades de la red y garantice la recuperación de datos perdidos. No existe una estrategia correcta o incorrecta, sólo la que sea apropiada para cada organización.

Consideraremos los siguientes aspectos:

Qué archivos vamos a copiar: Existe una regla de copia de seguridad general, si ya no va trabajar con un archivo, haga una copia de seguridad del mismo.

Si se va a realizar una copia de seguridad de red o múltiples copias de seguridad locales, esto depende de los equipos que utilice la organización para almacenar datos importantes.

Copia de seguridad de red: Haremos una copia de seguridad de red cuando los datos importantes se encuentren en varios servidores.

Ventajas:

- Requiere menos unidades de cinta.
- Hay menos medios que administrar.
- Un único usuario puede realizar la copia de seguridad.

Desventajas:

- Los usuarios deben copiar sus archivos importantes a los servidores.
- No se pueden copiar los registros remotos.
- Aumenta el tráfico de la red.
- Requiere más tiempo de diseño y preparación.

Copia de seguridad local: realizaremos varias copias de seguridad locales cuando los datos importantes se encuentren en equipos cliente.

Ventajas:

Se utilizan menos recursos de la red.

Desventajas:

Requiere más unidades de cinta y más cintas.

Los usuarios son responsables de realizar la copia de los datos de sus equipos, éstos pueden no ser fiables.

Copia de seguridad de red y local: Haremos copias de seguridad de red y locales cuando los datos importantes se encuentren en servidores y estaciones de trabajo. La frecuencia de realización de copias de seguridad depende de lo siguiente:

La importancia de los datos para la compañía. Los datos importantes se copian con más frecuencia.

La frecuencia con que cambian los datos. Si los usuarios crean o modifican informes solo los viernes, una copia de seguridad semanal de los archivos de informes sería suficiente.

Diseñe la realización de copias de seguridad cuando el uso de la red sea mínimo. Si hay archivos en uso, Windows NT sólo copia la última versión guardada del archivo.

Determinación de los archivos y carpetas que se van a copiar

Para determinar qué archivos y carpetas vamos a copiar seguiremos las siguientes directrices.

Realizar siempre una copia de seguridad de:

- Todos los archivos y carpetas importantes que se necesitan para la marcha de la organización.
- El registro del controlador de dominio. El registro contiene la base de datos de directorio donde se incluyen las cuentas de usuario y la información sobre la seguridad.
- Realizar periódicamente una copia de seguridad de los archivos que raramente cambian o que no son importantes para la organización.
- No realizar copias de seguridad de los archivos temporales puesto que cambian constantemente.

Tipos de copia de seguridad

El programa de "Copia de seguridad" de Windows NT proporciona cinco tipos de copia de seguridad, que también se conocen como métodos de copia de seguridad. Un plan efectivo de copia de seguridad podría combinar estos tipos.

Dependiendo del tipo de copia de que establezcamos puede establecer un indicador o marca de copia de seguridad, también conocido como atributo de archivado. Este indicador especifica que el archivo se ha copiado y afecta a las copias de seguridad progresiva y diferencial.

Los diferentes tipos de copia de seguridad son:

Normal: Hace una copia de los archivos y carpetas seleccionados, y marca sus atributos de archivado.

Copia: Hace una copia de los archivos y carpetas seleccionados, y no marca sus atributos de archivado.

Progresiva o incremental: Hace una copia de los archivos y carpetas seleccionados pero sólo de aquellos que hayan cambiando desde la última vez que se copiaron y se marcaron. Si marca sus atributos de archivado.

Diferencial: Hace una copia de los archivos y carpetas seleccionados pero sólo de aquellos que hayan cambiando desde la última vez que se copiaron y se marcaron. No marca sus atributos de archivado.

Copia diaria: Hace una copia sólo de los archivos y carpetas que hayan cambiado durante el día. No marca sus atributos de archivado.

Las políticas de copia de seguridad, en realidad, son una combinación de los diferentes tipos existentes, encaminadas bien a reducir el tiempo de realización del backup, bien a disminuir del tiempo de restauración de la copia de seguridad.

Conjuntos de copias, registro de copia y catálogos

Antes de realizar una copia de seguridad debemos conocer las diferencias entre conjuntos de copia de seguridad, registros de copia de seguridad y catálogos.

Conjunto de copia de seguridad: Un conjunto de copia de seguridad es un grupo de archivos o carpetas pertenecientes a un mismo volumen, resultante de una única operación de copia de seguridad. Una cinta puede contener varios conjuntos de copia de seguridad. Si una única operación de copia de seguridad requiere varias cintas, el grupo de cintas se denomina conjunto de familias.

Registro de copia de seguridad: Un registro de copia de seguridad registra las operaciones de copia de seguridad y almacena la información en un archivo de texto. El registro resulta útil a la hora de restaurar datos.

Hay tres opciones de registro:

- Detallar al máximo
- Sólo resumen
- No crear registro
    - Dependiendo de la opción de registro seleccionada, el registro puede contener la siguiente información:
        - Fecha de la copia de seguridad.
        - Archivos copiados
        - Equipos copiados
        - Número del conjunto de cintas

- Quién realizó la copia de seguridad
- Tipo de copia de seguridad
- Ubicación de la unidad de cintas

Catálogo: El catálogo es una representación gráfica de la copia de seguridad. Windows NT crea catálogos automáticamente durante el proceso de copia de seguridad y los almacena en la cinta.

Hay dos tipos de catálogos diferentes.

El catálogo de cintas muestra todos los conjuntos de copia de seguridad de una cinta.

El catálogo de conjuntos de copia de seguridad muestra todos los archivos y carpetas del conjunto de copia de seguridad.

Antes de restaurar los archivos, deberemos cargar los catálogos, A continuación, podremos seleccionar los conjuntos de copia de seguridad, archivos y carpetas que deseemos restaurar.

Restauración de Datos

Con el programa "Copia de seguridad" de Microsoft Windows NT puede restaurar archivos importantes en un volumen NTFS o FAT. Puede restaurar archivos localmente o a través de la red.

Los requisitos para restaurar datos mediante el programa "Copia de seguridad" de Windows NT son:

- El usuario debe tener el derecho de usuario apropiado, que es Restaurar archivos y directorios.
- Los miembros de los grupos Operadores de copia, Operadores de servidores y Administradores tienen este derecho a menos que se haya quitado.
- Puede conceder este derecho a un usuario o a un grupo.
- Los archivos que van a restaurarse se copiaron mediante "Copia de seguridad" de Windows NT o un programa de copia que admita el formato de cinta de Microsoft.

La opción Limitar el acceso al propietario y al administrador afecta sobre todo a quién puede restaurar los datos. Si se selecciona esta opción durante la copia de seguridad, sólo un administrador o el usuario que realizó la copia podrán restaurar los datos de la cinta.

Diseño de una estrategia para restaurar datos

Toda la documentación de la que disponga sobre una copia de seguridad en particular resulta muy útil. Con el programa "Copia de seguridad" de Windows NT puede disponer de la información siguiente:

- El registro de copia es un archivo de texto con información sobre la copia, La opción del registro se selecciona durante la copia de seguridad.
- Dependiendo del registro seleccionado, éste puede incluir información sobre el tipo de copia de seguridad, los archivos y carpetas que se han copiado y en qué cinta se encuentran.
- Debemos guardar copias impresas, en caso de que se dañe el archivo del registro de copia existente en el equipo, podremos utilizar el impreso.
- El catálogo proporciona una representación gráfica de la copia de seguridad. Windows NT genera automáticamente el catálogo y lo almacena en la cinta. Hay dos tipos de catálogos: El **catálogo de cintas** proporciona una lista de todos los conjuntos de copia y el tipo de copia de seguridad utilizado. El **catálogo de conjuntos de cinta** proporciona todos los archivos y carpetas del conjunto de copia. El catálogo permite seleccionar las unidades, los archivos y las carpetas que se desean restaurar.

Windows NT tiene internamente servicios propios del Sistema Operativo; aparte se pueden instalar otros en cualquier momento que se desee. Se deberían ejecutar tan pocos servicios como sea posible, para disminuir al máximo la posibilidad de accesos no autorizados por errores de configuración y "bugs" de los servicios.

Cortafuegos (Firewall)

Cuando se suministra a los usuarios de Internet acceso a los servicios de la red interna (LAN), hay que proteger los sistemas internos. Hay dos tipos de servicios de red disponibles en una computadora Windows NT:

- **SMB (Bloques de mensajes de servidor) de Microsoft que son servicios de archivos y red**. Estos servicios están instalados por defecto normalmente.
- **Servicios TCP/IP e Internet como servidores Web y FTP.** Se pueden instalar de modo opcional.

Cuando se conecta un sistema Windows a Internet existe el peligro potencial de los protocolos SMB. Si hay carpetas compartidas SMB en la red que conecta a Internet, potencialmente cualquiera de los usuarios de Internet puede acceder a las carpetas o secuestrar sesiones.

Además, hay problemas de seguridad intrínsecos a los protocolos. A continuación se describe como desactivar estos servicios apropiadamente:

¿Qué es un firewall?

Un FIREWALL es un sistema o grupo de sistemas que establece una política de control de acceso entre dos redes.

Tienen las siguientes propiedades

- Todo el trafico de adentro hacia fuera, y viceversa debe pasar a través de ella.
- Solo el tráfico autorizado, definido por la política de seguridad es autorizado para pasar por él.
- El sistema es realmente resistente a la penetración.

Filtrado de paquetes

Todos los firewalls desempeñan algún tipo de filtrado de paquete ip, comúnmente por medio de un ruteador de filtrado de paquetes. El ruteador filtra paquetes, haciendo que ellos pasan por el ruteador, implementando un conjunto de reglas con base en la política del firewall. Un ruteador filtrador de paquetes, usualmente puede filtrar paquetes ip con base en algunos o todos los criterios siguientes:

- dirección fuente ip,
- dirección destino ip,
- puerto fuente tcp/udp,y
- puerto destino tcp/udp.

El filtrado puede bloquear conexiones desde las redes o anfitriones específicos, y pueden bloquear conexiones a puertos específicos. Un sitio podría desear bloquear las conexiones desde ciertas direcciones tales como desde anfitriones, o los sitios que se consideren hostiles o indignos de confianza. Alternativamente, un sitio puede desear bloquear conexiones desde todos las direcciones externas al sitio (con ciertas excepciones, tales como con smtp para recibir e-mail).

Tipos de firewalls

Cuando se habla de Firewalls, uno debería tomar en cuenta que la tecnología evoluciona muy rápidamente. Los Firewalls de hoy tienden a combinar diferentes mecanismos, haciendo difícil clasificarlos. Por esa razón se describen los pasos que pueden ir en el diseño de un firewall. Estos son los firewalls más comunes:

Firewalls como filtros

El Router es un tipo especial de switch el cual realiza el trabajo de hacer las conexiones externas y convertir el protocolo IP a protocolos de WAN y LAN.

Los paquetes de datos transmitidos hacia Internet, desde un visualizador de una PC contenida dentro de una LAN, pasarán a través de numerosos ruteadores a lo largo del camino, cada uno de los cuales toma la decisión de hacia donde dirigir el trabajo.

Los ruteadores toman sus decisiones basándose en tablas de datos y reglas, por medio de filtros, así que, por ejemplo, solo datos de una cierta dirección pueden pasar a través del ruteador, esto transforma un ruteador que puede filtrar paquetes en un dispositivo de control de acceso o firewall. Si el ruteador puede generar un registro de accesos esto lo convierte en un valioso dispositivo de seguridad.

Si el servidor de Internet solicita información, o bien la suministra hacia sistemas de bases de datos distribuidas, entonces esta conexión entre el servidor y la estación de trabajo debería ser protegida.

Firewalls como gateway

Los firewalls son comúnmente referidos como gateways, controla el acceso desde afuera hacia adentro y viceversa de LAN o WAN.

Un gateway es una computadora que proporciona servicio de intercambio de datos entre dos redes, un firewall puede consistir en un poco mas que un ruteador filtrador, como un gateway controlada. El tráfico va hacia el gateway, en vez de dirigirse directamente hacia la red, el gateway pasa los datos de acuerdo a la política de control de los accesos, a través de un filtro, hacia otra red o hacia otro gateway conectada a otra red.

Esta mediación toma en una cuenta, direcciones de fuente y destino, tipos de paquetes de datos, política de seguridad. Típicamente un firewall registra los accesos y los intentos de acceso de una red a otra.

Firewalls como puntos de atrapado

Algunos firewalls proveen servicios de seguridad adicionales,como encriptación y descriptacion, ambas deben usar sistemas compatibles de encriptación. Existen varios fabricantes que ofrecen dichos sistemas. Encriptación de firewall a firewall es la forma que se usa en el Internet de hoy.

Verificar la autenticidad del usuario así como el sistema que este usando también es importante, y los firewalls pueden hacerlo, usando tarjetas inteligentes, fichas y otros métodos. Los firewalls, pueden incluso proteger otras redes exteriores. Una compañía puede aplicar las mismas restricciones de tráfico, mejorado con autenticación.

Firewalls internas

Alguien fuera de la empresa podría solicitar cierta información, pero no necesariamente necesita acceder a toda la información interna. En estas circunstancias los firewalls juegan un importante papel forzando políticas de control de acceso entre redes confiables protegidas y redes que no son confiables.

Separar las redes por medio de firewalls reduce significativamente los riesgos del ataque de un hacker desde adentro, esto es acceso no autorizado por usuarios autorizados. Agregando encriptación a los servicios del firewall se convierte en una conexión firewall a firewall muy segura.

Factores que no hacen deseable un firewall

INEFICIENTE: Normalmente la experiencia y conocimiento de los fabricantes de firewalls no se acerca siquiera a la tradición y conocimiento de los fabricantes tradicionales de enrutadores, por ello rara vez pueden cumplir el requisito anterior y lo que se consigue en la practica es un cuello de botella, así como enrutadores subutilizados debido a la situación anterior.

Este factor también nos conduce a que los costos para maquina de firewall que cumplan tales requisitos sean bastante altos ya que su volumen de producción (numero de unidades vendidas) no se acerca a la producción típica de los enrutadores correspondientes para ese nivel de procesamiento de paquetes por segundo.

NO TAN SEGURO: Los firewall son típicamente implementados en un sistema UNIX lo que los hace bastante vulnerables para los ataques de seguridad, ya que de tal sistema existe mayor conocimiento del público en general, y son bastante publicadas las posibles brechas de seguridad en ese sistema operativo, por ello es el blanco típico de ataque para los programas especializados de scanning de los hackers (estudian "pacientemente" múltiples opciones del sistema, hasta encontrar un punto de acceso o modificación).estos programas son en un 99% desarrollados para sistemas UNIX.

Si mi seguridad esta sustentada en una maquina cuyo núcleo está apoyada en el sistema UNIX (el cual es precisamente el más conocido por los enemigos de mi seguridad), entonces mi sistema no es realmente tan seguro.

Muchas veces no son transparentes a la operación del usuario: Debido a su diseño, algunos de estos modelos no son tan transparentes a la operación del sistema, complican la administración del sistema de comunicación (usualmente tienen interfaces de manejo propietarias). Algunos modelos basados en "proxies" pueden ser muy seguros, pero algunos de ellos requieren versiones modificadas de los aplicativos, llevandolos a ser poco deseables para montajes masivos.

Son inapropiados para montajes mixtos: Por su misma concepción el montaje solicitado por las compañías cuenta con dos niveles de VPNs (la Intranet corporativa y luego las Intranet de cada empresa), los cuales deben ser interrrelacionados de manera armoniosa para flujo de información y control de acceso. Este tipo de montaje seria bastante costoso, dificil de implementar y de administrar con dos niveles de firewalls.

Comprar o construir un firewall

Algunas organizaciones tienen la capacidad de colocar sus propios firewall, usando cualquiera de los equipos y componentes de software disponibles o escribiendo un firewall de raya. Al mismo tiempo, la totalidad de los vendedores ofrecen una amplia variedad de servicios en tecnología de firewall, desde proveer las herramientas necesarias hasta implementar pólizas de seguridad hasta cálculos fuera de riesgos, revistas de seguridad y entrenamiento de seguridad.

Una de las ventajas para una compañía al construir su propio firewall es que el personal de la misma entenderá las especificaciones del diseño y uso del firewall.

Tal conocimiento puede no existir para un vendedor - proveedor de firewall. Además, un firewall puede requerir una gran cantidad de tiempo para construirla, documentarla y mantenerla.

Un firewall puede ser tan efectiva como la administración que la hizo. Un mantenimiento pobre puede empezar a ser inseguro y permitir roturas mientras provee una ilusión de seguridad. La póliza de seguridad podría reflejar claramente la importancia de la administración de un firewall fuerte, y el manejo demostraría su importancia en términos de personal, fondos y otros recursos necesarios.

El contar con una firewall no es excusa para prestar menos atención a la administración de un sistema en el lugar, de hecho, si un firewall es penetrada, una administración pobre permitirá amplias intrusiones resultando dañada, también un firewall no reduce las necesidades de administrar un sistema altamente calificado al mismo tiempo.

Un problema encontrado por muchos compradores de firewall es que los vendedores, preparan literatura que ponen a sus productos en lo más alto posible y describen diseños y filosofías de ventas apropiadas para la compañía, sin embargo, los estándares han surgido en otras areas de hardware y software, ambos en tecnología y descripción de funciones.

Servidores proxy y su función

Un servidor proxy, algunas veces se hace referencia a el, con el nombre de "gateway" (puerta de comunicación) o "forwarder" (agente de transporte), es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los proxies se utilizan a menudo, como sustitutos de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes. Muchos proxies contienen logines auxiliares y soportan la autentificación de usuarios.

Un proxy debe entender el protocolo de la aplicación que está siendo usada, aunque también puede implementar protocolos específicos de seguridad (por ejemplo: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente). Los servidores proxy, son aplicaciones específicas.

Virus

Un *virus* es un programa cuyo objetivo prioritario es su propagación entre ordenadores sin ser advertido por el usuario. Una vez que el virus considera que está lo suficientemente extendido pasa de su *fase de latencia* a su *fase de activación*.
En esta fase los efectos del virus pueden ser tan variados como alcance la imaginación de su autor: pueden limitarse a mostrar inofensivos mensajes en pantalla o bien, eliminar información del disco duro o dañar la BIOS del ordenador.

Sus vías de propagación son las clásicas del software: disquetes, CD-ROMs, discos ZIP, copia de archivos por la red, descarga de un archivo por FTP o HTTP, adjunto de correo electrónico, etc.

Sin embargo, las estadísticas demuestran que la principal vía de infección de virus es el correo electrónico; concretamente, los archivos adjuntos del correo. Debemos extremar las precauciones cuando recibamos un correo electrónico con un archivo adjunto.

¿Cómo podemos proteger nuestra red de virus? Básicamente por dos frentes: mediante una adecuada *formación de los usuarios (prevención)* y mediante programas *antivirus (detección y desinfección)*. La primera forma es la más eficiente puesto que es aplicable tanto para virus conocidos como desconocidos.

Formación de los usuarios

¿Saben los usuarios de nuestra empresa lo que *no* deben hacer? ¿Saben que si abren un archivo ejecutable desde su puesto de trabajo pueden comprometer la seguridad de toda la empresa? La formación de los usuarios, especialmente aquellos que tengan acceso a Internet en sus puestos, es lo primero que tenemos que tener en cuenta como administradores de una red.

- La navegación por Internet y la lectura de correos electrónicos no se consideran situaciones de riesgo. No es necesario siquiera tener un antivirus funcionando.
- La visión de imágenes (.GIF o .JPG) u otros archivos multimedia (.MP3, .MID, .WAV, .MPEG...) que habitualmente se transmiten por correo electrónico, tampoco suponen ningún riesgo.
- Los documentos de Office pueden contener virus de macro (archivos .DOC y .XLS principalmente). Se deben comprobar siempre con un programa antivirus antes de abrirlos.
- Los archivos ejecutables recibidos por correo electrónico *no se deben abrir bajo ningún concepto*. Los formatos más habituales son .EXE, .COM, .VBS, .PIF y .BAT.

- En caso de duda es preferible no abrir el archivo adjunto, aunque provenga de un remitente conocido. Los archivos más sospechosos son los que tienen un nombre gancho para engañar a usuarios ingenuos: LOVE-LETTER-FOR-YOU.TXT.vbs, AnnaKournikova.jpg.vbs, etc. Este tipo de archivos, en un 90% de probabilidades, no contienen lo esperado o, si lo contienen, también incluyen un *regalito* malicioso oculto para el usuario.

Los nuevos virus tratan de aprovecharse de la ignorancia de los usuarios para hacerles creer, mediante técnicas de *ingeniería social*, que cierto correo con datos interesantes se lo está enviando un amigo suyo cuando, en realidad, son virus disfrazados.

Si todos los usuarios siguieran estos consejos habríamos conseguido probablemente una red libre de virus. Microsoft, consciente del elevado riesgo que supone el correo electrónico, dispone de una actualización de seguridad para su programa Outlook (no Outlook Express) que impide al usuario abrir archivos potencialmente peligrosos. Como administradores de redes debemos considerar la opción de aplicar esta actualización en todos los puestos.

Es responsabilidad del administrador instalar en todos los equipos de la red tanto los últimos parches de seguridad como las últimas actualizaciones del antivirus.

¿Cómo podemos configurar los puestos de trabajo para reducir las situaciones de riesgo en el correo electrónico?

- *Desactivar la ocultación de las extensiones* de los archivos.
- *Instalar la última versión* de Internet Explorer y de Outlook Express / Outlook junto a todas sus actualizaciones.
- *Instalar todas las actualizaciones críticas de Windows* recomendadas en www.windowsupdate.com.
- Si usamos el gestor de correo Outlook, *instalar la actualización de seguridad* que impide abrir archivos adjuntos potencialmente peligrosos.
- *Establecer la seguridad de nuestro programa de correo electrónico en alta*. En Outlook Express hay que elegir la opción "Zona de sitios restringidos"

Antivirus

Los programas antivirus detectan la presencia de virus en archivos impidiendo la infección del sistema. Además disponen de rutinas de desinfección con mayor o menor éxito en función del tipo de virus y de la calidad del programa antivirus.

Cada día se desarrollan nuevos virus los cuales pueden no ser detectados por nuestro programa antivirus. Las desinfecciones de archivos en caso de que un posible virus haya destruido datos (sobrescribiéndolos con caracteres basura, por ejemplo) pueden no tener ningún éxito.
En la mayoría de los casos, después de una infección no queda más remedio que reinstalar equipos y recuperar datos de copias de seguridad. Por lo tanto, debemos invertir en medidas de prevención y detección para que las infecciones no lleguen a producirse. Si a pesar de todo ocurre lo peor, nuestra red debe estar diseñada para que las consecuencias sean las menores posibles.

¿Dónde colocar el antivirus?

Se puede situar en los clientes y/o en los servidores:

- **En los servidores**. Teniendo en cuenta que el correo es la principal vía de propagación de virus, el servidor más crucial es el de correo. Existen en el mercado programas antivirus diseñados para acoplarse a los principales servidores de correo (para *Exchange Server*, por ejemplo). Téngase en cuenta que el servidor de correo nunca va a ser infectado por mucho que esté reenviando virus puesto que estos programas nunca llegan a ejecutarse en el servidor. La misión de un antivirus en un servidor de correo es proteger la red interna de virus externos recibidos por correo. Los usuarios de la red nunca recibirán virus en sus cuentas de correo (al menos, en las que dependen de este servidor, nada puede hacer con cuentas de correo gratuitas tipo Hotmail). Como inconveniente de la instalación del antivirus está la sobrecarga de trabajo en el servidor así como el elevado coste del software. Debemos hacer un balance de los factores coste, potencia del servidor y necesidad real de esta protección.

También podemos pensar en la instalación de un antivirus permanente en el servidor de archivos de la empresa. Sin embargo, esta no suele ser una buena idea precisamente por la sobrecarga que esto supone para la máquina. Sí es interesante, en cambio, analizar diariamente todos los archivos de usuarios en momentos en que el servidor tenga poca carga (por la noche, por ejemplo) mediante un análisis programado. Este análisis se puede realizar desde el propio servidor o bien, desde un puesto de trabajo que haya iniciado sesión con privilegios de administrador y tenga acceso, por tanto, a los documentos de todos los usuarios.

- **En los clientes**. Se pueden utilizar dos tipos de antivirus:

    - Antivirus residentes en memoria. Suele identificarse mediante un icono en la barra de tareas. Analiza todos los archivos antes de que el sistema operativo los abra (tecnología *on-access*) e informa de la presencia de virus. Este sistema es necesario en las empresas puesto que protege no sólo del correo sino también de virus provenientes de otras fuentes (como disquetes o descargas por FTP). de forma transparente para el usuario.

    - Antivirus bajo demanda. Se activa únicamente a petición del usuario para analizar una unidad, directorio o archivo determinado. Es útil para usuarios avanzados que prefieren tener desactivado habitualmente el antivirus residente para trabajar a mayor velocidad pero resulta demasiado complejo de utilizar para usuarios comunes.

    - Este tipo de antivirus se utiliza en la práctica para analizar discos duros completos o dispositivos de datos que acabamos de recibir (disquete, CD regrabado, disco LS-120, etc...)

Como norma general debemos instalar un antivirus residente en cada puesto de la red (pero no en los servidores). Si se trata de una red de dimensiones considerables y el presupuesto lo permite, podemos considerar también la instalación de un antivirus específico para el servidor de correo de la empresa.

Como administradores de la red tenemos que preocuparnos de: *Formar al usuario* para que distinga las situaciones que entrañan riesgo para la empresa de las que no. Es importante comprender que un sólo equipo infectado puede propagar la infección al resto de equipos de la red.

1.- Mantener los antivirus de todos los puestos actualizados. La actualización debe ser diaria o, como mucho, semanal. Para evitar la tediosa tarea de actualizar el antivirus puesto por puesto, se debe buscar un sistema que permita la actualización de forma centralizada.

2.- Realizar copias de seguridad diaria o semanal de los documentos de los usuarios almacenados en el servidor de archivos y mantener un historial de copias. Los usuarios deben ser conscientes de que los únicos datos que estarán protegidos serán los que estén almacenados en el servidor pero no los que residan en sus equipos locales. Las copias de seguridad se suelen dejar programadas para realizarse durante la noche. El historial de copias se consigue utilizando un juego de cintas (las hay disponibles de varias decenas de GB) que se van utilizando de forma rotativa. Por ejemplo, con un juego de 7 cintas tendríamos siempre un historial de 7 copias de seguridad anteriores. Por supuesto, las cintas deben guardarse en lugar seguro y, a ser posible, lo más alejadas físicamente del servidor con objeto de evitar la destrucción de todos los datos en caso de desastres naturales: inundaciones, incendios, etc.

3.- Evitar la compartición de unidades y carpetas en los ordenadores cliente. Todos los recursos compartidos deben estar en los servidores, nunca en los ordenadores cliente. De esta forma se evitan propagaciones masivas de virus entre los puestos de trabajo.

Caballos de Troya

Los *caballos de Troya* o *troyanos* son programas que se distribuyen siguiendo los mismos métodos que los virus. Las medidas de prevención son las explicadas anteriormente para el caso de los virus. Los troyanos más conocidos son también detectados por programas antivirus.

Pero, ¿qué es exactamente un caballo de Troya? Es un programa que tiene una apariencia inofensiva pero que realmente tiene objetivos hostiles. En concreto, se trata de un programa con dos módulos: un módulo servidor y otro cliente.

El atacante se instala, con fines nada éticos, el módulo cliente en su ordenador, el módulo servidor es el troyano propiamente dicho que se envía a la víctima bajo alguna apariencia completamente inofensiva (unas fotos, un juego, etc.). Una vez que la víctima cae en la trampa y ejecuta el archivo éste se instala en su ordenador. A partir de ese momento, el atacante puede monitorizar todo lo que la víctima hace en su ordenador incluyendo el robo de contraseñas y documentos privados.

El troyano, después de ejecutarse, abre un determinado puerto en modo escucha en el ordenador de la víctima. El atacante puede crear entonces una conexión desde su ordenador hasta la dirección IP y puerto de la víctima (debe conocer estos dos números o diseñar algún método para obtenerlos). Una vez que está establecida la conexión, el atacante, que puede estar a miles de kilómetros, tendrá acceso completo al ordenador de la víctima.

Para detectar la presencia de un troyano basta con utilizar el comando *NETSTAT -A*. Si observamos algún puerto a la escucha que no esté asociado con ninguna aplicación conocida de nuestro ordenador es señal de una posible presencia de troyanos. Si, además, observamos que se establece una conexión con una dirección IP desconocida es muy probable que nuestro ordenador esté transfiriendo datos sin nuestro consentimiento.

Los antivirus no son los programas más efectivos para enfrentarse a los caballos de Troya. En su lugar, es más recomendable la utilización de cortafuegos o *firewall* que nos avisará cuando detecte el establecimiento de una conexión TCP sospechosa o, simplemente, la rechazará. En las redes suele ser suficiente con la colocación de un cortafuego justo en la salida de Internet.

Ley de los mínimos privilegios

Todos aquellos servicios que no sean imprescindibles en una red se deben deshabilitar. Además, todos aquellos privilegios que no sean indispensables para que los usuarios ejerzan con comodidad su trabajo deben ser suprimidos.
Todo esto se resume con la *ley de los mínimos privilegios*: ningún usuario ni ordenador debe poder hacer más de lo necesario. Veamos unos ejemplos:

- El servidor de correo de la empresa no tiene porqué tener habilitados los servicios de páginas Web, FTP e impresión si no están siendo utilizados.
- El servidor de usuarios de la empresa no tiene porqué tener habilitados los servicios de páginas Web y mensajería si no son indispensables.
- Los usuarios del departamento de diseño gráfico no tienen porqué tener acceso a los archivos del departamento de contabilidad.
- Los puestos de trabajo no deben tener programas que no sean indispensables para la empresa. Por ejemplo: clientes de IRC, programas de descarga de MP3, programas de mensajería, etc.
- Los usuarios no tienen porqué poder compartir carpetas en sus ordenadores locales si existe un espacio en un servidor preparado para el intercambio de datos.

Desde el punto de vista de la seguridad, la red más segura sería aquella que no dejara hacer nada (ni trabajar, siquiera) y la red más insegura aquella que lo permitiera todo (entrar desde el exterior a usuarios anónimos, por ejemplo). Por supuesto, debemos buscar un compromiso entre seguridad y número de servicios / privilegios requeridos para trabajar con comodidad.

Deshabilitar servicios innecesarios

Un servidor con pocos servicios habilitados tiene las siguientes ventajas: funciona más rápido puesto que tiene menos tareas a las que atender, consume menos memoria y hace un menor uso del procesador, produce menos errores (hay menos cosas que pueden fallar y menos módulos que puedan interferir entre sí), es más resistente a agujeros de seguridad (sólo le afectan los agujeros de seguridad de los servicios que tiene activos) y, por último, tiene un mantenimiento más sencillo (sólo hay que instalar los parches de seguridad de los servicios que tiene habilitados). La gestión de servicios en Windows NT se realiza desde Panel de control / Servicios.

Los servidores deben tener el menor número de puertos abiertos. Esto se consigue eliminando todos los servicios innecesarios. De esta forma evitamos posibles ataques desde el exterior que se aprovechan de algún reciente agujero de seguridad para puertos concretos. Los puertos abiertos se listan con la orden *NETSTAT -A*. Por supuesto, los clientes sólo deben tener abiertos los puertos imprescindibles para sus tareas (generalmente los puertos NetBIOS: 137, 138 y 139): nunca un puesto de trabajo puede ser un servidor Web o similar (esto se produce en ocasiones con puestos de trabajo que funcionan con Windows 2000 Professional).

La gestión de los privilegios de los usuarios debe realizarse cuidadosamente en los servidores de usuarios y archivos. Aunque los usuarios sean de confianza siempre reduciremos riesgos por descuidos.

Además, en el caso de una infección por virus, el virus no podrá traspasar los departamentos si no hay ninguna vía de acceso o recurso compartido común. En general, la aplicación de la ley de los mínimos privilegios reduce la mayor parte de riesgos potenciales.

Parches de seguridad

El *software* que sale al mercado dista mucho de ser un producto perfecto e infalible: habitualmente contiene una serie de errores que no fueron detectados o corregidos a tiempo antes de su comercialización. Desde el punto de vista de la seguridad nos interesan aquellos fallos que pueden ser utilizados por personas maliciosas para romper la seguridad de un sistema, extraer datos, dejar un sistema fuera de servicio, etc. Cada día se descubren nuevos *agujeros de seguridad* en los productos más utilizados y también cada día se lanzan *parches de seguridad* que subsanan estos errores. El tiempo que transcurre entre que un agujero de seguridad es publicado y la instalación del correspondiente parche en el servidor es tiempo que el servidor está a merced de los *hackers* que pululan por la Red.

Si bien los servidores son las máquinas más sensibles de la red y a las que debemos prestar una mayor atención, tampoco debemos olvidarnos de los clientes. Los puestos de trabajo deben contener al menos todas las *actualizaciones críticas* que recomienda www.windowsupdate.com

Hackers - Crackers

Podemos encontrarnos con diferentes términos para definir a estos personajes: *hackers*, *crackers*, piratas, etc., estando normalmente condicionado el calificativo a los objetivos y a los efectos de sus ataques a los sistemas. El término *hacker*, por ejemplo, se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños. Los *crackers*, en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los piratas, su actividad se centra en la obtención de información confidencial y *software* de manera ilícita.

Es muy difícil establecer perfiles de estas personas, porque salvo en los casos en que han saltado a la luz pública como resultado de sus actividades, en su conjunto forman un círculo cerrado e impenetrable. Una aproximación podría ser la de un joven, bastante inteligente, con necesidad de notoriedad, inclinaciones sectarias, y en muchos casos, algo de inadaptación social. Su principal motivación es la de acceder a sistemas protegidos de forma fraudulenta, en una escala que va desde la mera constancia de su éxito, hasta la destrucción de datos, obtención de información confidencial, colapso del sistema, etc.

Normalmente los objetivos más apetecibles son los sistemas relacionados con la seguridad nacional, defensa e instituciones financieras, pero ante las posibles consecuencias legales de estos actos optan por otros organismos públicos, las universidades y las empresas.

Existe una serie de grupos que tienen un carácter supranacional, y que se extiende a través de su hábitat natural: Internet. A través de este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización. Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectara a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas.

Ataques a la información

¿Cuales son las amenazas?

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines.

Genios informáticos, por lo general veinteañeros, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, etc.

Como los administradores de todos los sistemas, disponen de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando. Todos los movimientos del sistema son registrados en archivos, que los operadores revisan diariamente.

Métodos y herramientas de ataque

En los primeros años, los ataques involucraban poca sofisticación técnica. Los insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando un password válido.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos.

El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y Web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

Sniffing

Muchas redes son vulnerables al *eavesdropping*, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El *sniffer* puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrante y saliente. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Snooping y downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron : el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

Tampering o data diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor. Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet.

Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma comun de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

Jamming o flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Importancia de las Bitácoras

Hoy en día los sistemas de cómputo se encuentran expuestos a distintas amenazas informáticas. Las vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos. El número de ataques también aumenta.

Los sistemas de cómputo generan una gran cantidad de información (bitácoras o *logs)* que puede ser de ayuda ante un incidente de seguridad.

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera.
– Fecha y hora.
– Direcciones IP origen y destino.
– Dirección IP que genera la bitácora.
– Usuarios.
– Errores.

La utilización de bitácoras nos puede ayudar a la recuperación ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, entre otras.

Entre las desventajas que se tienen es que se necesita de una revisión diaria de las bitácoras lo que lo vuelve una tarea tediosa, debido a esto es una actividad que pocos administradores llevan a cabo. Además que se desconoce que las bitácoras nos pueden evitar horas de angustia.
Las bitácoras contienen información crítica, es por ello que las bitácoras deben ser analizadas, además de que están teniendo mucha relevancia como evidencia en aspectos legales. El uso de herramientas automatizadas es muy útil para el análisis de bitácoras. Es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo activos.

Herramientas de análisis de Bitácoras

Para UNIX

- Logcheck.
- Swatch.
- Entre otras.

Para Windows

- LogAgent

Snnifers

Usando los Sniffers a nuestro favor

Los sniffers pueden ser una pesadilla para un administrador si son utilizados por usuarios no autorizados. Sin embargo, hay pocas herramientas tan poderosas como estas para detectar problemas en nuestra red. Es indispensable para un administrador de sistemas el conocer al menos el funcionamiento básico de estas herramientas y utilizarlas como parte de su rutina cotidiana. Entre los más útiles encontramos a:

tcpdump

Uno de los sniffers más comunes. Nos permite trabajar rápidamente desde línea de comando especificando los patrones que nos interesan, puede examinar una gran cantidad de protocolos, puede guardar el flujo capturado en un archivo o tomar un archivo como fuente para el flujo a analizar.

darkstat y traffic-vis

Diseñados para funcionar como proceso demonio, recolectando estadísticas de uso de la red. Ambos reportan sus resultados a través de una interfaz Web, un reporte Postscript u otros formatos.

ngrep

Tiene una filosofía de uso muy similar a la del comando 'grep' de Unix, tomando como entrada el flujo de la red en vez de archivos locales.

snort

Muy completa herramienta de detección de intrusos en red, toma como entrada el tráfico capturado en una red y lo va comparando cun una serie de reglas, registrando cualquier tráfico sospechoso de llevar un ataque.

Snort únicamente lo registra, pero puede trabajar en conjunto con otras herramientas para sanear el tráfico, bloquear a la máquina atacante, generar reportes, etc.

nwatch

Formalmente es un sniffer, pero es más bien una herramienta para realizar lo que sus autores definen como barridos de puertos pasivos: Para detectar puertos que están abiertos por muy cortos periodos de tiempo y para no mostrar actividad sospechosa de barrido, nwatch se queda escuchando la actividad de la red, y manteniendo una lista de qué hosts proveen qué servicios.

ethereal

Un magnífico sniffer con interfaz gráfica de usuario, nos brinda un análisis completo y detallado de cada paquete a varios niveles, desde nivel Ethernet hasta detalles de diversos protocolos. Es capaz de convertir en adicción el comprender cómo funcionan determinados protocolos

ettercap

Permite sniffear redes switheadas. Además de sniffer es interceptor (permite inyectar datos en conexiones existentes o "secuestrar" conexiones).

kismet

Sniffer específico a Linux para redes inalámbricas. Funciona correctamente con los dos principales tipos de tarjetas inalámbricas.

AUDITORIA INFORMÁTICA

La auditoria es un examen crítico, que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Para el auditor informático lo más importante es la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información.

Al igual que los demás órganos de la empresa los Sistemas Informáticos están sometidos al control correspondiente, o al menos deberían estarlo. La importancia de llevar un control de esta herramienta tiene que ver con varios aspectos, algunos de ellos son:

Las computadoras y los Centros de Proceso de Datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoria Informática de Seguridad.

Las computadoras creadas para procesar y difundir resultados o información elaborada, pueden producir resultados o información errónea si dichos datos son falsos. Este caso es olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto que dañe a todos. En este caso interviene la auditoria Informática de Datos.

Un Sistema Informático mal diseñado puede convertirse en una herramienta muy peligrosa para la empresa, ya que las máquinas obedecen las órdenes recibidas y la organización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, por la tanto la empresa no puede depender de un Software y Hardware mal diseñados. Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la Auditoria de Sistemas.

La auditoria nace como un órgano de control de algunas instituciones estatales y privadas, su función inicial es estrictamente económico-financiero.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones.

Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoria contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionarios, dichos cuestionarios llamados Check List, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad. La Check List puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. Sólo una metodología precisa puede desentrañar las causas por las cuales se realizan actividades teóricamente inadecuadas o se omiten otras correctas.

Auditoria interna y externa

La auditoria interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoria interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoria externa es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la Auditoria Interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoria interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su Plan Anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorias, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

Una Empresa o Institución que posee auditoria interna puede y debe en ocasiones contratar servicios de auditoria externa. Las razones para hacerlo suelen ser:

- Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- Servir como mecanismo protector de posibles auditorias informáticas externas decretadas por la misma empresa.
- Aunque la auditoria interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorias externas como para tener una visión desde afuera de la empresa.
- La auditoria informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido ajeno a la propia estrategia y política general de la empresa.

La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

Alcance de la auditoria informática

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. La indefinición de los alcances de la auditoria compromete el éxito de la misma.

* Control de integridad de registros:

Hay Aplicaciones que comparten registros, son registros comunes. Si una Aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

* Control de validación de errores:

Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

Síntomas de necesidad de una Auditoria Informática

Las empresas acuden a las auditorias externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

Síntomas de descoordinación y desorganización:

- No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.

- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

[Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna norma importante]

Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

- No se reparan las fallas de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

Síntomas por debilidades económico-financiero:

- Incremento desmesurado de costes.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones Presupuestarias significativas.
- Costes y plazos de nuevos proyectos

Síntomas de Inseguridad: Evaluación de nivel de riesgos

- Seguridad Lógica
- Seguridad Física
- Confidencialidad

[Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales]

- Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia Totales y Locales.
- Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoria. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

Planes de contingencia

En la mayoría de las empresas generalmente se tienen que hacer Backups de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro fuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, para que en caso de que se produzca la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas.

Objetivo fundamental de la auditoria informática

Operatividad

Consiste en que la organización y las maquinas funcionen, siquiera minimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoria debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados.

Los Controles Técnicos Específicos, son necesarios para lograr la Operatividad de los Sistemas.

Control de Procesos y Ejecuciones de Programas Críticos

El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones.

Si los programas fuente y los programas módulo no coincidieran podrían provocarse errores que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc .

Auditoria Informática de Sistemas

Se ocupa de analizar la actividad que se conoce como Técnica de sistemas en todas sus facetas. La importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no haga daño ni condicione al Sistema.

Software de Teleproceso (Tiempo Real):

No se incluye en Software Básico por su especialidad e importancia.

Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. El tunning revisa y así establece previamente planes y programas de actuación según lo observado.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los Sistemas y Subsistemas:

Técnica de Sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas.

Optimización: Un ejemplo es cuando se instala una Aplicación, normalmente está vacía, no tiene nada cargada adentro, a medida que se va cargando, la Aplicación se va poniendo más lenta, porque la información que está moviendo es cada vez mayor.

Lo que se tiene que hacer es un análisis de performance, para luego optimizarla y así mejorar el rendimiento de dicha Aplicación.

Administración de Base de Datos:

El diseño de las bases de Datos, se ha convertido en una actividad muy compleja y sofisticada. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración, se analizará los sistemas de salvaguarda existentes y se revisará la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

Investigación y Desarrollo:

La auditoria informática deberá cuidar de que la actividad de Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

Auditoria Informática de Comunicaciones y Redes

El auditor de comunicaciones deberá poner atención sobre los índices de utilización de las líneas contratadas con información abundante 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. La inexistencia de datos sobre cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas.

Auditoria de la Seguridad informática

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas, etc. y puede ser mal utilizada por personas que hagan mal uso de esta, también puede ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas")y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica.

La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a las de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, etc.

La seguridad lógica se refiere a la seguridad del uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

La decisión de abordar una Auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida.

Herramientas y Técnicas para la Auditoria Informática

Cuestionarios:

Las auditorias informáticas se materializan recabando información y documentación de todo tipo. Por lo tanto, es habitual solicitar la complementación de cuestionarios

Entrevistas:

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Checklist:

Es un conjunto de preguntas muy estudiadas que han de formularse flexiblemente a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes, las Checklists por lo regular deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

Checklist de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

Checklist Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Trazas y/o Huellas:

El auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Las "trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas, no deben modificar en absoluto el Sistema.

Log:

El log es un historial que informa que fue cambiando y cómo fue cambiando (información), te permite analizar cronológicamente lo que sucedió con la información que está en el Sistema o que existe dentro de la base de datos.

Software de Interrogación:

En la actualidad se han utilizado productos software llamados (paquetes de auditoria), capaces de generar programas para auditores. Los productos Software especiales para la auditoria informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada.

MODELOS DE REDES SEGURAS

Las **contraseñas** escogidas en la red deben ser contraseñas seguras. No solamente las contraseñas de los servidores sino también la de los usuarios que inician sesión en sus puestos de trabajo. Las contraseñas deben tener más de 5 0 6 caracteres, cuanto mas larga sea la contraseña, más complicado será romperla, también se pueden combinar números y letras en mayúsculas para tener una mayor seguridad

Las contraseñas se deben renovar periódicamente (cada dos meses,) por si alguna hubiese podido ser descubierta. Además, se deben utilizar contraseñas distintas para cada servicio de la red. Por ejemplo, sería muy inseguro utilizar la misma contraseña para el correo electrónico que para la cuenta de administrador de un servidor. ¿Por qué? Sencillamente porque una contraseña de correo no viaja encriptada por la red y podría ser descubierta fácilmente.

La utilización de **switches** es preferible a la utilización de hubs. Recordemos que un hub difunde la información que recibe desde un puerto por todos los demás. La consecuencia de esto es que todas las estaciones conectadas a un mismo hub reciben las mismas informaciones. Si en uno de estos puestos se sitúa un usuario malicioso (o bien, ese puesto está controlado remotamente mediante un troyano u otro tipo de acceso remoto) es posible que trate de instalar una herramienta conocida como *sniffer* para analizar todo el tráfico de la red y así, obtener contraseñas de otros usuarios. Los sniffers utilizados correctamente pueden mostrar información muy útil para el administrador de una red, pero en manos de usuarios maliciosos y en redes mal diseñadas supone un elevado riesgo de seguridad. Un sniffer instalado en un puesto de trabajo carece de utilidad si en la red se utilizan switches para aislar los puestos. En cambio, un sniffer instalado en un servidor (de correo o de usuarios) puede revelar datos altamente confidenciales. Es muy importante, por tanto, restringir el acceso de usuarios a los servidores así como mantenerlos protegidos con las últimas actualizaciones de seguridad.

Es preferible que las **zonas pública y privada de nuestra red utilicen cableado distinto**. Así evitaremos que un servidor de la zona pública comprometido pueda escuchar tráfico de la zona privada. Veamos dos ejemplos:

Configuración incorrecta. El servidor *proxy* que separa las zonas pública y privada utiliza una sola tarjeta de red. Tanto los servidores públicos como los puestos de trabajo internos comparten el mismo cableado, es decir, se pueden conectar indistintamente a cualquier puerto libre de cualquier hub de la red. Y, lo que es más grave, cualquier usuario podría autoasignarse una IP pública y comprometer toda la seguridad de la red.

Configuración correcta. El servidor *proxy* utiliza dos tarjetas de red. Una tarjeta de red se conecta al hub de la zona pública y la otra, al hub de la zona privada. La única vía física posible de pasar de una zona a otra es mediante el servidor proxy. Si un usuario trata de asignarse una IP pública a su puesto de trabajo quedará aislado de todos los demás.

Los servidores

¿En la zona pública o en la zona privada?

Estamos de acuerdo en que los servidores tienen que tener direcciones IP públicas para que sean accesibles desde todo Internet. Sin embargo, no suele ser recomendable asignar directamente las IP públicas a los servidores. En su lugar se les puede asignar direcciones privadas e implantar un sistema de traslación de direcciones públicas-privadas. De esta forma se consigue que todo el tráfico público de la red se filtre por un router o/y cortafuegos antes de llegar a los servidores.

Los **cortafuegos** o *firewalls* se sitúan justamente en la salida a Internet de la red. Disponen de un panel de control que permite cerrar aquellos puertos que no se van a utilizar y así solventar descuidos de configuración de servidores internos.

Por último, debemos recordar que el **servidor de archivos** debe estar correctamente configurado de forma que cada usuario pueda ver únicamente sus archivos pero no los de los demás usuarios. En el caso de redes grandes puede resultar interesante la división de departamentos en **subredes** (con cableado separado además) con el fin de crear unidades de administración independientes. De esta forma los usuarios de un departamento serán completamente independientes de los de otros departamentos.

Todo lo anterior son ideas que nos pueden guiar durante el diseño de una red segura. Cada caso hay que estudiarlo por separado evaluando los factores coste, nivel de seguridad requerido, comodidad de los usuarios y facilidad de administración.

CONCLUSIONES

- Tenemos como conclusión general que la información es uno de lo activos intangibles más importantes con los que cuentan las empresas, ya que con este es con lo que la empresa hace uso todos los días. De la información van a depender las decisiones que se tomen dentro de la empresa, por estas razones es por lo que las empresas de hoy en día trabajan para tener los mejores procedimientos y tecnología para protegerla. Como se menciono dentro de los objetivos, este trabajo servirá como guía para elaborar las políticas adecuadas e implementar las herramientas de seguridad adecuadas en nuestra LAN.

- La elaboración de Políticas de Seguridad no es un trabajo sencillo, es por esto que en la mayoría de las empresas no se le da la importancia necesaria a este tema. La raíz del problema esta en que no se tienen bien definidos los roles dentro de las empresas o los usuarios no tienen bien claro la importancia que tiene la información. Tomando como referencia Instituciones Gubernamentales o Privadas dentro de Morelia, las Políticas de Seguridad son un tema que casi es nulo dentro de las mismas, ya que en la mayoría no tienen Políticas de Seguridad o si las tienen no las llevan a cabo, esto es debido a varios factores, uno de ellos es que los usuarios no tienen la suficiente cultura para darle la importancia necesaria al uso de la información que utilizan o que generan, y por lo mismo muchas veces permiten el acceso a personas ajenas o de la misma institución a sus equipos de trabajo, sin pensar siquiera que a la información le vallan a dar un uso inadecuado. Es por esto que las Instituciones deben de empezar con la delegación de responsabilidades y con el concientizar a los usuarios de la importancia de la información que es generada.

- En este trabajo se tomo como base operativa para el desarrollo del mismo el uso del Sistema Operativo Windows NT, ya es uno de los Sistemas Operativos más utilizados en las LANs. Pero no es único, tenemos otros Sistemas Operativos que nos brindan características diferentes, entre estos se encuentran los Sistemas Operativos Linux, UNIX, Novell entre otros. Se hace mención de estos Sistemas Operativos, debido a que muchas de las empresas no quieren invertir demasiado dinero a la parte de seguridad en sus redes, pero teniendo un conocimiento más amplio de los diferentes Sistemas Operativos, no es necesario gastar mucho dinero en la implementación de la seguridad en nuestra LAN.

- En la actualidad se han visto ataques muy frecuentes de diferentes tipos de virus, como lo fueron el Sobig, Blaster, Sasser, entre otros. Debido a esto muchas de las empresas están muy preocupadas para tratar de no ser infectadas, pero como se comento en el segunda párrafo, los usuarios muchas veces no tienen el conocimiento necesario de que hay correos electrónicos que pudieran ser virus, y estos al no saberlo, abren dichos correos trayendo esto como consecuencia la infección de la máquina donde se abre el correo y en ocasiones la infección de toda la LAN.

Debido a esto, muchas de las empresas han adoptado políticas de seguridad respecto al paso de correos electrónicos sospechosos, y a su ves también le brindan información a los usuarios para que no abran correos electrónicos de procedencia dudosa. Otro de los temas donde se han venido implementando políticas de seguridad, es en el uso del Chat como el Messenger de Hotmail o de Yahoo que son los más utilizados. En varias de las empresas han tomado decisiones drásticas y lo que hacen es cerrar los puertos por donde estos Chat se conectan.

RECOMENDACIONES

- Además de tomar en cuenta las diferentes recomendaciones que se hicieron durante el desarrollo del trabajo, como por ejemplo el saber quienes van a ser los responsables de la realización de las Políticas de Seguridad, el tener a los usuarios al corriente con el conocimiento de las mismas, el ver que estén actualizadas. Otra recomendación sería el darles a los usuarios una capacitación constante, sobre todos los posibles ataques a los que se esta expuesto por hacer uso del Internet, y tratar de concientizarlos de que el uso del correo electrónico, Chat, Web, es una arma muy poderosa para violar las barreras de seguridad implementadas en la institución. Esta recomendación es más que nada de información, ya que muchas de las veces en que la seguridad de una LAN es violada, fue por que algún usuario entro a un sitio a donde no debió de entrar o descargo algún archivo de dudosa procedencia, entre otras. Y todo esto por que el usuario no estaba informado.

- Debido al avance tan rápido y creciente de la tecnología en cuanto al Software y Hardware para la seguridad, siempre se tendrá que estar actualizado en cuanto a las nuevas versiones y parches de seguridad, ya que los ataques a nuestra LAN van a estar siempre presentes, y el no estar actualizados nos hará vulnerables tanto por usuarios internos o externos así como a través del Internet.

- Como recomendación final y como se comento en alguno de los apartados del documento, "no hay Sistema 100% seguro" solo el que encuentra aislado o el que no es usado, pero debido a que esto no se puede hacer por el simple hecho de que es necesario para realizar nuestro trabajo. Nos debemos hacer a la idea, que aunque en el desarrollo e implementación de las Políticas de Seguridad se hayan visto todos los posibles aspectos de la seguridad, siempre va a ver algo que va a fallar y que violará la Seguridad de nuestra LAN, es por esto que se debe estar conciente de este problema y en ves de estar viendo en que momento pudiera ser violada la seguridad, es mejor estar preparados ante un problema de seguridad, esto es que se debe de hacer un buen plan de contingencia, para tratar de mantener la información segura, ya que como se comento anteriormente esto es lo que se debe proteger y si es necesario que por algún problema de seguridad sea necesario el tener aislado los sistemas donde se almacenan la información, es preferible hacer esto, que el tenerlos trabajando con el riesgo de que la información pueda sufrir ataques.

BIBLIOGRAFIA

Libros:

RAYA, José Luis, Cristina Raya, **Redes Locales**. 2da ed. Mc Graw Hill, 2000

STRASSBER, Keith E, Richard J. Condek, Cary Rollie, **Firewalls.** 4ta ed. Mc Graw Hill, 2002

HORTON, Mike, clinton Mugge, **Claves Hackers.** 1era ed. Mc Graw Hill, 2003

ROBINSON, Ed, Michael James Bond, **Seguridad.** 2da ed. Mc Graw Hill, 2003

MADRUGA PAYNO, Javier, **Internet.** Anaya Multimedia, 2004

NOMBELA, Juan José, **Seguridad Informática.** 2da ed. Thomsom Paraninfo, S.A, 1996

VV, AA, **Seguridad en las Instalaciones de Telecomunicaciones, Informática y Sistemas Automáticos.** Editex, S.A, 2001

Web:

http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1128.html

http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_1165.html

http://www.monografias.com/trabajos12/fichagr/fichagr.shtml

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

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

http://www.iec.csic.es/criptonomicon/articulos/expertos71.html

http://fmc.axarnet.es/winnt4svr/indice_m.htm

http://www.ilustrados.com/PUBLICACIONES/EplpVpluZApDVycVbU.php

http://www.utp.ac.pa/seccion/topicos/SEGURIDAD/firewall.html

http://www.cisco.com/global/LA/powernow/spa/docs/White_Paper_BDM_SPA.pdf

Glosario de términos.

10 BASE 2	Implementación de Ethernet de 10 Mbps en cable coaxial delgado. Su máximo segmento es de 200 metros.
10 BASE 5	Implementación de Ethernet de 10 Mbps en cable coaxial grueso. Su máximo segmento es de 500 metros.
10 BASE F	Especificación para red Ethernet de 10 Mbps en fibra óptica.
10 BASE T	Estándar de transmisión de Ethernet sobre MIT a 10 Mbps.
100 BASE FX	Especificación para correr Ethernet 100 Mbps sobre fibra óptica.
100 BASE T	Estándar de transmisión sobre MIT de velocidad 100 Mbps.
100 BASE T4	Especificación para correr Ethernet 100 Mbps sobre cable 3,4 y 5 MIT de 4 pares.
100 BASE TX	Esquema que ofrece 100 Mbps sobre cable categoría 5 MIT.
Address	En redes, la palabra dirección se refiere a un distintivo único para cada nodo de la red.
Administrador	Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman superusuario.
Algoritmo	Serie de pasos para realizar una tarea específica.
Ancho de banda	Relación de velocidad para la transmisión de datos medidos en Kbps (kilo baundios por segundo) y que representa la capacidad del canal de comunicación para transportar datos.
ANSI	Organización encargada de la documentación de los estándares en Estados Unidos.
APPC	Protocolo de comunicación de dos equipos donde no existe director.
Application Server	Computadora destinada a brindar los servicios de una aplicación específica a los usuarios de una red.
ARCNet	Red de computadoras y recursos compartidos creado por Datapoint muy popular en los años setenta, cuyas características eran: bajo costo, cableado en estrella y velocidad hasta 2.5 Mbps.
ARP	Proceso en donde se asigna al número de la tarjeta una direccion formato TCP/IP.
ARPA	Agencia militar de Estados Unidos encargada de proyectos tecnológicos como las redes computacionales militares.
ARPANET	Proyecto del Departamento de Defensa de los Estados Unidos que utiliza protocolos tipo X.25 donde la cantidad de información (paquetes) no es fija. La dividieron en dos: Milnet para uso militar e Internet para uso público.
ASCII	Código utilizado para representar los caractere de escritura en formato binario (7 bits para 128 caracteres o el modo extendido de 8 bits para 256 caracteres).
Asíncrona	Forma de trasmisión de datos donde no se necesita señal adicional de reloj. La señal contiene la informació de cuándo cambia cada dato.
ATM	Tecnología de reciente introducción que permite la transmisión de grandes volúmenes de datos a gran velocidad, con tecnología de paquetes retrasados. Se considera la arquitectura del futuro en comunicaciones digitales.
AUI	Conexión utilizada para poder cambiar de tipo de cables en topologías Ethernet.
Average seek	Intervalo promedio de tiempo desde que el sistema solicita datos hasta que dispositivo los tiene disponibles.
Backbone network	Red de Infraestructura. Red que actúa como conductor primario del tráfico de datos de la red. Comúnmente recibe y manda información a otras redes.
Backup server	Servidor dedicado a realizar las copias de seguridad y restaurar los datos borrados por error de toda la información de la red.
Baud rate	Unidad de velocidad igual a un bit por segundo.
BIOS	Porción de firmware de una computadora que maneja el flujo de señales entre el sistema principal y los dispositivos periféricos. Controla puertos, memoria, teclado y dispositivos primarios.
BIT	Dígito binario, unidad mínima de información de los dos estados 0/1. Abreviación de Binary Digit que puede ser 0 o 1. Es la unidad básica de almacenamiento y proceso de una computadora. 8 bits = 1 byte.

BOOT	Proceso inicial por el que se cargan los programas para el total funcionamiento de la computadora.
BPS	Bits por segundo. Velocidad de transmisión serial.
Bridge	Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.
Broadcast	Transmisión abierta. Mensajes que se mandan sin destino específico.
Buffer	Espacio físico de memoria destinado a guardar datos temporalmente.
BUS	Circuito de interconexión eléctrica para transmitir información.
Byte	Conjunto de 8 bits. Representa un carácter en lenguaje binario.
CABLE NIVEL 3	Cable tipo MIT 2 pares que soporta 10 MHZ.
CABLE NIVEL 4	Cable tipo MIT que soporta 20 MHZ.
CABLE NIVEL 5	Cable tipo MIT 4 pares que soporta 100 MHZ.
Caché	Memoria más cercana al CPU, es utilizada como buffer entre el CPU principal y el resto de la computadora. Normalmente es la memoria de más rápida, fina y cara por ser la que más se ocupa.
Carrier o portadora	Señal eléctrica que permite la modulación de otra señal que contiene la información. Se utiliza para la transmisión remota vía la infraestructura de comunicaciones.
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía.Encargado de los estándares internacionales de comunicación.
CD-ROM	Memoria de lectura grabada en tecnología láser de CD.
CHIP SET	Referente al grupo de circuitos integrados que se utilizan para una función.número de pistas en los diferentes discos fisícos.
Cliente	Producto o presentación de front end (directamente con el usuario) que interactúa con otros servidores o productos de back end (sin presentación directa con el usuario). El cliente realiza solicitudes y presenta los resultados. No realiza los procesos ni los cálculos, eso se los deja a los programas de back end que son más poderosos pero no tienen la capacidad de comunicarse directamente con el usuario.
CMOS RAM	Memoria no volátil de lectura. Escritura que almacena la configuración del sistema.
Colisión	Definido como un exceso en portadora eléctrica. Sucede en Ethernet cuando dos o más estaciones hablan al mismo tiempo y las señales de datos se pierden.
Communication Server	Computadora destinada a dar los servicios de comunicaciones de la red.
Concentrador	Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.
Conectividad	Estado que permite la transferencia de datos entre dos computadoras.
CPU	Unidad de Proceso Central. Director y principal realizador de procesos de la computadora. Circuito microprocesador que realiza los procesos de datos básicos y controla el funcionamiento general de la computadora.
CSMA/CD	Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica sumada (portadora). En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.
Data Address	Localización fisíca dentro del dispositivo de almacenamiento.
DDP	Tipo de conexión a Internet creado por Datasys de América. Se lleva a cabo por medio de una línea telefónica que comunica a la computadora del cliente con el ruteador que da acceso a Internet. Mantiene velocidades de 56.4 Kbps y tiene la capacidad de alimentar una red de hasta 10 computadoras. Para su instalación, el DDP necesita: dos modems idénticos de 28.8 Kbps conectados a la computadora cliente y al ruteador del proveedor; instalación de Windows NT en la computadora cliente, y de una configuración especial para el ruteador del proveedor. Este producto elimina el ruteador del lado del cliente.
Dial Up	Circuito de comunicación que se establece vía telefónica.
Dirección Destino	En el lenguaje de redes es la computadora que envía los datos de una transmisión.
Dirección Fuente	En el lenguaje de redes es la computadora que recibirá los datos en una transmisión.
DLC	Protocolo para el manejo de datos a través de líneas de comunicación.

DMA	Procedimiento de bajo nivel que permite que un dispositivo secundario de puertos (externo) tenga acceso a los recursos de memoria sin que el microprocesador tenga que atender el proceso.
Dominio	Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.
DOS	Sistema operativo más usado en PC's.
Drive	Dispositivo que permite el alojamiento de un tercer elemento para completar un dispositivo (por ejemplo: un drive de cinta es el hardware que permite leer y escribir en una cinta).
Driver	Manejador. Es el programa que contiene el algoritmo de manejo de un tercer elemento para poder manejarlo como otro dispositivo (ejemplo: el programa que nos permite manejar una tarjeta de red como otro dispositivo es el driver).
DS0	Enlace de comunicación dedicado sencillo. Canal digital de ancho de banda igual a 64 Kbps.
DS1	Canal de comunicación digital de señal tipo 1; puede ser E1 de 1.44Mbps en Estados Unidos o T1 de 2.108 Mbps en el estándar europeo.
DS3	Canal de comunicación digital de señal tipo 3; puede ser de 44.736 Mbps.
DS4	Canal de comunicación digital de señal tipo 4, de 274.176 Mbps en estándar de Bell.
DTE	En redes, son los equipos en donde los datos tienen origen y destino.
E0	Término utilizado para referirse a los canales de ISDN de 64 Kpbs en estándar americano.
E1	Estándar europeo de transmisión de datos 2.048 Mbps.
E3	Cana de comunicación digital de 34 Mbps. El más veloz del mercado.
EEC	Método que consiste en grabar información adicional para poder corregir algún dato que se borre.
ECMA	Fija los parámetros de fabricación para los equipos de cómputo en europa.
EISA	Estándar de intercomunicación entre CPU/motherboards y tarjetas secundarias, dispositivos de I/O, bus AT mejorado de 32 bits compatible a ISA y con las ventajas de MCA.
E-mail	Correo que se establece vía electrónica mediante Internet. Cada persona tiene una dirección asignada en su computadora de tal manera que puede enviar y recibir mensajes.
Encriptamiento	Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.
EOT	Señal que se manda para indicar dónde termina una transmisión.
Escalabilidad	Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y tarjetas periféricas.
Estación	Computadora que puede realizar procesos.
Ethernet	Estándar de red más popular e implementado. Utiliza CSMA/CD con una velocidad de 10 Mbps.
Fast Ethernet	Topología de transmisión digital tipo Ethernet que transmite a 100 Mbps.
FAT	Archivo que utiliza DOS para saber la ubicación física de los archivos en un medio de almacenamiento.
FDDI	Estándar de transmisión de datos vía fibra óptica hasta de 100 Mbps con topología parecida a Token Ring/Token Passing.
File Server	Computadora dedicada a proveer y almacenar los archivos.
Firewall	Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.
Firmware	Conjunto de programas de sólo lectura que contienen el algoritmo para una función específica. Algoritmo o pequeño programa de bajo nivel grabado en un EEPROM para uso del procesador. También se llama Microcode.
Frame Relay	Paquetes retrasados. Protocolo de comunicación asíncrono con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño fijo.
FTP	Servicio que permite transferir archivos entre sistemas y entre redes remotas con sistemas diversos. De uso común en Internet.

Full Duplex	Característica de un canal de comunicación en el que dos terminales pueden mandar y recibir información simultáneamente.
Gateway	Dispositivo que permite conectra dos redes o sistemas diferentes. Es la puerta de entrada de una red hacia otra.
Gigabyte	GB, 1 073'741 824 bytes, formalmente es 1 K de MB.
GUI	Medio de desplegar las salidas para presentar al usuario un formato gráfico.
Half duplex	Característica de un canal de comunicación en el que dos terminales mandan y reciben información turnándose, una a la vez.
Hamming Code	Código de detección de errores de comunicación que consiste en enviar bits adicionales con la información acerca de los datos transmitidos para poder compararla en su destino.
Hardware	Referente a dispositivos reales, físicos. Todos los componentes electrónicos, magnéticos y mecánicos de las computadoras.
HDLC	Protocolo para redes X.25.
Hexadecimal	Sistema numérico con base en 16, comúnmente utilizado por su estructura fácil de transformarse al binario.
Hipertexto	También llamado Texto Virtual. Se refiere a la capacidad de recibir información en múltiples dimensiones. Una línea de texto puede llevar a otro texto, una imagen o una melodía.
Host	Computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.
Hub	Dispositivo inteligente que sirve de infraestructura para la red. Comúnmente asociado con un concentrador 10 base T con funciones inteligentes de retraso de señal (retiming), y retransmisión de la misma (repeating).
ICMP	Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.
IEEE	Agrupación de ingenieros que, entre otras funciones, documenta todos los desarrollos tecnológicos.
IEEE-802.1	Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
IEEE-802.2	Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI) llamado LLC.
IEEE-802.3	Define las formas de protocolos Ethernet CSMA/CD en sus diferentes medios físicos (cables).
IEEE-802.4	Define cuadros Token Bus tipo ARCNET.
IEEE-802.5	Define hardware para Token Ring.
IEEE-802.6	Especificación para redes tipo MAN (de área metropolitana).
IEEE-802.7	Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
IEEE-802.8	Especificación para redes de fibra óptica tipo Token Passing/FDDI.
IEEE-802.9	Especificaciones de redes digitales que incluyen video.
IEEE-802.11	Estándar para redes inalámbricas con línea de vista.
IEEE-802.12	Comité para formar el estándar de 100 base VG que sustituye CSMA/CD por asignación de prioridades.
IEEE-802.14	Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.
Interface	Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.
Internet	Red de redes con base en TCP/IP y acceso público mundial.
Internetworking	Término usado para referirse a la interacción entre varias redes.
Interoperabilidad	Término referente a la capacidad de diferentes redes para comunicarse entre sí.
Intranet	Red de área amplia con gran infraestructura y acceso privado.
IP	Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.

IPX	Protocolo definido para redes Netware que tienen direcciones en tres campos (nodo, red y socket), lo cual le permite mantener varios enlaces entre redes y procesos en varios servidores.
ISDN	Red pública utilizada para trasmitir varios tipos de información, texto, imágenes, sonido, etcétera.
ISO	Organización que especifica estándares de calidad internacionales.
ISO 9000	Juego de normas de calidad internacional que unifica el control de calidad a nivel mundial.
ISO 9001	Modelo de calidad para empresas de diseño, fabricación e instalación de equipo.
ISO 9002	Modelos de aseguramiento de calidad y satisfacción del cliente en el producto final.
Kernel	Parte del sistema operativo que actúa directamente con el hardware al más bajo nivel.
Kilobyte	KB. 1024 bytes.
Láser	Tecnología de semiconductores que permite concentrar la luz en un solo punto mediante señales electrónicas. Utilizada en tecnologías de impresión.
Layer	En el lenguaje de redes se refiere a cada uno de los subsistemas que interactúan en los procesos de la red.
LED	Tecnología electrónica que permite emitir luz imitando estados binarios 1=luz, 0=apagado.
Link	Término utilizado para referirse a los componentes lógicos y físicos que permiten la comunicación entre dos sistemas.
LLC	Controla las tareas de interacción entre la tarjeta de red y el procesador (nivel 2 y 3 del OSI).
Login	Proceso de entrada a la red utilizado como término para indicar que la estación está dentro de la red.
Logon	Proceso de entrada a un host. Utilizado para indicar que en realidad el trabajo se desarrolla en el host.
LPT	Abreviatura para asignar puertos paralelos.
MAC	Capa de control de acceso a medios. Capa del modelo de comunicación OSI, que es la encargada del control lógico del medio físico.
MAN	Red de Area Metropolitana.
Marcado por pulsos	Técnica utilizada para mandar la señal del número telefónico al que queremos contactar mediante cambios de intensidad en el voltaje.
Marcado por tonos	Técnica utilizada para mandar la señal del número telefónico al que queremos contactar mediante cambios de frecuencia del voltaje.
MAU	Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él asigna quién tiene el Token Passing o derecho de transacción.
Megabyte	MB. 1'048,576 bytes. Formalmente es 1 K de KB.
MIME	Especificación para redes y transmisiones multipunto.
MIT	Cable de par trenzado sin blindaje.
Módem	Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmitibles por vía telefónica.
Motherboard	Tarjeta principal que contiene los lugares donde se alojarán todos los dispositivos físicos de la computadora.
Multimedia	Incorporación de varios tipos de información: sonidos, textos, gráficos, video, etcétera.
Multitasking	Capacidad de un equipo de llevar más de una tarea a la vez.
NetBios	Interface estándar para procesos de red. Son los servidores de software y firmware entre la tarjeta y las aplicaciones.
NFS	Sistema de archivos de red. Genéricamente es un sistema que permite el acceso a un servidor de archivos.
Nodo	Estación de trabajo con identificación propia que puede ser fuente y destino en la red.
OSI	Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.
Output	Salida de datos se llama a los procesos de una computadora que entregan datos a otro dispositivo o directamente al usuario.
Packet	Unidad de información a transmitir. No contiene dirección ni destino, tan sólo ruta (el siguiente punto a llegar).

Partición	Porción específica de un dispositivo dedicado a una determinada tarea y que está organizada como una sola unidad lógica.
Patch Panel	entro de empalme. Lugar donde llegan todos los cableados para conexión a la infraestructura de red.
Path	Nombre asignado a la variable que nos indica las rutas lógicas de los datos.
PBX	Comúnmente llamado conmutador, es el sistema de intercambio de líneas telefónicas.
PC cards	Dispositivos periféricos que agregan una amplia variedad de posibilidades a las computadoras: almacenamiento, memoria, manejo de periféricos, fax, red, comunicaciones, etc. Existen tres tipos de acuerdo a su tamaño.
PCI	Estándar de bus para periféricos que típicamente utiliza DMS tipo F y Fast IO bidireccional. Desarrollado por Intel.
PCMCIA	Estándar de bus para tarjetas periféricas de computadoras portátiles.
PDN	Redes públicas de conmutación de paquetes.
Peer-to-peer	Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.
Ping	Transmisión de datos de prueba para verificar la integridad de la comunicación entre dos sistemas.
Propietario	Término utilizado en computación para decir que la tecnología utilizada es desarrollada por la marca propia y no es similar a los estándares.
Protocolo	Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.
Queue	Fila de espera. Grupo de procesos por realizar.
RAID	Arreglo de discos redundante. Juego de discos armado para aumentar la velocidad de lectura/escritura y seguridad de la información. Existen 5 niveles, desde la copia espejo hasta la escritura paralela con redundancia.
RAM	Memoria de lectura y escritura.
RAS	Servicio de acceso remoto a la red.
RDI	Red digital de servicios integrados. Clase de servicios para transmitir varios tipos de información, texto, imágenes, sonido, etcétera, mediante la red pública.
Repetidor	Dispositivo que transmite y amplifica la señal de la red.
RG11	Cable coaxial grueso usado en Ethernet.
RG58	Cable coaxial delgado de 50 ohms usado en Ethernet.
RG62	Cable coaxial delgado de 62 ohms usado en ARCNet.
RJ11	Conector para MIT 2 pares.
RJ45	Conector para MIT 4 pares.
ROM	Memoria de sólo lectura.
Router	Ruteador. Dispositivo que pasa todos los mensajes entre una red y otra distinguiendo a qué red pertenece el destino del mensaje.
RS232	Interface serial entre DTE y DCE.
SAA	Enfocado a dar conectividad y migración entre sistemas de las aplicaciones.
SAC	Concentrador que en una red FDDI tiene conexión de círculo.
SCSI	Estándar desarrollado para conectar dispositivos periféricos y a microcomputadoras con una velocidad máxima de 5 Mbps. Utiliza cable de 50 hilos.
SDH	El equivalente del comité CCITT para redes ópticas.
SDLC	Estándar en las arquitecturas SNA para transmisiones punto a punto.
Seek time	Tiempo de búsqueda. Intervalo entre la activación de la señal y la llegada de la cabeza al sector.
Servidor	Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.
Shareware	Software de disponibilidad y evaluación total que se puede encontrar sin costo en la red o en cualquier otro sitio. El pago por dicho software se realiza cuando el programa ha sido evaluado durante un tiempo razonable y el usuario decide utilizarlo de forma permanente. Este sistema se basa en la buena fe del usuario que responsablemente registra su software con su autor sin responsabilidad para el distribuidor del mismo.
Síncronia	Forma de transmisión de datos donde se necesita señal adicional de reloj para que el transmisor y el receptor funcionen a la misma velocidad.

SLIP	Protocolo para TCP/IP vía serial.
SNA	Arquitectura de protocolos para redes.
SNMP	Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.
SPX	Trabaja en el cuarto nivel de OSI. Brinda apoyo a IPX garantizando la llegada y controlando las secuencias.
SQL	El lenguaje de consulta a la base de datos cliente/servidor más conocido.
STP	Cable de par trenzado con blindaje o aislamiento magnético.
Supervisor	Usuario de la red con autoridad para realizar las tareas de alto nivel de cliente-servidor. Tiene acceso y control total de todos los recursos de la red. Algunos otros sistemas también lo llaman administrador.
T3	Servicio de transmisión de datos que opera a 45 Mbps.
TCP/IP	Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.
TELNET	Utilería de TCP/IP que permite un logon remoto sobre un host.
Terminador	Componente del cableado que empata la impedancia característica del cable para regular las señales eléctricas en la red.
Tiempo de acceso	Intervalo entre el tiempo de una solicitud de datos por el sistema y el tiempo en que el dispositivo los tiene disponibles.
Token Passing	Estafeta. Método de comunicación en red en el que cada elemento debe recibir el permiso para hablar o la estafeta.
Token Ring	Red local en la que el permiso para transmitir es secuencial o en anillo.
Topología	Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.
TP	Cable de pares trenzados.
Transfer rate	Promedio de datos que son enviados y recibidos por un disco duro.
Transciever	Dispositivo de Ethernet que permite el cambio de medio físico a cable.
UPS	Fuente de poder que se activa cuando la señal de corriente alterna se pierde para evitar que los servidores se apagen de manera abrupta.
Usuario	Persona que trabaja con la estación de trabajo. El que realiza tareas de acceso a los recursos de la red pero no los modifica sustancialmente. Tiene derechos de uso pero no de mantenimiento mayor.
Virtual Circuit	Conexión lograda vía programación que se comporta como si existiera conexión física directa.
WACK	Describe el estado de espera hasta que se recibe confirmación de que la transmisión se realizó con éxito.
WAN	Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.
WEB site de WWW	Servidores de internet que contienen la información disponible para los usuarios de esa red.
X.21	Protocolo usado en las redes telefónicas digitales para voz y datos en transmisión síncrona Full Duplex.
X.25	Protocolo para red de paquetes conmutados. Generalmente se incluyen los protocolos X.3 y X.28 en estas redes.
X.28	Estándar para la forma en que las terminales asíncronas tienen acceso a los paquetes de la red y sus comandos.
X.3	Estándar de comunicaciones ANSI.