UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"DISEÑO E IMPLANTACION DE REDES VIRTUALES PRIVADAS SEGURAS ORIENTADAS A LA PEQUEÑA Y MEDIANA EMPRESA"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

I N G E N I E R O E N C O M P U T A C I O N

P R E S E N T A N:

PAOLA SORIA PALMA

EVA IRENE RAMIREZ DELGADO

DIRECTOR DE TESIS: M EN C. MA. JAQUELINA LOPEZ BARRIENTOS

México, D.F. **OCTUBRE 2005**

A quienes marcaron mi vida

DON "LUPE" por enseñarme lo que se puede lograr con fortaleza y a ser el mejor en lo que hagas no importa lo que sea.

GERMÁN por enseñarme lo que es luchar en la vida, a quererla, respetarla y a ser feliz. Por heredarme la risa en cada momento y saber que nunca aprendes suficiente. Sobre todo por apoyarme a llegar hasta donde estoy ahora.

"Si tocan mi cuerpo y está frío es porque mi corazón está muerto y mi corazón eres tú"

Les agradezco haberme hecho en todos sentidos una mejor persona. Todos los días en mi corazón y mi mente.

A mis padres

Sin ustedes no sería lo que soy, gracias por el amor que transformaron en esfuerzo, paciencia y dedicación.

A mi hermano

Porque aprendimos juntos a superarnos, molestarnos y con todo y todo a querernos. Creo que está demás saber que siempre contaremos el uno con el otro.

A mis amigos

Miguel Ángel T., Ilse, Lizbeth, Fernando, Daniel, Miguel Angel G., Martín, Maru, Ulises, Iliana por compartir tantos momentos importantes y estar siempre cerca cuando los necesité.

A mi abuela

El mejor ejemplo de lo que significa disfrutar la vida y ser feliz con todos y cada uno de sus hijos, nietos, bisnietos y agregados.

A DIOS

Por dejar que tenga a tantas personas a las cuales agradecer. Y tantas œosas por las cuales ser feliz y estar agradecida.

Paola

Jaqui,

Gracias por todo tu apoyo y preocupación por nosotras, no sólo como estudiantes si no como amigas.

Eva y Paola

INDICE

PRÓLOGO

Las Pequeñas y Medianas Empresas (PyMEs) se han convertido en verdaderas protagonistas de la economía de nuestro país y han captado un gran interés por parte de diferentes grupos y la razón es sencilla: según datos de la Secretaría de Economía (Censo Económico 1999), el 99% de las empresas mexicanas son Pequeñas y Medianas Empresas, PyMEs (incluidas las microempresas), y ocupan el 64% del personal de la planta productiva del país, por lo tanto, son el gran sustento económico de las familias mexicanas. (Tabla 1)

Composición por tamaño y sector (participación porcentual)				
Tamaño	Sector			Total
	Industria	Comercio	Servicios*	2,844,308
Micro	94.4	94.9	97.4	95.7
Pequeña	3.7	4.0	1.6	3.1
Mediana	1.7	0.9	0.5	0.9
Grandes	0.4	0.2	0.4	0.3
Total	100	100	100	100

Tabla 1
*** Servicios Privados No Financieros**
Fuente: Censo Económico 1999

Una de las características de las PyMEs es que buscan soluciones prácticas. Una realidad es que muchas empresas de este sector no tienen un área de Sistemas o de Tecnología de Información, por lo tanto, el sector no solo busca precio y financiamiento, sino sencillez y soluciones rápidas de implantar. Aún dentro de las mismas PyMEs hay grandes diferencias y es

muy difícil llegar a las empresas más pequeñas. Ellas necesitan soluciones orientadas al negocio y sobre todo muy orientadas a las ventas, por lo que para este segmento es necesario ampliar su región y su mercado, solo que este tipo de empresas no requiere incrementar su infraestructura sino hacer más eficiente el manejo de su información de manera que les permita incrementar sus ventas, por ende sus ganancias y solidificarse en el mercado.

Podemos afirmar que las PYME's son técnicamente muy capaces para generar un producto o servicio y hacerlo llegar a los clientes, pero administrativamente son deficientes en el manejo de sus recursos. Según comenta Juan Bueno Torio Subsecretario para la pequeña y mediana empresa de la Secretaría de Economía (Censo Económico 1999) "el 35% de los problemas de una PYME es la necesidad de crédito, pero el otro 65% es administración".

Sabemos de la importancia de los recursos económicos, materiales y humanos, pero existe un nuevo recurso que da soporte operacional a la organización y que ha tomado relevancia en este mundo globalizado y competitivo, es el Recurso Información, de manera que si se administran todos los recursos "tradicionales" de la empresa por qué no administrar la información, la cual se ha convertido en el recurso más valioso de cualquier empresa.

La Tecnología de información es una herramienta de la ciencia de la informática capaz de realizar tareas como almacenar, procesar y transformar datos de las actividades operativas de su empresa, mediante el uso de equipo de cómputo; es importante comentar que día con día el precio de las computadoras ya está al alcance de la mayoría de las empresas. Por lo tanto la pregunta sería: ¿Aplica el empresario Tecnología de Información para administrar su empresa?

Administrando la tecnología de información obtendremos como resultado un recurso confiable, verás y oportuno (el Recurso Información) que nos permitirá administrar eficientemente los recursos tradicionales para lograr modernizar operaciones, reducir tiempos, disminuir desperdicios, podremos aumentar nuestro nivel de calidad y hasta obtener ventajas competitivas que nos diferencien de las empresas del ramo.

Es conocido que en la mayoría de las empresas ya se cuentan con equipos de cómputo y diferentes tecnologías al servicio de la administración, y que se han hecho importantes inversiones en tecnología.

También es una realidad que la mayoría de las PyME'S en México carecen de una estructura organizacional formal e incluso no tienen personal capacitado para esta labor tan específica, entonces es necesario contratar o asesorarse de personal consultor externo a la empresa que conocen por completo las aplicaciones de estas tecnologías disponibles. Una opción atractiva para las empresas que no tengan mucho presupuesto, es acercarse a las universidades, que por lo general, poseen programas de vinculación dedicados a la formación de egresados en estas áreas de conocimientos y que puedan apoyar el desarrollo de las organizaciones que lo necesiten a costos realmente accesibles.

Una empresa que logre llevar a cabo una administración eficiente de la Tecnología de Información obtendrá a cambio un buen desempeño, logrando incrementar la productividad, alcanzando los objetivos gerenciales de la organización que son el fin o la razón de ser y existir de las instituciones.

La ventaja competitiva que ofrece la tecnología de información es una necesidad para las PyME's; para poder sobrevivir en un ambiente empresarial deben integrar la tecnología de información en la organización, de forma tal, que produzca un control administrativo sobre los demás recursos de la empresa.

Al final, la Tecnología de Información no solo permite a las PyME's que sus productos y servicios lleguen al cliente, si no que además, obtendrán una mejor administración de todas las funciones básicas de su empresa, lograrán un incremento en la productividad, mejorarán las relaciones con los clientes y proveedores, incrementando las utilidades y por último, permitirá tomar y aplicar las decisiones necesarias para mejorar al máximo las relaciones dentro de la organización y poder cumplir las metas establecidas.

La nueva economía exige, no como un lujo sino como una necesidad, una cobertura global entre oficinas centrales y remotas. Sin embargo, debido a lo costoso que resulta diseñar, mantener y dar seguridad a una red de datos privada para estandarizar procedimientos internos, en la mayoría de las empresas esta opción es para reconsiderarse.

La tecnología de Internet actualmente facilita la posibilidad de construir una Red Privada Virtual. Hoy en día, utilizando ambas, se puede contar con la funcionalidad y seguridad de una red dedicada a un menor costo. Además la tasa de crecimiento de la VPN es importante en el sentido de que seguirá la rapidez de difusión de Internet.

El aspecto más importante a comprender acerca de la tecnología VPN es que se trata de una estructura, no de una entidad en sí misma. Es la estructura donde el cifrado, la autenticación y la confidencialidad pueden coexistir.

La seguridad en la VPN es esencial. La tecnología VPN cambia las reglas cuando se trata de pensar sobre la seguridad de su compañía, propone transmitir datos hacia Internet impidiendo que alguien los altere. También puede abrir un agujero en su red (por ejemplo, para tráfico de correo) asegurando que nadie entre a través de ese agujero sin la autorización adecuada.

Las Redes Privadas Virtuales son una de esas tecnologías que no se está seguro de donde vinieron, pero una vez que se establecen en la estructura de una compañía, uno se pregunta cómo se pudo haber trabajado sin ellas; la razón más importante es que existe una carencia de información y recursos claros para comprender todas las piezas que se agrupan para hacerla funcionar.

Objetivos

- Definir las bases para lograr una Infraestructura confiable.
- Método para lograr la transferencia segura de información.
- Acceso y procesamiento remoto de la información corporativa.
- Acceso remoto a bases de datos.
- Plantear soluciones para lograr la interconexión total de las diferentes oficinas separadas Geográficamente de una empresa, de forma segura a través de una infraestructura pública.

- Buscar la adaptación de nuevas tecnologías.

Metodología

Se configurará una red WAN (Wide Area Network o Red de Área Extensa) que atraviese la red Internet ya existente, lo que permitirá reducir los costos de mantenimiento al utilizarse sólo una conexión WAN en lugar de dos conexiones distintas. Pero no sólo es posible utilizar una red WAN a través de otra, sino que, además, es posible hacerlo de forma segura para salvaguardar la integridad de los datos que se transmitan ya que éstos son encriptados al pasar por los segmentos públicos. La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN, crea un pasillo privado a través de Internet y consigue reducir las responsabilidades de gestión de una red local.

Ante todo lo que se pretende es proporcionar al lector las bases para configurar una red segura. Sabemos que el activo más importante para una organización cualquiera que sea su tamaño es la información por lo que es importante protegerla. Los parámetros de seguridad para los túneles individuales se pueden negociar entre sitios no homogéneos para alcanzar niveles altos de seguridad. Con la seguridad que se implementará:

- No disminuye el desempeño de las redes.
- La VPN dará confiabilidad a los usuarios y garantizará transacciones de índole privado.
- Instalando la VPN, se conseguirá reducir las responsabilidades de gestión de una red local.

Resultados Esperados

Proporcionarle a la PyME un ejemplo de herramienta y una metodología para útil y confiable que permita a los empresarios realizar una administración segura de su información que además fortalezca sus tomas de decisiones; asimismo Un importante ahorro económico, debido a la reducción de los costos de telecomunicación, puesto que el pequeño empresario podrá transportar de forma simultanea, el flujo de información de varias aplicaciones y comunicaciones, utilizando unos recursos de red únicos

Optimización de la red. El diseño de la misma se hará en función de las auténticas necesidades del cliente y tras un detallado análisis de las mismas.

Transparencia. El usuario tiene un control completo del proceso de transferencia de la información a través de la estructura de la red. La implantación de una VPN supone adquirir ventajas de diversidad ya que las empresas además de la interconexión LAN, tendrán acceso a otros servicios de valor añadido como puede ser la conexión a las vías de información, Internet o conexiones de datos y voz.

Y por supuesto cumplir con los objetivos planteados.

1 ANTECEDENTES DE SEGURIDAD

1.1 Seguridad Informática

1.1.1 Definición de Seguridad Informática

La definición de la seguridad informática es lograr adquirir, almacenar, procesar y transmitir información en un entorno preservando lo más que se pueda los servicios de seguridad.

La seguridad tiene como objetivos principales lograr la confidencialidad (la información sólo la conocen quienes tienen derecho a ello), integridad (la información no es alterada sin autorización), autenticidad de la información (la información proviene de fuentes autorizadas) y garantizar la disponibilidad de la misma y de los recursos de cómputo (sólo los usuarios legítimos puedan usar la información en el momento que se requiera). Estos objetivos pueden traslaparse o pueden ser mutuamente exclusivos. Por ejemplo, requerimientos fuertes de confidencialidad pueden restringir severamente la disponibilidad.

En general, la seguridad de un sistema tiene que ver con cualquier técnica, procedimiento o medida que reduce la vulnerabilidad del sistema. Otra forma de expresarlo es todo aquello que permite defenderse de una amenaza. Se considera que algo es o está seguro si ninguna amenaza se cierne sobre ello o bien el riesgo de que las existentes lleguen a materializarse es despreciable, lo cual pocas veces se podrá afirmar de forma tajante, sea cual sea la naturaleza de lo que se esté hablando.

La seguridad informática abarca la seguridad en redes, la seguridad de las computadoras, la seguridad de aplicaciones, seguridad de datos, la seguridad de acceso y la seguridad física, entre otras.

Asimismo, es necesario tener presente que la seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas, como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad o auditoría de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto a otra.

En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión, la complejidad organizativa o el volumen de la entidad así lo demandan.

Debe existir una definición de funciones y una separación suficiente de tareas respecto a la seguridad física, como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego y el agua, y otras similares.

La llamada seguridad lógica, como el control de accesos a la información exige la identificación y autenticación del usuario, o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida por línea. Puede haber cifrado de la información por dispositivos físicos o a través de programas, y en casos más críticos existen los dos niveles.

Para valorar las necesidades de seguridad de una organización de forma efectiva y para evaluar y elegir varios productos de seguridad y las políticas, el administrador responsable de la seguridad necesita algunos métodos sistemáticos para definir los requerimientos de seguridad y clasificar el enfoque de seguridad para cumplir con los requerimientos. Se deben considerar tres puntos clave en la seguridad informática.

Ataque de seguridad: Cualquier acción que comprometa la seguridad de la información que posee una organización.

Mecanismo de seguridad: Un mecanismo de seguridad está diseñado para detectar, prevenir y recobrarse de un ataque de seguridad.

Servicio de seguridad: Un servicio que mejora la seguridad del procesamiento de datos y transferencia de información en sistemas de procesamiento de una organización.

El mundo de la seguridad connota protección contra ataques malintencionados por parte de intrusos, pero también involucra controlar los efectos producidos por errores y fallas de los equipos.

Las medidas de seguridad deben entenderse de la misma forma como se entiende la utilización de candados en las puertas de las casas de la gente honesta.

1.1.2 Servicios de Seguridad Informática

Los servicios de seguridad fueron creados para alcanzar los objetivos de seguridad, los cuales definen objetivos específicos a ser implementados a través de *mecanismos de seguridad*. Estos mecanismos consisten en alguna funcionalidad específica para algún servicio de seguridad.

La arquitectura de seguridad OSI (Estándares ISO 7498-2 y ITU-T X.800) identifica cinco clases de servicios de seguridad*: confidencialidad, autenticación, integridad, control de acceso y no repudio.* Del mismo modo, esta arquitectura, hace distinción entre los conceptos de servicio y mecanismo de seguridad.

"Un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad. Un mecanismo de seguridad es un procedimiento concreto utilizado para implementar el servicio de seguridad"

En otras palabras, un servicio de seguridad identifica lo que es requerido; mientras que el mecanismo describe *cómo* lograrlo.

Hay un servicio de seguridad que no está considerado en las normas de ISO y es la disponibilidad, sin embargo es tratada por varios autores. Esto se debe a que es un tema complejo y se aplica tanto a datos como a recursos. Algunos conceptos asociados a disponibilidad son: presencia de datos y recursos en forma usable, capacidad de responder a necesidades, respuesta en tiempo.

Los objetivos de la disponibilidad de datos y de recursos son: respuesta puntual, asignación justa, tolerancia a fallas, utilidad, concurrencia controlada (soporte para acceso simultáneo, manejo de abrazos mortales, y acceso exclusivo cuando se requiera).

A continuación se definen los servicios de seguridad definidos por los estándares de ISO.

1.1.2.1 *Confidencialidad*

El servicio que mejor se entiende es la confidencialidad, pues se refiere a permitir acceso a los activos de la empresa y sólo a partes autorizadas. No obstante, existen problemas tales como: ¿quién debe determinar quien está autorizado y quién no? y ¿a qué está autorizado y a qué no? En cuanto a este tema deberán establecerse los criterios en lo que más adelante se definirá como política de seguridad informática (PSI). En algunos contextos este servicio se conoce también como privacidad.

Este servicio, y su implementación, constituyen uno de los principales objetivos de la seguridad informática, resultado de las técnicas más ancestrales de ocultamiento de información.

Actualmente, una de las técnicas más importantes para implementar este servicio es la criptografía.

El modelo OSI identifica los siguientes tipos de servicios de confidencialidad:

1. *Confidencialidad orientada a conexión.* Proporcionan confidencialidad a todos los datos transmitidos durante una conexión.

2. *Confidencialidad no orientada a conexión.* Proporcionan confidencialidad de unidades simples de datos.

3. *Confidencialidad de campo selectivo.* Proporcionan confidencialidad de campos específicos de los datos durante una conexión, o para una unidad de datos.

4. *Confidencialidad de flujo de tráfico (protección contra análisis de tráfico).* Proporcionan protección de información que de otra forma podría resultar comprometida u obtenida indirectamente mediante un análisis de tráfico.

1.1.2.2 *Autenticación*

Este servicio consiste en garantizar que las partes o entidades participantes en una comunicación sean las que dicen ser. Es decir, consiste básicamente en el proceso de identificación de una parte ante las demás, de una manera incontroversial y demostrable.

Estrictamente hablando existen dos tipos de autenticación: *autenticación de identidad o identificación, y autenticación de origen de datos*. Este último tipo de autenticación se refiere a la certeza de que los datos hayan salido de donde se supone deben haber salido y no exista la posibilidad de haber suplantado el origen y que en realidad los datos tengan un origen distinto al supuesto.

La autenticación, entendida como proceso de *identificación* clasifica en tres tipos, de acuerdo a la naturaleza de los elementos en que se basa su implementación:

i) En algo que se sabe

ii) En algo que se tiene

iii) En algo que se es

En el primer caso la autenticación puede basarse en algo que se aprende o memoriza, tal como una contraseña, palabra clave o comúnmente una clave confidencial llamada password. Al ser revelado ante la entidad con la que desea identificarse, se demuestra ser quien se dice ser.

En el segundo caso, la autenticación se basa en algo que se posee tal como una moneda, una llave física (metal), o cualquier otro objeto tangible como puede ser una tarjeta con banda magnética en la cual está contenida la clave.

En el tercer caso, la identidad se demuestra comparando patrones relacionados a alguna característica inherente a la naturaleza de la entidad que se identifica. Si se trata de una persona, una característica inherente a su naturaleza podría ser sus huellas digitales, su voz, etc. Este tipo de autenticación también se conoce como *biométrica*.

También la autenticación puede ser *directa* o *indirecta*. Es directa si en el proceso de autenticación sólo intervienen las partes interesadas que se van a autenticar. Es decir, no interviene ninguna tercera parte actuando como juez. Es indirecta si en el proceso interviene una tercera parte confiable que actúa como autoridad o juez que avala la identidad de las partes.

Además puede ser *unidireccional* o *mutua*. Es unidireccional si basta que una de las partes se autentique ante la otra. Es mutua cuando se requiere que ambas partes se autentiquen entre sí.

Como se mencionó anteriormente, la arquitectura OSI reconoce dos servicios de autenticación. Y proporcionan autenticación en el proceso de comunicación entre dos entidades o para autenticar el origen de datos.

1. *Los servicios de autenticación de entidades parejas* sirve para proporcionar la capacidad de verificar que la entidad pareja de una asociación es quien dice ser. En concreto, el servicio de autenticación de entidades parejas permite asegurarse de que una determinada entidad no está intentando realizar una suplantación o réplica no autorizada de una asociación anterior. La autenticación de entidades parejas se realiza típicamente durante la fase de establecimiento de la conexión o. en ocasiones, durante la fase de transferencia de datos.

2. *El servicio de autenticación del origen de los datos* permite reclamar el origen de las fuentes de los datos recibidos. Sin embargo, el servicio de autenticación del origen de los datos no proporciona protección contra la duplicación o la modificación de unidades de datos. En este caso, debe utilizarse conjuntamente un servicio de integridad de los datos. La autenticación del origen de los datos se realiza generalmente durante la fase de transferencia de datos.

Los servicios de autenticación son importantes, ya que se requieren para las tareas de autorización y contabilidad. La autorización se refiere al proceso de concesión de derechos, lo que incluye la concesión del acceso basada en los derechos de acceso. La contabilidad se refiere

a la propiedad que asegura que las acciones de una entidad guardarán el rastro sólo para esa entidad.

El servicio de autenticación está íntimamente relacionado al de control de acceso y algunas de las principales técnicas de no repudio.

1.1.2.3 *Integridad*

Este servicio protege los activos del sistema contra modificaciones, alteraciones, borrado, inserción y en general, contra todo tipo de acción que atente contra la integridad de los activos. Este concepto de integridad es difícil porque puede significar cosas distintas dependiendo del contexto. Algunos de estos significados distintos pueden ser: precisión, exactitud, inalterabilidad, modificación sólo en modos aceptables, modificación sólo por partes o procesos autorizados, consistencia, resultados significativos y correctos, etc.

Es común reconocer tres aspectos de la integridad: acciones autorizadas, separación y protección de recursos, detección y corrección de errores.

La arquitectura OSI identifica los siguientes servicios de integridad:

1. *Integridad orientada a conexión con recuperación.* Proporcionan integridad a los datos durante una conexión. Si es posible, permiten la recuperación de fallos de integridad.

2. *Integridad orientada a conexión sin recuperación.* Proporcionan integridad a los datos durante una conexión. No se recuperan los fallos de integridad.

3. *Integridad de campo seleccionado orientado a conexión.* Proporcionan integridad de campos específicos en los datos durante la conexión.

4. *Integridad no orientada a conexión.* Proporcionan integridad a las unidades de datos.

5. *Integridad sin conexión de campo seleccionado.* Proporcionan integridad de campos específicos dentro de las unidades de datos.

La manera en que este servicio de seguridad se implementa normalmente es a través de funciones hash o funciones de dispersión, un tipo de criptografía que no utiliza llaves.

Al realizar una conexión, si se utiliza un servicio de autenticación de entidad al inicio de la misma y un servicio de integridad orientado a conexión durante ésta, se puede proporcionar conjuntamente la corroboración de la fuente de todas las unidades de datos transferidas durante la conexión, la integridad de dichas unidades de datos, y adicionalmente se puede detectar la duplicación de unidades de datos, utilizando, por ejemplo, números de secuencia.

1.1.2.4 *Control de Acceso*

Este servicio protege a los activos del sistema contra accesos y usos no autorizados. Este es de los servicios que normalmente no utilizan técnicas criptográficas para su implementación; en cambio, existe un gran número de técnicas propias y tipos de control de acceso, así como también modelos específicos para su implementación.

Está cercanamente relacionado al de autenticación ya que un usuario debe ser autenticado antes de tener acceso a los activos del sistema. Por esta razón, su estudio detallado se integra con el de autenticación, en algunas de sus partes. Por ejemplo un usuario o proceso que pretenda ocupar el lugar de otro usuario se deberá autenticar antes de que un servicio de control de acceso pueda obtener acceso efectivo a un recurso del sistema.

1.1.2.5 *No Repudio*

El no repudio proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje, u originado o haber sido el destinatario de una acción. Los servicios de no repudio identificados por OSI son:

- No repudio con prueba de origen.
- No repudio con prueba de entrega.

Normalmente, para implementar este servicio se utilizan esquemas de clave pública tales como las firmas digitales, pero no se restringe a ellas; también se pueden utilizar otras técnicas de cifrado de clave pública y de clave secreta; siempre y cuando se utilice una tercera parte confiable.

1.1.3 Mecanismos de Seguridad

La arquitectura OSI de seguridad diferencia entre mecanismos de seguridad específicos y mecanismos de seguridad generalizados.

Mecanismos Específicos:

La arquitectura OSI enumera ocho mecanismos específicos de seguridad, los cuales sirven para atender específicamente un servicio de seguridad:

- Cifrado
- Mecanismos de Firma digital

- Mecanismos de Control de acceso
- Mecanismos de Integridad de datos
- Mecanismos de relleno del tráfico, Traffic padding (Protección contra análisis de tráfico)
- Mecanismos de intercambio de Autenticación
- Mecanismos de Control de ruteo
- Mecanismos de Certificación

1. El *cifrado* se utiliza para proteger la confidencialidad de las unidades de datos y la información de flujo de tráfico, o para dar soporte o complementar otros mecanismos de seguridad.

2. Los *mecanismos de firma digital* se utilizan para proporcionar una analogía electrónica a la firma manuscrita en los documentos electrónicos. De forma similar a las firmas tradicionales, las firmas digitales no deben ser clasificables, los receptores deben ser capaces de verificarlas, y el firmante no debe poder rechazarlas posteriormente.

3. Los *mecanismos de control de acceso* son las identidades autenticadas de las entidades involucradas, información sobre dichas entidades o capacidades de determinar y reforzar los derechos de acceso. Si una entidad intenta utilizar un recurso no autorizado o un recurso autorizado con un mecanismo impropio de acceso, la función de control de acceso rechazará el intento y podrá, además, informar del incidente con el propósito de generar una alarma y guardarla como parte los informes de auditoría sobre seguridad.

4. Los *mecanismos de integridad de datos* protegen la integridad de unidades de datos y de campos dentro de la misma, así como de secuencias de unidades de datos y campos dentro de dichas secuencias. En general, los mecanismos de integridad de datos no protegen de ataques tipo réplica. La protección de la integridad de una secuencia de unidades de datos y de campos dentro de la misma requiere habitualmente algún tipo de ordenación explícita, como numeración en secuencia, marcado temporal o encadenamiento criptográfico.

5. Los *mecanismos de protección de relleno del tráfico* se utilizan para la protección contra ataques de análisis de tráfico. El término relleno del tráfico se refiere a la generación de ejercicios de comunicación ilícitos, unidades de datos ilícitas y datos ilícitos dentro de dichas unidades. El objetivo es no revelar si los datos que se están transmitiendo representan y codifican realmente la información. En consecuencia, los mecanismos de relleno de tráfico sólo serán efectivos si son protegidos por un servicio de confidencialidad de datos.

6. Los *mecanismos de intercambio de autenticación* se utilizan para verificar la supuesta identidad de los principales. Se dice que un mecanismo de este tipo es fuerte si se basa en el uso de técnicas criptográficas para proteger los mensajes que se van a intercambiar[1]

[1] ITU X.509 (ITU, 1987)

7. Los *mecanismos de control de encaminamiento* (ruteo) se pueden utilizar para la selección dinámica o preestablecida de rutas específicas para la transmisión de los datos. Los sistemas de comunicaciones que detectan de forma persistentes ataques activos o pasivos pueden indicar al proveedor de servicio de red que desean establecer una conexión por una ruta diferente. De forma similar, el transporte de datos de cierto nivel de seguridad puede estar prohibido por la política de seguridad para ciertas redes, servidores de reenvío o enlaces.

8. Los *mecanismos de certificación* se pueden emplear para asegurarse de ciertas propiedades de los datos que se comunican entre dos o más entidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

Mecanismos de seguridad generalizados o penetrantes (filtros):

Los mecanismos de seguridad generalizados no son específicos de un servicio en particular, y en algunos casos pueden ser contemplados también como aspectos de la gestión de la seguridad. La importancia de estos mecanismos está en general relacionada directamente con el nivel de seguridad requerido. La arquitectura de seguridad OSI enumera cinco mecanismos de seguridad generalizados.

- Etiquetas (Niveles) de seguridad
- Funcionalidad de confianza
- Detección de evento
- Rastreo de auditoría de seguridad (Auditoría de ruta segura)
- Recuperación segura o de seguridad

1. Los recursos del sistema pueden tener asociadas *etiquetas de seguridad* (por ejemplo, para indicar niveles de sensibilidad). A menudo es necesario que los datos en tránsito lleven la etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito (por ejemplo, por el uso de una clave específica para cifrar los datos o por el contexto de los datos, como su fuente o ruta).

2. El concepto general de *funcionalidad de confianza* se puede utilizar bien para extender de otros mecanismos de seguridad o para establecer su efectividad.

3. La *detección de eventos* relevante para la seguridad se utiliza para detectar violaciones aparentes de la seguridad.

4. La *auditoría de seguridad* es la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas y procedimientos operacionales establecidos y recomendar los cambios adecuados en dichos controles, políticas y procedimientos. En consecuencia, el *rastreo de auditoría de seguridad* se refiere a los datos que se adquieren y que potencialmente facilitan las auditorías de seguridad.

5. Las *recuperaciones de seguridad* funcionan como gestores de eventos y realizan acciones de recuperación resultado de la aplicación de una serie de reglas o políticas de seguridad.

No hay que olvidar que la arquitectura de seguridad de OSI no se desarrolló para resolver una necesidad particular en la seguridad de las redes, sino para dotar a la comunidad de seguridad en redes con una terminología común que se pueda utilizar para describir y discutir sobre los problemas relacionados con la seguridad y sus correspondientes soluciones.

A continuación se presentan dos tablas, la Tabla 1.1 en la que se muestran los servicios de seguridad que se implementan en cada capa, conforme a la arquitectura definida en el modelo OSI, y la tabla 1.2 así con los mecanismos de seguridad empleados para implementar cada servicio.

Servicio de Seguridad	CAPA						
	FISICA 1	ENLACE 2	RED 3	TRANSPORTE 4	SESION 5	PRESENTACION 6	APLICACIÓN 7
Autenticación de identidad			Si	Si			SI
Autenticacion de origen			Si	Si			SI
Control de acceso			Si	Si			SI
Confidencialidad con conexión	Si	Si	Si	Si			SI
Confidencialidad sin conexión		Si	Si	Si			SI
Confidencialidad selectiva de campo							SI
Confidencialidad de flujo de tráfico	Si		SI				SI
Integridad con conexión y con recuperación				SI			SI
Integridad con conexión y sin recuperación			SI	SI			SI
Integridad con conexión selectiva de campo							SI
No repudio con prueba de origen			SI	SI			SI
No repudio con prueba de entrega							SI

Tabla 1.1
Servicios de seguridad en la capa OSI

Servicio de Seguridad	MECANISMOS							
	Cifrado	Firma Digital	Control de acceso	Integridad	Autenticación	Traffic Padding	Control de Ruteo	Notarización
Autenticación de identidad	SI	SI			SI			
Autenticacion de origen	SI	SI						
Control de acceso			SI					
Confidencialidad con o sin conexión	SI						SI	
Confidencialidad selectiva de campo	SI							
Confidencialidad de flujo de tráfico	SI					SI	SI	
Integridad con conexión con o sin recuperación	SI			SI				
Integridad con conexión selectiva de campo	SI			SI				
Integridad sin conexión	SI	SI		SI				
Integridad sin conexión y selección de campo	SI	SI		SI				

Tabla 1.2
Mecanismos asociados a los servicios de seguridad

No hay un solo mecanismo que provea todos los servicios de seguridad antes mencionados. Sin embargo, como podemos notar hay un mecanismo que sustenta la mayoría de de los mecanismos de seguridad que haya actualmente en uso y son las técnicas criptográficas.

1.1.4 Importancia de la Seguridad Informática

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de la tecnología informática disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados, por lo que se considera que

"La Información es el activo más importante del negocio"

Ésta es mucho más que una simple frase; es una regla básica para el buen funcionamiento de cualquier compañía. El problema es que muy pocas empresas cuentan con una política de seguridad diseñada de manera que impida al máximo posible cualquier ataque de virus, robo de datos y visitas inesperadas de hackers. De hecho, en un estudio realizado por Price Waterhouse Coopers se detectó que las empresas y organizaciones a nivel internacional reportaron pérdidas por 1.5 trillones de dólares tan sólo por el concepto de virus; además, hay análisis que enlistan, por lo menos, 30,000 sitios de hackers. Estos datos dan cuenta del peligro que corre la información de cualquier negocio.

Para tratar de asignar un valor al costo del delito electrónico podríamos mencionar además el reporte de la agencia norteamericana Defense Information Systems Agency titulado "Defending the Defense Information Infrastructure", del 9 de julio de 1996. En dicho informe las corporaciones más grandes de los Estados Unidos reportan haber experimentado pérdidas estimadas en US$ 800 millones dólares en 1996 debido a ataques a la red. Asimismo el informe de marzo de 1997 de The Computer Security Institute (CSI) indica que el crimen de cómputo continúa al alza y se reportan pérdidas superiores a los US$ 100 millones de dólares y esto es tan solo durante el primer cuarto del año 1997. Si además, tenemos en cuenta que según las estadísticas de estas agencias norteamericanas sólo 1 de cada 500 ataques son detectados y reportados, ya es posible hacerse una idea de los valores involucrados en este tipo de delito.

Por esto, y por cualquier otro tipo de consideración que se tenga en mente, es realmente válido pensar que cualquier organización que trabaje con computadoras y hoy en día más específicamente con redes de computadoras debe tener normativas que hagan referencia al uso correcto de los recursos y de los contenidos, es decir, al buen uso de la información.

Los riesgos que corre la información son básicamente su pérdida, alteración y robo. La pérdida de información es, en casi todos los casos, el problema más grave y el que afecta a todos los usuarios.

El robo de la información es un riesgo que no afecta demasiado a los usuarios particulares, pero puede tener graves consecuencias en una empresa, ante el peligro, por ejemplo de que la información de un determinado proyecto caiga en manos de la competencia.

La no disponibilidad de un sistema o parte de la información en él contenida supone, como efecto inmediato, una pérdida de tiempo que puede desembocar, por ejemplo, en la pérdida de clientes de una empresa por la demora en la entrega de trabajos. Si el sistema es un servidor

central o de red la pérdida se puede multiplicar por el número de usuarios que pierden el servicio.

Otra pregunta que podemos hacernos reflexionando sobre lo que hemos expuesto hasta ahora es: *¿Quién necesita la seguridad?*

En mayor o menor grado, todo sistema necesita seguridad, incluso la computadora particular que utilizamos en casa para escribir documentos. Al menos habrá que protegerla contra la entrada de virus y se tendrán que hacer copias de seguridad por muy poca que sea la información que se genere.

En una primera aproximación, para determinar cuál es la seguridad adecuada en un sistema habrá que estudiar cuáles son los riesgos a los que está expuesto teniendo en cuenta el valor de la información que contiene, los costos de recuperación ante un posible desastre y, por supuesto, evaluar lo que costaría la protección.

1.1.5 Dificultades de la Seguridad Informática

Algunos de los factores que intervienen en esta dificultad son los siguientes:

- La mayoría de los responsables de la empresa y los administradores ignoran el valor de sus propios recursos de cómputo.
- Temor a dañar la imagen pública.
- Las definiciones legales son vagas o inexistentes y la persecución legal es difícil.
- El criminal debe rastrearse y no se cuenta con herramientas confiables.
- Los criminales son vistos como intelectuales curiosos y no se ajustan a un estereotipo.
- Las leyes y la ética son frecuentemente poco claras.
- Los firewalls perimetrales no pueden resolver el problema de riesgos internos de seguridad.
- Las redes hospedan una cantidad cada vez mayor de valiosos activos empresariales.
- Las herramientas de los hackers y las vulnerabilidades de las redes y sistemas están disponibles en Internet.
- Suponer que los problemas desaparecerán si no se les hace caso.

- Autorizar soluciones reactivas y parches de corto plazo tales que los problemas reaparecen rápidamente, además de que no se le da seguimiento para asegurar que de verdad estén resueltos.

- No entender cuanto dinero vale la información y qué tanto depende de ella la reputación corporativa. (Dificultad en agregar un valor a un dato)

- Depender principalmente de un firewall (cortafuegos).

- No entender la relación que existe entre la seguridad y los problemas de funcionamiento. Entienden la seguridad física pero no ven las consecuencias de una mala seguridad informática.

- Designar a personas no capacitadas para mantener la seguridad y no las capacitan ni les dan tiempo para capacitarse.

Sin la cooperación de los usuarios el mejor sistema de seguridad hará aguas por más de una vía. De nada vale tener una protección por clave para el acceso al sistema si los usuarios la apuntan en una nota pegada a un lado de la computadora, o disponer de una potente aplicación para realizar las copias de seguridad si su poca amigabilidad o los insuficientes conocimientos del usuario motivan que no las haga con la frecuencia.

La formación de los usuarios es imprescindible para que las normas de seguridad se apliquen correctamente. A veces, unas pequeñas instrucciones son suficientes para que éstos puedan trabajar con una aplicación que les permita realizar copias de seguridad, sepan recuperar un archivo borrado o dañado, asignen palabras clave seguras a sus cuentas en diferentes sistemas.

Las nociones básicas evitarán pérdidas de tiempo y la idea de que cada vez que ocurre algo extraño en la computadora sea causado por virus. La formación también contribuye a evitar las pérdidas de información por errores humanos, una de las principales causas por las que éstas se producen.

Para conseguir que los usuarios cooperen es fundamental que las medidas de seguridad no supongan una molestia para ellos; de otra forma, tarde o temprano, se producirá una relajación en su aplicación. Por ello es importante que sean sencillas de aplicar y que los usuarios sean conscientes de la importancia de seguirlas y conozcan las pérdidas que se podrían producir de no hacerlo.

1.2 Seguridad en Redes

1.2.1 Definiendo seguridad en redes

Dado que se está tratando con conceptos que pueden tener múltiples interpretaciones, es importante acordar ciertos significados específicos. Por tanto, se citan algunas definiciones, todas ellas extraídas del diccionario.

- Seguridad, calidad de seguro
- Seguro, libre de riesgo.
- Información, acción y efecto de informar, conjunto de datos con significado.
- Informar, dar noticia de una cosa.
- Redes, el conjunto sistemático de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin.

Uniendo todas estas definiciones, podemos establecer qué se entiende por Seguridad en Redes, y trabajamos en definir Seguridad en Redes con los elementos de seguridad que conocemos, podemos llegar a una definición aún mas clara:

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

La seguridad en redes debe de ser considerada como una parte de la seguridad general de una empresa. El sistema de gestión de una red local de empresa puede apreciarse en función de la eficacia de su sistema de seguridad. El sistema de seguridad debe ser completo, flexible y ajustarse a las necesidades de seguridad propias de cada organización. Debe poder aplicarse tanto en las pequeñas estructuras poco afectadas por grandes métodos de seguridad, y por las empresas en las que la seguridad de la red es un elemento primordial, como la milicia y las instituciones financieras.

Los recursos de una red pueden sufrir violaciones de los derechos de acceso a partir de cualquiera de los tres componentes fundamentales de la red: el servidor, la estación de trabajo, el cableado. Un sistema de seguridad completo debe tener la capacidad de proteger a la red contra cualquier intrusión posible a partir de uno de esos tres puntos.

El nivel de protección deseado está relacionado con el valor de los recursos que se protegen, con la vulnerabilidad de esos recursos y la importancia de un posible riesgo de violación. El sistema de seguridad debe ser lo suficientemente fuerte como para disuadir el acceso de un usuario mal intencionado, y lo suficientemente flexible como para permitir una seguridad menos constrictiva en entornos menos sensibles a ese tipo de riesgo. Esto es

importante desde el punto de vista de sucursales, proveedores u oficinas centrales de una PyME ya que aún entre ellas habrá diferencias en cuanto a la seguridad de sus sistemas.

A medida que más usuarios acceden a Internet y las empresas expanden sus redes, el reto de proporcionar seguridad a las redes internas se incrementa en dificultad. Las empresas deben determinar cuáles áreas de sus redes internas deben protegerse, deben aprender cómo restringir el acceso de sus usuarios a esas áreas, y también a determinar qué tipos de servicios de red necesitan limitar para evitar posibles hoyos de seguridad.

Cuando se habla de seguridad, normalmente se piensa en asegurarse que los usuarios de una red o sistema sólo puedan realizar tareas o acciones que tienen autorizadas, qué sólo puedan obtener información que están autorizados a tener, y que no puedan causar daños a los datos, a las aplicaciones, o a la operación de la red o del sistema.

Cuando se piense en la seguridad de redes, especialmente cuando se implemente en las *Redes Virtuales Privadas, VPN* por sus siglas en inglés, se deberá revisar la estructura de Interconexión de Sistemas Abiertos (OSI). El modelo OSI se ha utilizado virtualmente en todos los sistemas de cómputo actuales. Describe la forma en que los componentes de los niveles individuales están a cargo de un conjunto específico de servicios y en el que cada nivel se ubica por encima de otro.

La seguridad en redes es un tópico bastante amplio que puede involucrar el nivel de enlace de datos, el medio, los protocolos de red, el encaminamiento de paquetes, y el nivel de aplicación.

Como se explicó en los servicios de seguridad, el modelo OSI consta de siete niveles:

1. Aplicación
2. Presentación
3. Sesión
4. Transporte
5. Red
6. Enlace de datos
7. Físico

Cada nivel es responsable de su propio conjunto de funciones individuales, por ejemplo, confiabilidad, configuración, corrección, etc. Pero en esto reside un problema de seguridad fundamental. Los ataques más comunes en la actualidad, como pueden ser las sobrecargas en la memoria intermedia (búfer), el aprovechamiento indebido de los recursos del sistema y otros ataques de seguridad, suceden a través de todos estos niveles. Cada nivel puede ser atacado y verse comprometido, por lo tanto, ¿qué hará que una red sea segura? Podríamos entonces decir, que el mecanismo de seguridad se ubique en los niveles más bajos posibles del modelo OSI.

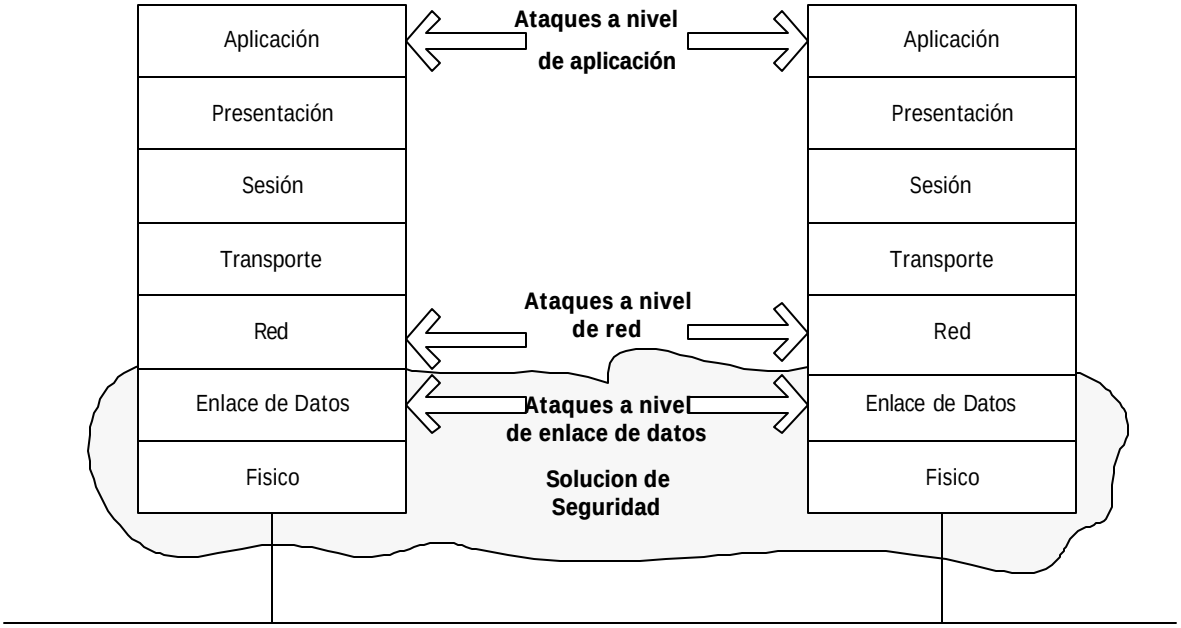


Figura 1.1
Implementación de una Solución de Seguridad en el modelo OSI

La figura 1.1 ilustra una ubicación óptima para la tecnología VPN. Esto crea un beneficio y a la vez un problema, pues a la vez que aseguramos una menor cantidad de ataques, podríamos crear problemas de compatibilidad.

1.2.2 Servicios de Seguridad en Redes

Existe confusión en cuanto a este tema. ISO lista los siguientes servicios: No Repudio, Autenticación, Confidencialidad e Integridad. Sin embargo, como se mencionó anteriormente, algunos textos incluyen también la Disponibilidad. A continuación se resumen estos servicios de seguridad desde el punto de vista de seguridad en la red.

En la tabla 1.1 y 1.2, se mostraron las capas de red donde se pueden implementar los distintos servicios de seguridad.

1.2.2.1 *Confidencialidad*

Objetivo. En el contexto de la seguridad en redes, la confidencialidad tiene como objetivo el restringir el acceso a los datos durante el tránsito o almacenamiento. Proteger la información contra la divulgación no autorizada.

Método. Los métodos para lograr confidencialidad pueden variar de acuerdo a las necesidades, la red, etc. Algunos de los más comunes son los siguientes:

- Transformar los datos en contenidos ilegibles.
  - Cifrado.
- Almacenar datos en el dominio de un solo sistema.
  - Sistemas de cómputo seguros o estados de procesador confiables.
- Uso de controles basados en etiquetas.
  - Prohibir flujo de información hacia abajo, en niveles de confidencialidad.
  - Permitir a entidades en niveles de confidencialidad alta observar información a niveles de confidencialidad baja.

Problemas. Entre los problemas a ser considerados al implementar confidencialidad en las redes están, entre otros, los siguientes:

- Administración de llaves.
  - Centros de distribución para llaves privadas.
  - Servidores de Certificados para llaves públicas.
  - Separación de cifrado de no cifrado.

1.2.2.2 *Integridad*

Objetivo. En seguridad en redes, la integridad tiene como objetivo prevenir fla modificación no autorizada de los datos, e incluye.

- Proteger la información de modificación no autorizada.
- Integridad de la información que en la transmisión de paquetes.
- Orden de paquetes en una transmisión.
- Garantizar la trasmisión de mensajes completos a los destinos deseados.

Método. Entre los métodos que se utilizan para implementar integridad, en seguridad en redes, están los siguientes

- Utilizar códigos MIC/MAC, también conocidos como candados de integridad.
- Uso de controles basados en etiquetas.
  - Derivados del modelo de integridad de Biba.

- Prohibir el flujo de información hacia arriba en niveles de integridad.
- Permitir a entidades en niveles inferiores de integridad observar información de integridad mayor.

Problemas. Entre los problemas a ser considerados al implementar la integridad en las redes están, entre otros, los siguientes:

- Administración.
  - Proteger los mecanismos que implementan integridad.
  - Determinar los atributos específicos de integridad. Ejemplos etiquetas o MIC y MAC.

1.2.2.3 *Autenticación y No repudio*

En el contexto de la seguridad en redes, estos dos servicios pueden analizarse juntos debido a su relación y cercanía en cuanto a objetivos, mecanismos, consideraciones de implementación y problemas.

Objetivo. Los objetivos de la autenticación y el no repudio son, respectivamente.

Autenticación: Garantizar la correcta autenticación de entidades activas del sistema. Prevenir la suplantación o enmascaramiento.

- Identificación de entidades
- Autenticación de origen de los datos
- Establecer el origen del mensaje (autor).

No repudio: Prevenir el repudio de eventos anteriores.

Método. Los métodos para lograr confidencialidad pueden variar de acuerdo a las necesidades, la red, etc. Algunos de los más comunes son los siguientes:

- Firmas.
- Instantáneas.

Problemas. Los problemas más importantes en la implementación de estos dos servicios son los siguientes:

- Diseño de los protocolos.
  - Los protocolos pueden ser complicados.

1.2.2.4 *Disponibilidad*

Aunque sería deseable, este servicio no se puede especificar de la misma manera precisa, global y persistente como los de políticas de confidencialidad e integridad.

Esto se debe a la subjetividad que encierran muchos de los conceptos relacionados a este servicio, entre los cuales están los siguientes.

- ¿Qué significa ejecución en progreso?
- ¿Qué significa terminación de una tarea?
- ¿Qué significa terminación exitosa?

Otra razón es que en este servicio no se pueden observar componentes individuales. Se debe examinar el sistema completo.

Otro problema es que los usuarios autorizados pueden competir por recursos del sistema. Para reducir el alcance del problema, los usuarios externos podrían excluirse total o parcialmente.

Otros problemas son:

- ¿Cómo están definidos los atributos de disponibilidad?
- ¿Cómo son asignados y revocados los atributos de disponibilidad?

En resumen, de nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de la red de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema. Para cumplir con éste último punto se crean las políticas de recuperación de desastres, que pueden incluirse en las políticas de seguridad general de seguridad estableciendo los pasos a seguir en caso de contingencia.

1.2.3 Mecanismos de Seguridad en Redes

Los mecanismos de seguridad en redes implementan los servicios de seguridad en red y usan diferentes técnicas para ello, entre las que se encuentran: cifrado, la denominada Base de red Confiable o TNB y la protección física entre otras.

La tabla 1.3 muestra una visión general de estos mecanismos de seguridad en redes en relación con los servicios que implementan.

	Cifrado	Base de Red Confiable	Protección Física
Autenticación	Sí. Valida la autenticación del demandante del servicio. Algunas veces "los certificados son producidos para demandas futuras"	Sí. Integridad obligatoria de los campos, pero la información debe estar bajo control. TNB	Sí. Debe usar técnicas de detección de errores para soportar protección física.
Control de Acceso	No. Pero puede ayudar a reforzar decisiones TCB de control de acceso	Sí. Decisiones de control de acceso basadas en etiquetas.	Uso restringido del sistema solamente para usuarios autorizados.
Confidencialidad	Sí. Semántica de datos alterados que son ilegibles.	Sí. Pero los datos deben permanecer bajo control del TNB; de otro modo, se requieren mecanismos complementarios tales como cifrado.	Separa los usuarios que deben tener acceso a la información de los que no.
Integridad	Sí. El cifrado de datos puede tener una revisión interna. El texto en claro puede tener verificación por medio de algoritmos criptográficos.	No en el caso de comunicaciones. Ejecución del modelo de integridad de Biba dentro del sistema. Cifrado para la integridad de la comunicación.	La modificación maliciosa puede evitarse combinado controles físicos y personales.

Tabla 1.3
Ejemplos de mecanismos de seguridad en redes

1.3 Políticas de Seguridad

1.3.1 Definición de Políticas de Seguridad Informática

Una Política de Seguridad es el conjunto de lineamientos que regirá el buen uso de los recursos informáticos y de cómputo de una Organización. Refleja los principales objetivos de la Organización. En ella se describen tanto los derechos como las obligaciones a que están sujetos los diferentes tipos de usuarios.

Se conoce también como política de seguridad a la descripción bajo la forma de reglas, en la que se incluyan las propiedades de confidencialidad, integridad y disponibilidad, en la medida requerida por los objetivos establecidos en la Misión de Seguridad de la Organización.

Surgen como una herramienta organizacional para hacer conciencia en cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen al desarrollo de la organización y su buen funcionamiento.

Estos lineamientos deben ser definidos de acuerdo a las normas que rigen a la Organización, tanto internas como externas (o de carácter jurídico), así como de un análisis de riesgos sobre los activos de la misma. No hay recetas mágicas, cada Organización, dependiendo de su giro y de su entorno, deberá diseñar su propia Política de Seguridad.

Una PSI es además una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de los mecanismos de seguridad, ni de una expresión legal que involucre sanciones o conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el por qué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

La meta al desarrollar una PSI es definir las expectativas de la Organización en lo que se refiere al buen uso de los recursos, y en la respuesta y prevención de incidentes. Durante este proyecto, deben considerarse diferentes aspectos de la Organización, y se deben llegar a acuerdos entre los miembros del grupo que realizará la Política.

Política de seguridad en cómputo quiere decir la documentación de las decisiones sobre seguridad de equipos de cómputo. Incluye:

- Asignación de recursos
- Resolución de objetivos competitivos
- Estrategia de la organización para proteger recursos técnicos y de información
- Guía las acciones de los empleados
- Directivas de la alta administración que establecen los objetivos de la organización y asignan responsabilidades (basadas en la misión)
- Reglas específicas para proteger sistemas específicos
- Decisiones administrativas sobre temas específicos como la confidencialidad del correo electrónico o sobre la seguridad del fax

Las políticas por si mismas no constituyen una garantía para la seguridad de la organización. Como se mencionó anteriormente deben responder a intereses y necesidades organizacionales basados en la visión del negocio, que lleven a un esfuerzo conjunto de los involucrados por administrar sus recursos y reconocer los mecanismos de seguridad informática; factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización.

1.3.2 Elementos de una Política de Seguridad Informática

Como mencionábamos en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para logra una visión conjunta y servicios informáticos críticos de la compañía.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- La responsabilidad de los administradores, proveedores y usuarios de información debe hacerse explícita (responsabilidad). Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para la configuración de seguridad de los sistemas que cobija el alcance de la política.
- Los administradores, proveedores y usuarios de información deben tener conciencia de la existencia y dimensión de las medidas de seguridad (conciencia).
- Los servicios de información y su seguridad deben prestarse en forma ética (ética).
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Los sistemas de seguridad deben adoptar un enfoque multidisciplinario (enfoques múltiples).
- Mínimo Privilegio: No asignar más privilegios a un usuario de aquellos estrictamente necesarios para realizar sus funciones.
- “Need to Know”: En ocasiones es necesario “debilitar” los controles sobre algún usuario o proceso para que pueda realizar sus funciones.
- Separación de funciones o roles: Principio fundamental para no dar demasiado poder a un usuario al asignarle muchas funciones

Resumiendo, podemos listar los puntos a considerar

1. Protección de los recursos.
2. Clasificación de recursos.

3. Separación de Funciones.
4. Lo que se necesita saber o hacer, (Need to know).
5. Monitoreo.
6. Redundancia de las herramientas.
7. Continuidad de la operación.
8. Actualización.
9. Cultura.
10. Ética.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan la comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

1.3.3 Recomendaciones para establecer PSI

Si bien las características de la PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación algunos aspectos generales recomendados para la formulación de las mismas.

- Considerar efectuar un ejercicio de análisis de riesgos informáticos, a través del cual se valoren los activos, el cual permitirá afinar las PSI de la organización.

- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones de la PSI.

- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.

- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

Como último consejo: NO SE DÉ POR HECHO ALGO AUNQUE SEA OBVIO. Haga implícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

1.3.4 Problemática en la implantación de PSI.

Muchas veces las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios resulta una labor ardua convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadotecnia de los especialistas en seguridad que llevan a los altos directivos a pensamientos como: “mas dinero para que se diviertan los de sistemas”. Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que, en muchos de los casos, lleva a comprometer su información sensible y su imagen corporativa. Además situándonos en el contexto de la pequeña y mediana empresa no se pueden invertir sumas fuertes de dinero.

Ante esta situación, los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos. En particular, la gente debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una intrusión o una simple travesura pueden convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos. Además, para que las PSI logren abrirse espacio en el interior de una organización deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

De igual forma, las PSI deben ir acompañadas de una visión de negocio que promueva actividades que involucren a las personas en sus actividades diarias, donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, sus elementos culturales y comportamientos nos debe llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación, mencionamos algunas recomendaciones para hacer conciencia sobre la importancia de la seguridad informática y el cumplimiento de las políticas:

- Desarrolle ejemplos organizacionales relacionados con fallas de seguridad que capten la atención del personal.
- Asocie el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades.
- Articule las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información. Muestre una valoración costo-beneficio, ante una falla de seguridad.
- Justifique la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

1.3.5 Posturas para definir Políticas de Seguridad Informática

- Nada está permitido (Paranoico)
- Lo que no está expresamente permitido está prohibido (Prudente)
- Lo que no está expresamente prohibido está permitido (Permisivo)
- Todo está permitido (Promiscuo)

1.4 Políticas de seguridad en Redes

En seguridad en redes, es necesario examinar las políticas y cómo serán asignadas a los componentes de red. Estas políticas deben expresarse en función de los usuarios y de la información que manejan.

En este sentido, es necesaria una política de seguridad de red sencilla y uniforme. Si existen múltiples compañías involucradas, entonces la política de seguridad necesita definirse durante las primeras etapas del proceso de desarrollo de la red.

Por ejemplo, las políticas de control de acceso deben dividirse en las correspondientes al control de acceso obligatorio y al discrecional.

1.4.1 Problemas del soporte de Políticas de Seguridad en Redes

Para el soporte de políticas de seguridad en redes se tienen que tomar en cuenta, entre otros problemas, los siguientes:

- Contar con capacidad adicional relacionada a la contabilidad individual de actividades de seguridad relevantes.
- Proporcionar ambientes para ejecución y monitoreo de las políticas de control de acceso obligatorias y discrecionales.

Dentro de este contexto, existen dos subcategorías principales.

Identificación y autenticación.- Esta subcategoría relaciona el soporte de controles de acceso obligatorio y discrecional, así como también con capacidad para autenticar identidades y acreditación. Igualmente involucra el soporte de bases para determinar los miembros de grupos.

Auditoría .- Esta subcategoría involucra los eventos relevantes de seguridad que son únicamente asociados con el usuario. También implica el mantener cuentas de usuarios para acciones de red. Deben formularse recíprocamente una serie de políticas de soporte aceptables.

1.4.2 Modelo formal de Política de Seguridad

Un modelo formal de política de seguridad es el punto de inicio de una cadena de argumentos dirigidos a incrementar la seguridad. La forma del modelo puede ser influenciada por las características técnicas del sistema a construirse.

A este respecto, se recomienda siempre buscar un parecido intuitivo con las características de sujetos, objetos y accesos de la implementación pretendida. Por cada componente de la red es necesario un monitor de referencia.

Cada monitor de referencia debe tener un modelo formal de políticas de seguridad, aunque no es necesario contar con un modelo formal de política de seguridad para todo el sistema de red. Debe haber expresión a priori de las políticas de seguridad.

1.5 Vulnerabilidades, Amenazas y Ataques

1.5.1 Conceptos

Para reducir la complejidad del tema, es necesario hacer algunas precisiones acerca de los elementos involucrados en ella.

En primer lugar, se entenderá como *sistema de cómputo* al conjunto formado por la colección de hardware, software, medios de almacenamiento, datos, datos o información y personas involucradas en el conjunto.

Se entiende como *compromiso* de seguridad a cualquier forma posible de pérdida o daño en un sistema de cómputo. De esta forma, *comprometer* la seguridad de un sistema equivale a la posibilidad de provocar pérdida o daño al sistema.

Una *vulnerabilidad* consiste en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. De esta manera, el punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.

Una *amenaza* es cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema. Ejemplos de amenazas son los ataques humanos, los desastres naturales, los errores humanos inadvertidos, fallas internas del hardware o del software, etc.

Un *ataque* consiste en cualquier acción que explota una vulnerabilidad. Existen diversos tipos de ataques. Una clasificación muy general es dividirlos en ataques *pasivos* y *activos*.

1.5.2 Clasificación de amenaza

Los principales activos o recursos que hay que proteger en un sistema de cómputo son: *hardware, software y datos.*

Existen cuatro tipos de amenazas principales a los sistemas que explotan las vulnerabilidades de los activos en el sistema. Estas amenazas son: *interrupción, intercepción, modificación y fabricación.*

Interrupción:

En el caso de una interrupción, un activo del sistema se pierde, se hace no disponible o inutilizable. Este es un ataque a la *disponibilidad*. (VER FIGURA 1.2)

Ejemplos:

- Destrucción maliciosa de un dispositivo de hardware.
- Borrado de un programa o de un archivo de datos.
- Malfuncionamiento del manejador de archivos del sistema operativo que trajera como consecuencia que no se pueda hallar un archivo particular en el disco duro.

Intercepción:

Alguna parte no autorizada logra acceso a un activo del sistema. Este es un ataque a la *confidencialidad*. La parte no autorizada puede ser una persona, un programa, o una computadora. (VER FIGURA 1.2).

Ejemplos:

- Copiado ilícito de programas o archivos de datos.
- La intervención del canal para obtener datos sobre la red.

Modificación:

Cuando una parte no autorizada además de lograr acceso al activo del sistema y manipula ese activo. Este es un ataque a la *integridad.* (VER FIGURA 1.2)

Ejemplos:

- Cambiar datos en una base de datos o en un archivo de texto.
- Alterar un programa para que realice algún proceso adicional o distinto al que realiza.
- Modificar el contenido de un mensaje que está siendo transmitido en una red.

Fabricación:

Una parte no autorizada fabricar objetos falsos y los inserta en un sistema. Este es un ataque a la *integridad*. (VER FIGURA 1.2).

Ejemplos:

- Inserción de transacciones ilegítimas en un sistema de comunicación en red.

- Agregar registros a una base datos existentes.

Para tener más claro lo anterior lo explicaremos con el siguiente algoritmo en donde hay dos grandes entidades: una que es la encargada de producir la información; la otra entidad es el consumidor de esta información y otra, llamada precisamente “otros”. Entre el productor y el consumidor, se define una relación que tiene como objetivo una transferencia de “algo” entre ambos, sin otra cosa que intervenga en el proceso. Si esto se logra llevar a cabo y se mantiene a lo largo del tiempo, se estará en presencia de un sistema seguro.

En la realidad, existen entidades y/o eventos que provocan alteraciones a este modelo. *El estudio de la seguridad, en pocas palabras, se basa en la determinación, análisis y soluciones de las alteraciones a este modelo.*

En una observación y planteamiento del modelo, determinamos que sólo existen cuatro tipos de alteraciones en la relación producción-consumidor (figura 1.2)

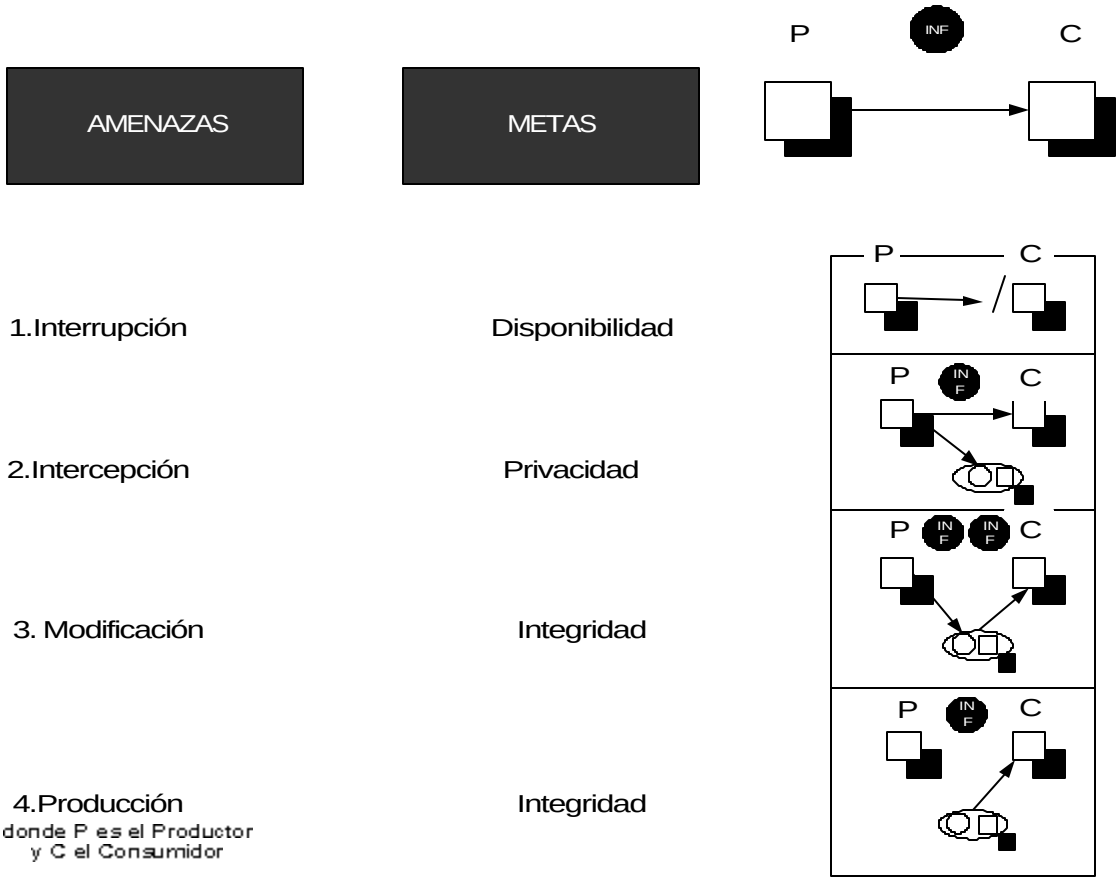


Figura 1.2
Algoritmo del productor-consumidor de información

A continuación se muestra gráficamente las amenazas y los ataques que pueden presentarse en hardware, Software y datos. (Figura 1.3).

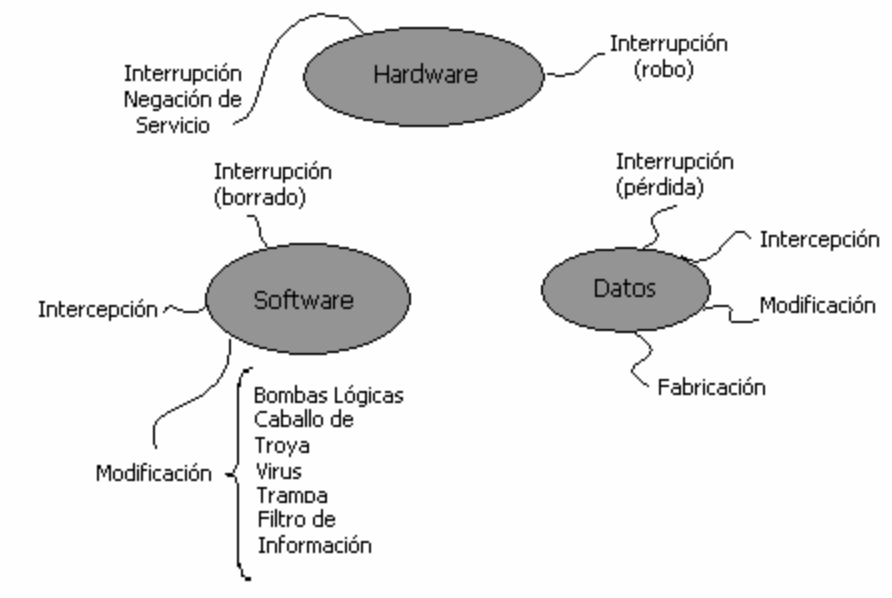


Figura 1.3
Ataques y amenazas en hw, sw y datos

1.5.3 Ataques Pasivos y Activos

Como mencionamos en el punto 1.5.1, los tipos de ataques se pueden clasificar en dos grandes grupos:

Pasivos

Observa comportamientos o lee información, sin alterar ni el estado del sistema ni la información. Sólo afecta la confidencialidad del sistema o de la información. El "atacado" no se percata de que está siendo observado. Los ataques pasivos son entonces de la naturaleza de escuchar a escondidas, monitorear transmisiones y comportamientos en la red. Hay dos subdivisiones dentro de los ataques pasivos y son (Ver figura 1.4):

1. **Liberación o bien lectura del contenido de los mensajes**. Este tipo de ataque es muy fácil de entender. Por ejemplo, una llamada telefónica, un correo electrónico o un archivo que se transfiere puede contener información confidencial o sensitiva. Lo que nos gustaría evitar es que alguien no autorizado tenga acceso a dicha información.

2. **Análisis de tráfico**. Éste segundo ataque es un poco más sutil. Supone que tenemos algún modo de enmascarar los contenidos de los mensajes o de otra información del tráfico en la

red de tal modo que el atacante, aunque haya capturado el mensaje, no puede extraer la información de dicho mensaje. La técnica común para enmascarar los contenidos es la criptografía. Si tenemos protección criptográfica, el atacante puede aún observar el patrón de los mensajes. El atacante puede determinar la localización y la identidad de los nodos y observar la frecuencia y la longitud de los mensajes que se intercambian. Esta información puede ser útil adivinando la naturaleza de la comunicación que se está llevando a cabo.

Los ataques pasivos son muy difíciles de detectar debido a que no involucran ninguna alteración a los datos. Sin embargo, es factible prevenir que estos ataques tengan éxito. Así que, el énfasis que debe hacerse sobre los ataques pasivos es en cuanto a prevención, en vez de la detección.

Activos

Estos ataques involucran modificación a la cadena de datos, la creación de una cadena falsa de datos, la modificación en general a un estado de sistema o alguna combinación de ellos.

Afecta no sólo la confidencialidad sino también la integridad y la autenticidad de la información o del sistema. El "atacado" se percata que está siendo víctima de un ataque debido a la alteración que ha sufrido su sistema o información. Está subdividido en cuatro categorías (Ver figura 1.4):

1. **Suplantación**. Este ataque toma lugar cuando una entidad pretende pasar por otra entidad distinta. Usualmente incluye alguna otra forma de ataques activos. Por ejemplo, una secuencia de autenticación puede ser capturado y repetirla después de que se haya terminado y validado correctamente. Así, se puede habilitar a una entidad que tenga pocos privilegios puede obtener privilegios extra haciéndose pasar por una entidad que si los tenga.

2. **Réplica**. Involucra el captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado.

3. **Modificación de mensajes**. Simplemente significa que algún fragmento de un mensaje legítimo es alterado, o es mensaje es retrasado o reordenado, para producir una acción no autorizada. Por ejemplo, si tenemos un mensaje que diga "Se autoriza a la persona A a leer los archivos confidenciales de contabilidad" puede ser modificado para que diga "Se autoriza a la persona B a leer los archivos confidenciales de contabilidad".

4. **Negación de servicio**. Impide o inhibe el uso normal o administración de servicios de comunicación. Este ataque puede tener un objetivo específico; por ejemplo, una entidad puede suprimir o interceptar todos los mensajes que estén dirigidos a un destinatario en especial, el servicio de auditoria de seguridad por mencionar alguno. Otra forma de negación de servicio es la interrupción en una red completa, puede ser deshabilitando la red o sobrecargando la misma con mensajes que degraden su rendimiento.

Normalmente un ataque pasivo es siempre la antesala o preparación para un ataque activo. El ataque pasivo sirve para estudiar al enemigo, conocer sus hábitos, horarios, entorno, etc. Esto muy bien se puede lograr con un buen análisis de tráfico. Una vez hecho esto, se puede montar un ataque activo.

Un ataque activo presenta características opuesta a la de los ataques pasivos. Mientras que los ataques pasivos son difíciles de detectar, como ya habíamos mencionado, y hay medidas disponibles para prevenir su triunfo; los ataques activos son muy difíciles de prevenir totalmente porque se requería hacer una protección completa de todas las facilidades y caminos de comunicaciones todo el tiempo. Es mejor detectarlos y recobrarse de cualquier interrupción o retraso que hayan causado.

A la entidad que realiza un ataque comúnmente se le conoce como atacante, intruso, enemigo, "cracker", "hacker", et.al. Esta entidad no necesariamente tiene que ser una persona; puede ser cualquier proceso, computadora, dispositivo, etc.

Cuando el atacante o enemigo es una persona o grupo de personas, en algunos medios y ámbitos también se les conoce como delincuentes o criminales informáticos o computacionales. Desde luego, llamarlos así puede ser exagerado.

Siempre se considera que en todo tipo de comunicación abierta a través de canales públicos, siempre está presente uno o varios atacantes y que estos tienen la capacidad para realizar todo lo que es posible realizar con la información en el medio de transmisión público: interceptar, leer, alterar, modificar, cambiar, fabricar, retener o reenviar información. También se asume que el atacante es capaz de interrumpir, desviar o retardar el flujo de información

En todos los casos, el objetivo de un atacante siempre es aprovechar en su favor la información, el medio, o los recursos de cómputo. Para ello también se asume que el atacante conoce, o puede conocer, la naturaleza y estructura de la información, los algoritmos de cifrado, si se usan; y, sobre todo, la implementación de ellos. Esta es una de las razones por las que la seguridad de la información no puede ni debe basarse en el ocultamiento de las herramientas de seguridad que se utilizan. Es decir, no debe utilizarse el clásico "*security by oscurity*" como premisa de seguridad, que tantas empresas de todo tipo han usado en el pasado con consecuencias siempre desastrosas.

La clasificación de los ataques ha ocupado y ocupa tratados completos y dependen siempre del sistema de cómputo, del sistema operativo, del tipo de aplicación y ambiente que se tengan, entre otros aspectos.

Siempre que se dice que una cierta herramienta es segura, hay que establecer siempre contra qué tipo de ataques es segura. Nunca se conocen, dada un sistema o aplicación, qué tipo de ataques nuevos sufrirá o será susceptible de sufrir en un futuro.

La razón de ello es que cada día surgen nuevas técnicas de ataques sobre un mismo tipo de sistema u aplicación. Y, desde luego, esto no se puede predecir. Y Debido a que no se pueden caracterizar formalmente, usando una herramienta formal, todos los posibles ataques. Si esto fuera posible, también sería posible construir una herramienta total que evitara cualquier tipo de ataque presente y futuro.

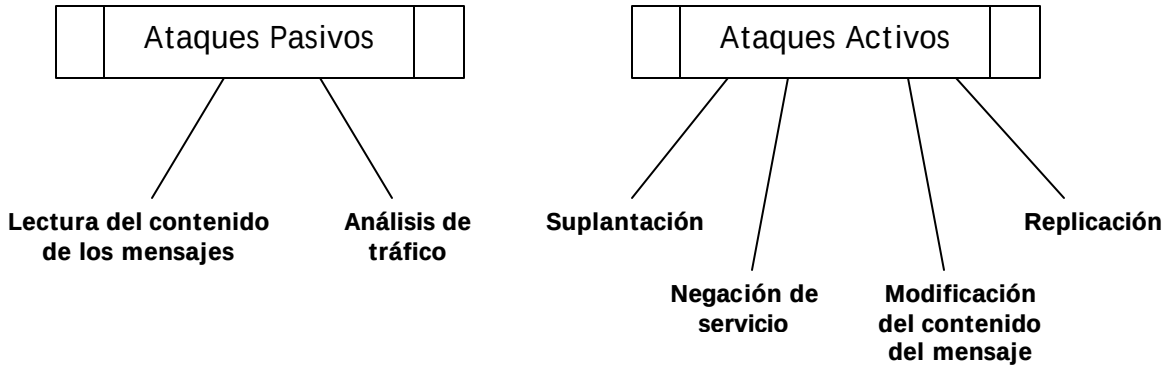


Figura 1.4.
Tipos de ataques

2 REDES VIRTUALES PRIVADAS VPN

2.1 Definición de VPN

2.1.1 Red Privada Virtual

Una VPN se puede definir a partir de las palabras: VIRTUAL y PRIVADA.

Virtual: Indica la conectividad dinámica en la red. Esta característica es debido a las necesidades de las organizaciones actuales, donde no existe un estándar en su conectividad y van creciendo incrementalmente. Este término también se puede asociar a la flexibilidad de los dispositivos que se presentan en la comunicación, adaptándose a los medios y características de transmisión que existan.

Privada: Indica la seguridad y garantía que debe tener la información que se envía por la red y la disponibilidad de ésta para los usuarios autorizados. Esta característica es un reto sobre todo cuando se habla de transmisión de datos en Internet. La privacidad es típicamente considerada como el hecho de ocultar información. La red utilizando VPN podrá ser tan segura como la red interna. La privacidad se presenta cuando un túnel aparece como un enlace privado.

En resumen, se define como:

Un proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto hacia otro de manera segura. La seguridad de los datos se logra gracias a una tecnología robusta de cifrado, y los datos que se transfieren pasan a través de una red abierta, insegura.

Esta definición revela varias cosas. Primero, un VPN es un proceso de comunicación cifrada y encapsulada. Cualquier comunicación entre dos nodos está cifrada, y es el mismo proceso de cifrado lo que garantiza la seguridad y la integridad de los datos (figura 2.1). Notará que los datos pasan a través de una red abierta

Al hablar de que pasa por una red abierta, se deja ver que es una tecnología de red que permite una extensión de la red local sobre una red pública no controlada, como por ejemplo Internet. Con una Red Privada Virtual (VPN, Virtual Private Network), los usuarios remotos que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de dicha red pública.

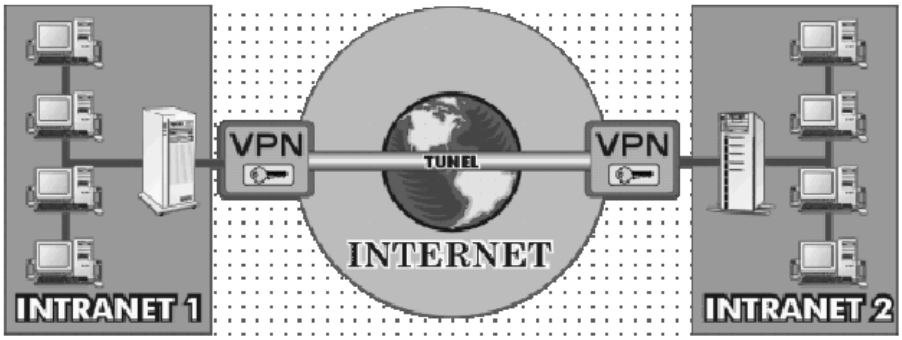


Figura 2.1
Comunicación VPN

Una Red Privada Virtual consiste en dos máquinas (una en cada "extremo" de la conexión) que están situados en diferentes localidades geográficas y una ruta o "túnel" que se crea dinámicamente en una red pública o privada y asegura la *confidencialidad* e *integridad* de los datos. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambas computadoras son encriptados por el *Point-to-Point Protocol*, también conocido como PPTP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP. Más adelante en este capítulo lo veremos más a fondo.

Una VPN está considerada como una solución punto a punto que puede ser adecuada para un amplio espectro de aplicaciones, tales como:

- Road Warrior: Usuario móvil que puede conectarse desde cualquier lugar a su red corporativa.
- Home Office: Permite a cualquier empleado trabajar desde su casa.
- Branch Office: Posibilita a un grupo de empleados trabajar desde oficinas remotas.
- Bussiness to Bussiness Partners: Para establecer e interconectar recursos de información con los principales socios comerciales de una empresa.

El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet (Branch office); también permitir a los miembros del equipo de soporte técnico la conexión desde sus casa al centro de cómputo (Home office), o que un usuario pueda acceder a su equipo hogareño desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.

Para hacer posible esta conectividad de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación.

- Autenticación y Autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados.
- Confidencialidad: Dado que los datos viajan a través de un medio hostil como Internet, los mismos son susceptibles de ser interceptados: por eso es fundamental el cifrado de los datos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.

Hay una gran variedad de redes públicas que pueden se empleadas para crear conexiones de VPN, pero la más prominente y pública de ellas, es por supuesto Internet. Debido a que Internet está en todos lados y es en donde la mayoría de las VPN actuales se están desarrollando. Por todo lo anterior vemos que es el medio mejor ubicado.

2.1.2 Ventajas y beneficios de las VPN

La información es crítica para cualquier compañía, y el no obtener esa información en el momento que se requiere puede significar perder negocios, retrasar contratos y cosas por el estilo. Por lo tanto implementar una tecnología VPN es buena idea para las organizaciones. Muchas compañías utilizan Internet para enviar correo electrónico; sin embargo la gran mayoría no toma en consideración que ese correo se envía en modo de texto y que

cualquiera que tenga acceso a Internet pueda leerlo. Además considerando que la fuerza laboral requiere de más movilidad, el costo de las líneas dedicadas sería muy alto en cuanto construcción y administración.

Una VPN tiene diferentes aplicaciones y en realidad ofrece los mismos servicios que una red tradicional. Sin embargo una VPN ofrece un servicio que una red tradicional no puede, que es la de dar un acceso remoto.

La operación de las redes virtuales privadas es transparente, práctica y sin complicaciones; adicionalmente, permite a las empresas tener disponible la información que considera crítica, sin importar el lugar donde se encuentre el usuario, accediendo a ella de una forma segura, ya que todas las transacciones, sin importar su magnitud, no podrán ser invadidas por nadie.

En la VPN se además de aprovechar la infraestructura que ya se tiene en la empresa, podemos beneficiarnos de que en Internet existen millones de clientes entre los cuales se distribuye el costo de la fibra, interruptores y encamindadores o routers. De esta forma podemos ver que los ahorros pueden ser considerables.

Desde el punto de vista económico una red virtual privada ayuda en la reducción de gastos de administración, de esta forma una empresa se ahorra en inversión de infraestructura tecnológica, administración y mantenimiento, y además, puede integrar varios servicios en un solo enlace.

Es por esto que el entusiasmo que han desarrollado las VPN es excesivo. Pues una VPN aprovecha la infraestructura existente para las conexiones, de esta forma se ahorran los costos de pagar su propia infraestructura como cable, el conducto de la fibra para unir las instalaciones y demás; tanto para los proveedores de servicio como para las empresas y es que la tecnología puede ser explotada por varios grupos de usuarios, haciendo un mejor uso de la infraestructura.

Otra importante motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto de líneas dial-up como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos:

- Se eliminan las largas distancias, mismas que son sustituidas por llamadas locales al servidor de Internet, es por esto desaparecen los pagos por concepto de enlaces dedicados para la interconexión de oficinas remotas. En los casos de accesos remotos, llamadas locales a los ISP (Internet Service Provider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización.

- En el caso de Sitio a Sitio, utilizando servicios de banda ancha para acceder a Internet, y desde Internet llegar al servidor VPN de la organización. Todo esto a un costo sensiblemente inferior al de los vínculos WAN dedicados.

Un análisis de *Data Comunications* hecho en noviembre del 2004 dice que tecnologías como frame-relay en el primer año se encuentra un 17% más abajo que una línea arrendada, pero comparado con la VPN es el doble del costo.

Las VPN también permiten:

- La administración y ampliación de la red corporativa al mejor costo-beneficio.

Otra gran característica de la tecnología VPN es su facilidad de ampliación. Conforme los proveedores de red incrementan el ancho de banda en sus backbones, las VPN pueden crecer y aprovechar este ancho de banda adicional. Además, puesto que son independientes de la plataforma y de cualquier Sistema Operativo específico, casi cualquier dispositivo de una compañía puede funcionar como cliente o como servidor de la VPN. Las VPN también dan cabida al crecimiento; muchos de sus dispositivos manejarán cualquier servicio que se coloque en ellas.

- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

Permitirán crear “túneles” o comunicaciones punto a punto con cifrado bajo demanda. Podrá crear túneles hacia otros sitios, como uno que vaya de las “oficinas centrales corporativas hasta las oficinas principales de ventas”, y más adelante crear otros túneles para otras oficinas. (figura 2.2)

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su computadora remota las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso público a Internet:

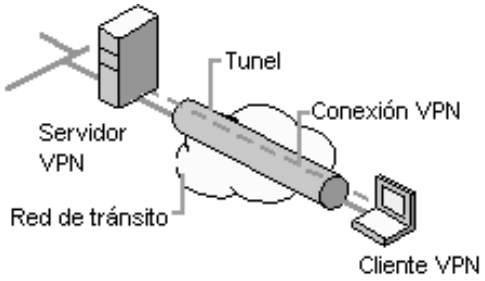


Figura 2.2
Túnel de una VPN

Así, las VPN constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de casi la mayoría de tipos de conexión a Internet. Esta combinación hace de las Redes Privadas Virtuales o VPN una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

La desventaja es que el ancho de banda no está garantizado, ni tampoco se sabe con precisión cuándo funcionarán correctamente las aplicaciones sensibles al retraso.

2.1.3 Arquitecturas de VPN

Las VPN se presentan en cuatro áreas, o bien, arquitecturas de conexión.

2.1.3.1 *Intranet*

Una VPN de Intranet se crea entre la oficina central corporativa y una oficina de ventas remota o entre las oficinas centrales y las oficinas dependientes (Ver figura 2.3). se utiliza para conectar dichas oficinas remotas con la sede central de la organización. Esto es una valiosa particularidad para los negocios que tienen pocas facilidades relativamente y necesitan contacto con la oficina central. Normalmente, sólo se utiliza dentro de la red de una compañía y únicamente acceden los empleados de la misma.

El equipo central VPN, que posee un vínculo para Internet permanente, acepta conexiones vía Internet provenientes de los sitios y establece el "túnel" VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

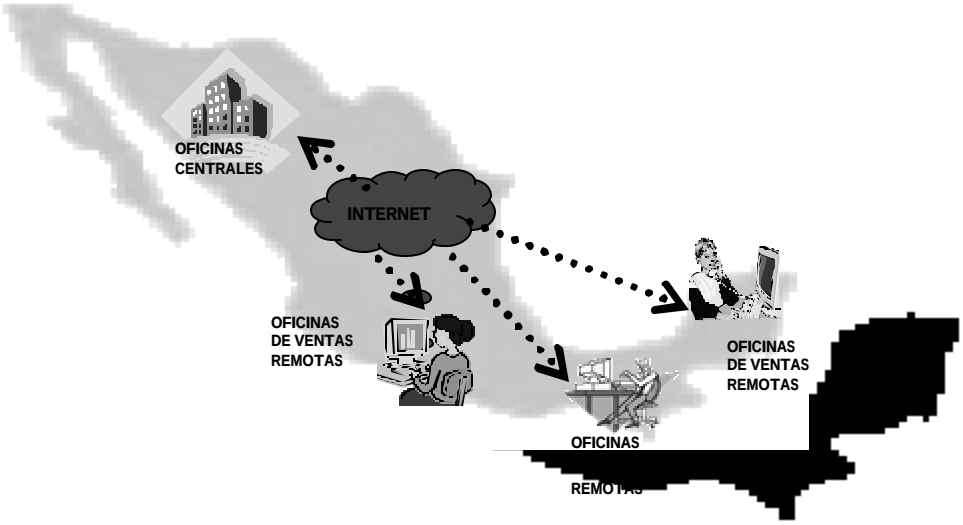


Figura 2.3
Una VPN de INTRANET

2.1.3.2 *Acceso Remoto*

Es quizá el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

Se crea entonces entre las oficinas centrales y los usuarios móviles remotos (figura 2.4). Con el software de cifrado cargado en una computadora portátil, una persona establecerá un túnel cifrado al dispositivo de la VPN en las oficinas centrales.

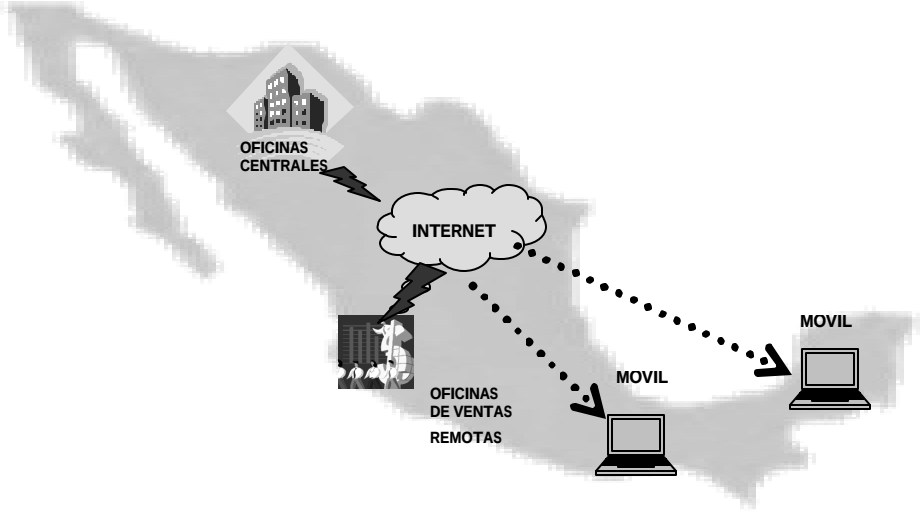


Figura 2.4
Una VPN de ACCESO REMOTO

2.1.3.3 *Extranet*

Se crea entre la empresa y sus clientes y proveedores (Ver figura 2.5). La extranet permitirá el acceso con el protocolo http normal utilizado por los navegadores actuales de Web, o permitirá que se realice la conexión utilizando otro servicio y protocolo acordados por las partes que se involucran. Aquí es donde el comercio electrónico tiene su mayor impacto. Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus principales socios comerciales y con clientes que generan ingresos.

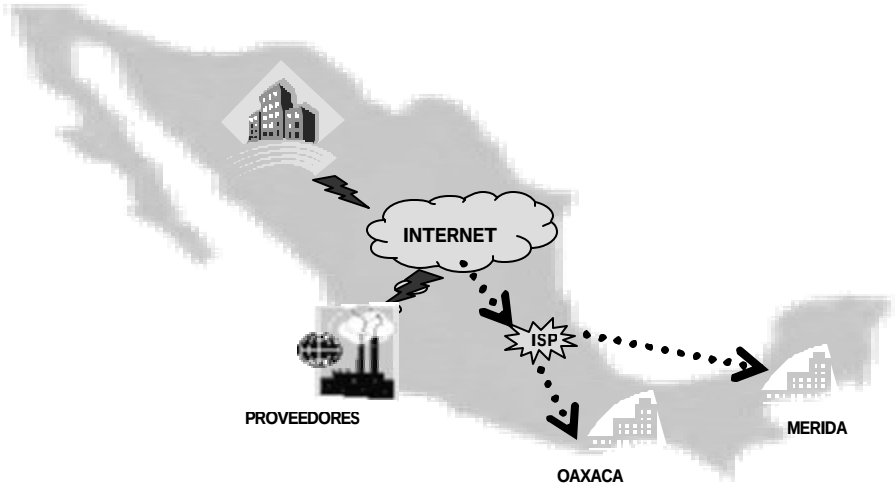


Figura 2.5
Una VPN de EXTRANET

2.1.3.4 *VPN Interna*

Este cuarto esquema es el menos difundido y del cual no hacen uso las compañías actualmente. Es una variante del tipo “acceso remoto” pero, en vez de utilizar Internet como medio de conexión, emplea la misma red LAN (Red de área local) de la empresa.

Los motivos por los que una compañía debería ocupar una VPN interna es que según estudios sobre seguridad indican que los ataques por empleados internos ocupan el primer lugar. Y este esquema sirve para aislar zonas y servicios de la red LAN interna, capacidad que la hace muy conveniente para mejorar las prestaciones de seguridad de redes inalámbricas.

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

2.1.4 Implementaciones de VPN

Todas las opciones disponibles en la actualidad se dividen en tres categorías básicas: soluciones de hardware, soluciones basadas en firewall y aplicaciones VPN por software.

Cada implementación utiliza diversas combinaciones de protocolos para garantizar las tres características fundamentales de seguridad mencionadas en el capítulo 1: Autenticación, Integridad y Confidencialidad.

El protocolo estándar es el IPSEC, pero también están PPTP, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados. Se dará una explicación de ellos más adelante en esté capítulo.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración aunque no tienen la flexibilidad de las versiones por software. Las aplicaciones por software son las más configurables cuando surgen problemas de interoperatividad en los modelos anteriores, es decir son fácilmente escalables. Obviamente el rendimiento es menor y la configuración delicada, porque suma el sistema operativo y la seguridad del equipo en general.

En el caso basado en firewall, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga VPN.

2.2 Funcionamiento de una VPN

2.2.1 Proceso túnel

A diferencia de una red local, en Internet los paquetes llegan a su destino con la ayuda de ruteadores los cuales contienen la información de las rutas, cada paquete pasa de ruteador a ruteador hasta llegar a su destino. En un proceso túnel, tanto emisor como receptor estará de acuerdo en la información que se envía, en los protocolos a utilizar y los arreglos de seguridad que se deben de tener para el envío de información; de esta forma habrá un estricto control del circuito entre ellos. La serie de paquetes que serán enviados a través de la red tendrán un cuidado detallado de la administración y comunicación.

El proceso túnel es la tecnología que pone "virtual" en una VPN permitiendo al sistema (o red) enviar sus datos a otro sistema utilizando Internet u otra conexión de red.

El término de túnel análogamente es como una tubería sólida, en donde existe una ruta directa, que en este caso se establece a través de Internet, una conexión que puede ser un claro ejemplo de este proceso es una conexión de teléfono. Esto es, que cada paquete del proceso túnel, incluyendo cualquier encabezado existente que haya sido adquirido de la LAN donde se originó, es encapsulado, envuelto y finalmente guardado en un nuevo paquete o encapsulado que lleva consigo las direcciones de la fuente al destino de los servidores VPN. En este proceso de encapsulado, el software VPN, que puede estar ejecutándose en una estación de trabajo, un servidor de red, un firewall o un ruteador; se añade al paquete un nuevo encabezado de la fuente a la dirección destino antes de ser enviado a través de Internet. El encabezado original se convierte en una información más en el paquete. De una forma simple, el proceso túnel significa que se ocultan los paquetes de la red de transporte encapsulando el encabezado original por uno que adjunta el protocolo del túnel.

Lograr la interacción de dos redes diferentes no es sencillo. Sin embargo, hay un una solución común que puede manejarse. Este caso es cuando el host de origen y el de destino están en la misma clase de red, pero hay una red diferente en medio (Es el caso de dos redes locales conectadas por una tercera que es Internet). Como ejemplo, considere que tenemos una empresa A con una red ethernet basada en TCP / IP, otra red ethernet de una empresa B basada igualmente en TCP / IP y una WAN PTT en medio, como lo ilustra la figura 2.6 y se desea construir un túnel a través de la WAN PTT para comunicar las redes ethernet de las empresas A y B.

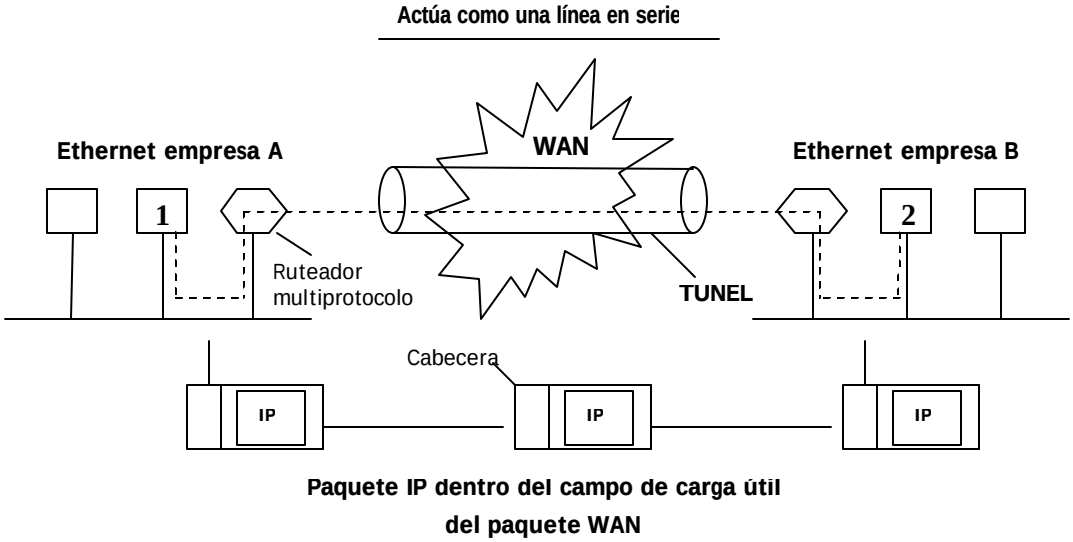


Figura 2.6
Proceso Túnel

El principio de funcionamiento para el proceso túnel es el siguiente: para enviar un paquete IP al host 2, el host 1 construye el paquete que contiene la dirección IP del host 2, lo inserta en un marco ethernet dirigido al ruteador multiprotocolo que enlaza la empresa X, y lo pone en el ethernet. Cuando el ruteador multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del ruteador multiprotocolo que enlaza con la empresa Y. Al llegar ahí, el ruteador retira el paquete IP y lo envía al host 2 en un marco ethernet.

La WAN puede visualizarse como un gran túnel que se extiende de un ruteador multiprotocolo al otro. El paquete IP simplemente viaja de un extremo del túnel al otro. No tiene que preocuparse por lidiar con la WAN. Tampoco tienen que hacerlo los hosts de cualquiera de las redes ethernet, sólo el ruteador multiprotocolo tiene que entender los paquetes IP y WAN.

Las redes privadas virtuales pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos usados desde hace mucho tiempo.

2.2.1.1 *¿Cómo trabaja la tecnología de túneles de una Red Privada Virtual?*

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Como comentamos en el punto anterior, la tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulado", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología VPN, añade otra dimensión al proceso de túneles antes nombrado “encapsulado”, ya que los paquetes están

encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor. Los proveedores de diferentes firewalls incluyen redes privadas virtuales como una característica segura en sus productos.

2.2.1.2 *Estructura de los paquetes IP transmitidos a través de los túneles*

Para entender lo que está pasando, al paquete IP básico. Como se presenta en la figura 2.7, consiste en distintas secciones, el contenido son los datos y en el frente lleva el encabezado IP.

Se incluyen en la descripción de la figura 2.7 los nombres de las secciones correspondientes al encabezado IP que son aplicables al proceso túnel. Por ejemplo, el campo marcado como protocolo, indica el nivel máximo de protocolo que está contenido en el encapsulado. Normalmente es TCP y UDP, pero un protocolo túnel como IPsec utiliza lo que se le llama *paquete de seguridad encapsulada* por lo cual agrega un valor distinto en el campo de protocolo, para indicar la receptor como tratarlo. El campo de offset indica donde inician los protocolos de alto nivel y los datos en relación con el inicio del paquete.

Los últimos dos campos marcados son los que nos indican la dirección IP fuente y destino para que el ruteador sepa hacia donde dirigir el paquete. En el nuevo protocolo túnel incluye un nuevo encabezado IP que contiene las direcciones origen y destino tanto del cliente de la VPN como las del host, así como también las direcciones de la red interna del punto de origen y del punto remoto.

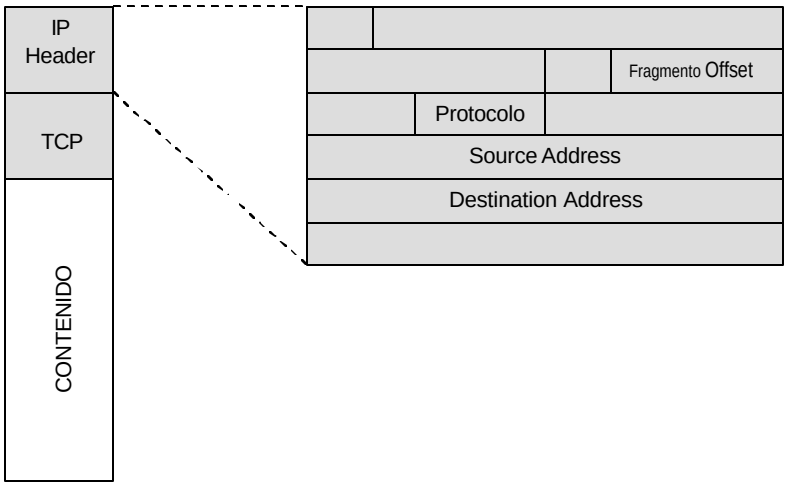


Figura 2.7
Estructura de los paquetes IP transmitidos a través de los túneles con secciones importantes resaltadas.

2.2.1.3 *VPNs y el modelo OSI*

Como se puede ver en la figura 2.8 y como explicamos en el capítulo 1, el modelo OSI consiste en siete capas y esencialmente describe la estructura de un sistema de red.

Cada capa provee servicios a la capa anterior. Los datos originados por la red en la capa superior, la capa de aplicación, se mueve hacia abajo por la pila, en donde cada capa hace lo necesario para que pueda ser manipulado por la capa siguiente. En una red TCP/IP, por ejemplo, en la capa 4, la de transporte, añade el protocolo TCP. Luego en la capa 3, la capa de red, añade un encabezado IP al paquete y lo envía a la capa de enlace de datos, que la envía a la capa física o de hardware que la envía fuera de la red. Al contrario, los datos que entran a la red destino pasan primero por la capa física, después hacia arriba a la capa de enlace, que luego la pasa a la capa de red donde el protocolo IP hace lo suyo, y lo sube a la capa de transporte donde TCP hace lo que le corresponde (incluyendo revisar llegaron sin haber sido modificados) antes de pasarlo hacia arriba.

La figura 2.8 también indica en que capas del modelo encontraremos los protocolos que discutiremos en el tema siguiente. Podemos notar que algunos de los protocolos están situados en la línea que separa dos capas distintas. Y es porque no están ubicados exactamente en una u en otra, lo cual también será explicado.

También hay que hacer notar que entre más debajo de la pila se encuentre la implementación del protocolo, ésta será más sencilla, mientras que asegurarlas se hará más difícil. Aunque esto es generalmente verdad, no debe ser

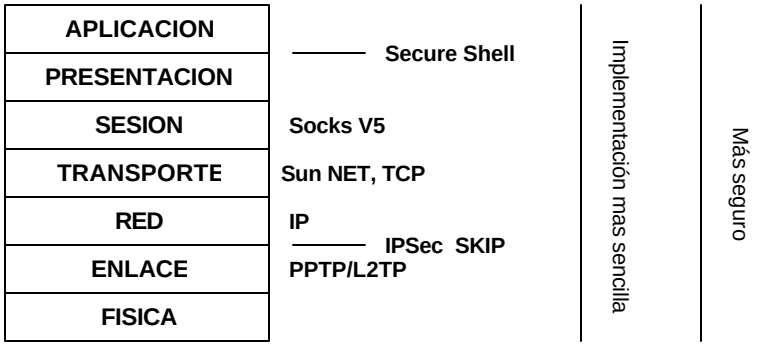


Figura 2.8
El modelo OSI y la ubicación de los protocolos

La Tabla 2.1 muestra las capas donde operan algunos protocolos dentro del modelo OSI.

Capa del modelo OSI	Tipo de datos	Protocolos
Aplicación	Datos de capa superior*	Telnet, SMTP, FTP
Presentación	Datos de capa superior*	ASCII, JPEG, GIF, TIFF, MPEG
Sesión	Datos de capa superior*	Llamada a procedimiento remoto (RPC), ZIP
Transporte	Segmentos	TCP, UDP, SPX
Red	Paquetes/datos	IP, IPX, RIP, BGP
Vínculo de datos	Tramas	PPP, SDLC, LAPB
Estructura física	Bits	V.24, V.35, X.21 bis
*Las capas de aplicación, presentación y sesión no tienen un tipo de datos específico.		
MPEG (*Moving Pictures Experts Group* o Grupo experto en imágenes en movimiento) **RIP** (*Routing Information Protocol* o Protocolo de información de encaminamiento) **BGP** (*Border Gateway Protocol* o Protocolo de pasarelas fronterizas) **SDLC** (*Synchronous Data Link Control* o Controlador de enlace de datos síncrono) **LAPB** (*Link Access Procedure Balanced* o Procedimiento balanceado de acceso de enlace)		

Tabla 2.1
Capas en las que operan los protocolos en el modelo OSI

2.3 Protocolos orientados a paquetes de una VPN

Se han implementado varios protocolos de red para el uso de las VPN. Estos protocolos tienen la finalidad cerrar todos los "hoyos" de seguridad inherentes en VPN, pues deja a la red vulnerable frente a los ataques de servidores de llamada, empleados descontentos y otros puntos de entrada. Las conexiones VPN pueden dar problemas, ya que es preciso configurar el cliente del usuario y la red del servidor para que admitan conexiones a Internet públicas sin que se comprometa la seguridad de la red del servidor. Los administradores de la red se oponen rotundamente a cualquier cosa que cree agujeros en sus firewalls. Como mecanismo de protección para Internet, el firewall establece un único punto de defensa para todos los dispositivos de su red interna. Estos protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

La VPN orientados a VPN son en los que se centra el mayor interés actualmente. Generalmente operan en la capa 2 y 3 del modelo OSI. Sin embargo, como veremos, esto no es tan sencillo. Algunos elementos de estos protocolos VPN operan en una capa, algunos en otra.

2.3.1 Point-to-Point Tunneling Protocol (PPTP)

Protocolo para establecimiento de túneles punto a punto, PPTP, es una especificación de protocolo desarrollada por varias compañías (Microsoft, U.S. Robotics, etc.). Es una combinación del Protocolo punto a punto (PPP) y del protocolo de control de transmisión/protocolo Internet (TCP/IP). Normalmente, se asocia con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP.

PPTP es una extensión de PPP que se utiliza para conexión de disco de Internet. Fue desarrollado por Microsoft, Ascend Comunications y 3Com y fue incorporado a Windows NT 4.0 Server y Estaciones de Trabajo, en Windows 98 y Windows 95. También es compatible con algunas versiones de Unix, pero de otra forma no puede ser extendido. Las versiones anteriores a las mencionadas de Windows no tienen el soporte para este protocolo.

La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autenticación estándar. Dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

Funciones del protocolo de Tunneling Punto a punto

- Pregunta el estado de los servidores
- Provee administración de la banda
- Localiza canales y maneja las llamadas salientes
- Notifica al servidor las llamadas entrantes
- Transmite y recibe datos de Usuario con el control de flujo en ambas direcciones
- Notifica al servidor las llamadas desconectadas.

Típicamente un cliente hace una conexión vía dial-up PPP a un proveedor de servicios de Internet, luego una conexión lógica secundaria se establece construyendo el túnel de la VPN al servidor PPTP y la LAN final. Los paquetes PPTP son recibidos y procesados por el servidor PPTP y son enviados a través de la LAN que está conectada a la Internet, la conexión PPP inicial no es requerida.

En la figura 2.9 se ilustra que cuando un cliente inicia una conexión de VPN vía marcación telefónica utilizando el protocolo PPTP, lo primero que se establece es una conexión PPP a una conexión a un servidor de acceso remoto (NAS) PPTP en Internet. Una vez establecido, una segunda conexión se hace por medio de una conexión PPP, por el NAS ye Internet con el servidor de VPN en el punto remoto. El servidor debe autenticar al cliente y viceversa, proveyendo confidencialidad a las dos entidades de que están hablando con

quien deben hablar. Una vez que está conectado y establecido el túnel, es por esa conexión por loa que pasan los paquetes encapsulados. La autenticación se realiza directamente por el protocolo túnel.

En algún momento PPTP será suplantado en por L2TP. Pero desde que está disponible en cada copia de Windows, PPTP está por todos lados es importante tenerlo siempre en consideración.

2.3.2 Layer Two Tunneling Protocol (L2TP)

El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de *enlace* del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

Así como PPTP y el protocolo L2F, no manejan un encripción o métodos de autenticación específicos, mientras IETF recomienda el uso del encripción IPSec, una característica importante de L2TP es que como el protocolo L2F está diseñado para el tráfico de túnel sobre diversas redes IP. Esto incluye Frame Relay, SONET y ATM. De este protocolo emerge un estándar que contempla los estándares de encriptado que comprende IPSec, es así por lo que destaca en el uso de la industria de las VPN.

Es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. Aceptado ya por la mayoría de firmas y vendedores de productos de conectividad. Es un protocolo de nivel 2, diseñado para encapsular en el nivel 2. Ofrece una compresión por software, lo cual reduce los paquetes de usuario. Las técnicas de compresión también añaden otro nivel de cifrado, aunque en pequeñas cantidades. L2TP utiliza dos funciones: una función de servidor de línea tipo cliente, conocida como LAC, que es un concentrador de acceso L2TP, y una función de servidor de red del lado servidor de llamada LNS. Cuando una computadora realiza una conexión PPP a un PSI, la función LAC inicia el túnel. Entonces la LAC agrega los distintos encabezados a la carga PPP. La LAC establece el túnel al dispositivo de terminación LNS; este dispositivo puede ser un enrutador, un servidor o un dispositivo de acceso. Después de que se estableció el túnel, se configura un mecanismo de autenticación de usuario. L2TP utiliza mensajes de control para optimizar el túnel.

2.3.2.1 *La Base PPP, y la diferencia entre PPTP Y L2TP*

Si se compararan y descodificaran los datos de ambos protocolos en el modelo de referencia de OSI, nos encontraríamos con que su principal punto en común es que ambos descansan en PPP (*Point-to-Point Protocol* o Protocolo punto a punto). PPP es la base para

los dos protocolos VPN y el protocolo que encapsula los datos de la transferencia (esto es, la carga) a través de una red privada. PPTP y L2TP añaden otra capa de encapsulación para transferir la carga a través de un túnel en una red pública.

PPP, en la capa de enlace de datos del modelo OSI, fue desarrollado inicialmente para encapsular datos y transportarlos a través de enlaces punto a punto. Si su empresa dispone de cualquier tipo de conexión punto a punto, como una línea T1, el encaminador utilizará probablemente la encapsulación PPP. También puede utilizar dicho protocolo para conexiones asíncronas (es decir, de acceso telefónico).

2.3.3 Alta Vista tunneling Protocol

El túnel Alta Vista fue creado para integrar los productos DEC. Consiste en un servidor de teleconmutador y un servidor extranet. La forma conexión permite la comunicación entre un servidor Alta Vista y los trabajadores móviles que se conectan desde la red de su hogar vía Internet.

Para establecer la conexión en primer lugar, se usa la autenticación, opciones que incluye autenticación SecureID . Cuando un cliente es contactado por Alta Vista, si el SecureID es implementado por las instrucciones del servidor de Alta Vista el túnel requiere que el cliente tenga sus credenciales de Secure ID. Una vez que la información se llama para procesar cualquier servidor autoriza la conexión del cliente o no la autoriza.

El encriptado es hecho de manera clara y transparente. El túnel de Alta Vista usa una llave criptográfica pública RSA para la autenticación y utiliza la llave privada durante la sesión. RCA desempeña un papel muy importante en el encriptado de datos. Las llaves son atadas a la identidad criptográfica de los usuarios, no especifica una estación de trabajo lo que significa que la dirección IP se asignan dinámicamente. Una vez que el túnel se establece, el servidor y el cliente intercambian automáticamente la llave pública RSA por una llave encriptada privada RC4. En intervalos de 30 minutos el cliente y el servidor cambian a nuevas llaves. La función Hash MD5 es usada para asegurar la integridad de los datos.

El túnel Alta Vista detalla la compresión de datos que comprende el protocolo. Si ambos tanto cliente como servidor tienen una compresión habilitada, Lempel-Ziv-Oberhumer(LZO) es implementado. De otra forma los datos se envían incompresos.

El hecho es que todos estos detalles son bien construidos en el túnel Alta Vista y provee una gran confianza en la interoperabilidad de problemas que no son un factor del túnel Alta Vista de VPN. Por otro lado, cuando se intenta construir una VPN usando clientes y servidores para diferentes proveedores, estos detalles tendrán que ser negociados, como que los nodos puedan conectarse confiablemente.

2.3.4 IP NEXT GENERATION: IPV6

Internet Protocol Security (IPsec, también conocido como IPv6): IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de *red* en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

Debido a la gran importancia que ha adquirido este protocolo hoy en día se tratará a mayor detalle que los anteriores.

2.3.4.1 *¿Qué es IPv6?*

El protocolo IPv6 surgió en el seno de la **Internet Engeeniering Task Force** como culminación de sucesivas tentativas de solucionar el problema de la limitación del espacio de direccionamiento que presentaba IPv4.

La necesidad de un espacio de direcciones extenso estuvo forzado a un cambio inmediato de IP. En particular, gran parte de estos se refieren al soporte de nuevas aplicaciones. Por ejemplo, debido a que el audio y el video en tiempo real necesitan determinadas garantías en los retardos, una nueva versión del IP debe proporcionar un mecanismo que haga posible asociar un datagrama con una reservación de fuente preasignada. Además como varias de las nuevas aplicaciones de Internet necesitan de comunicaciones seguras, una nueva versión del IP debe incluir capacidades que hagan posible la autenticación del emisor.

El primer intento de solucionar el problema de la falta de direcciones es el TUBA que tiene como características:

- Generalizar los protocolos UDP y TCP sobre un espacio de direcciones mayor
- Se emplea el protocolo CLNP (Connection-Less Network Protocol)

Este proyecto es abandonado por un nuevo trabajo llamado SIPP cuyas características más importantes eran:

- Direcciones de 64 bits
- Mezcla de dos implementaciones para sustituir a IPv4 (SIP y PIP)

Finalmente, en 1994 el IPng Area (IPng se refiere a discusiones y propuestas para la nueva versión de IP) elige SIPP como implementación adecuada variando el tamaño de las direcciones a 128 bits y el protocolo emergente se renombra a **IPv6**.

IPv6 es la abreviación de Internet Protocol, versión 6. IPv6 es un nuevo sistema, actualmente bajo desarrollo, para asignar direcciones IP en el futuro. IPv6 reemplazará eventualmente el actual sistema de direccionamiento IP, conocido como IPv4. Entre sus principales características destacan las siguientes:

- Arquitectura jerárquica de direcciones
- Autoconfiguración de equipos
- Computación móvil
- Seguridad e Integridad de Datos
- Calidad de Servicio, QoS
- Soporte a tráfico multimedia en tiempo real
- Aplicaciones multicast y anycast
- Mecanismos de transición gradual de IPv4 a IPv6

2.3.4.2 *Objetivos de IPv6*

IPv6 surge como una necesidad, esto es porque el protocolo de red que utiliza la Internet actualmente es el IPv4 pero en los 90's la comunidad Internet se percató entre otros problemas que las direcciones disponibles de Internet se estaban agotando, asimismo que el formato datagrama no ofrecía confidencialidad alguna, problemas de este tipo se tratan de erradicar con la implementación de IPv6.

IPv6 obtiene:

- *Mayor número de direcciones*. Pasa de 32 bits en IPv4 a 128 bits en IPv6.
- *Encabezado con formato flexible*. IPv6 utiliza un nuevo formato incompatible de datagrama Y un conjunto de encabezados opcionales.
- *Soporte para la reservación de recursos*. IPv6 reemplaza la especificación del tipo de servicio en IPv4 con un mecanismo que permite la reservación anticipada de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como video en tiempo real que requiere garantías en ancho de banda y retardo.
- La capacidad de extensión permitirá adaptar el protocolo a nuevas tecnologías en redes o a nuevas aplicaciones.

Usa direcciones IP de 128 bits de largo. Con este esquema, una dirección IP consistirá de 8 secciones, cada una conteniendo un valor de 16 bits. El número de direcciones IP que ésta crea es igual al espacio de direccionamiento del IPv4 al cuadrado, dos veces. Pretende permitir el futuro crecimiento de la tecnología de redes y expansión de Internet.

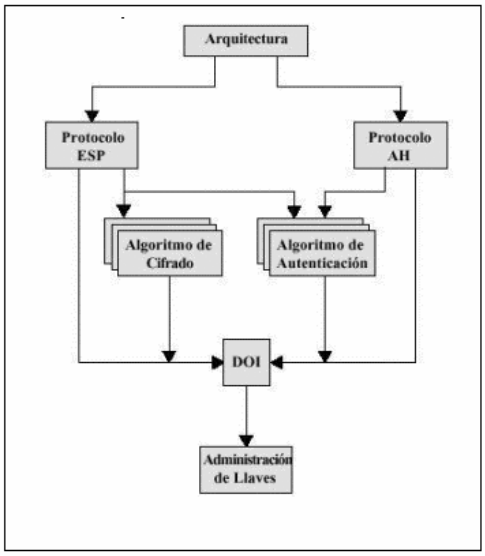


Figura 2.9
Nivel del Documento IPSec

2.3.4.3 *¿Cómo Funciona IP Sec?*

Reside debajo de la capa de transporte (TCP, UDP) y, por tanto, es transparente a las aplicaciones, por lo que no hay necesidad de cambiar software de usuario o sistema cuando se implementa IPSec en el firewall o en el ruteador y aún cuando se implemente en sistemas finales, el software de capas superiores, incluyendo aplicaciones, no se afecta.

IPSec es una extensión del protocolo IP que provee no sólo encriptado sino autenticación en la capa de transporte, la siguiente generación de IP es IPv6, quien soporta al IPSec nativo ya que IPSec es un requerimiento de la IETF dentro de las especificaciones de IPv6.

IPSec es un protocolo de elección para las VPN, aun sobre PPTP. Windows NT 5.0 reporta su éxito sobre PPTP y L2TP. Cisco Systems anuncia que ello tendrá la estructura IPSec dentro de sus routers. IPSec abarca casi todos si no es que todos los elementos que requiere una VPN. Puede usarse como un protocolo entero de la VPN o elementos de éste pueden usarse para hacer estándares para otros protocolos VPN.

Procura asegurar la interoperabilidad detectando acertadamente las fallas que cualquier implementación puede contener con respecto a la autenticación de la carga útil y del paquete encriptado. Estas fallas son un grupo mínimo y no permiten proveer el acuerdo de seguridad o funcionalidad que se requiere en la VPN.

IPSec debe ser transparente para los usuarios finales y no necesitan entrenamiento de seguridad, ni problemas de manejo de llaves sobre una base usuario a usuario y tampoco hay problemas de revocación de llaves cuando los usuarios dejan la empresa. Puede proporcionar seguridad a usuarios individuales si es necesario, por lo que es útil para

empleados fuera del sitio y para definir una subred virtual segura dentro de una empresa para aplicaciones vulnerables.

Ofrece servicios de seguridad en la capa IP, permitiendo al sistema: elegir los protocolos de seguridad requeridos, determinar los algoritmos a usar para los servicios y establecer cualquier llave criptográfica que se requiera para proporcionar los servicios.

IPSec requiere de dos protocolos para proporcionar seguridad, (véase figura 1.4):

- Un protocolo de autenticación, designado por el encabezado del protocolo, llamado Authentication Header (**AH**).
- Un protocolo que combina cifrado y autenticación, designado por el formato del paquete para ese protocolo, llamado Encapsulating Security Payload (**ESP**)**.**

ESP de IPSec provee un túnel con capacidad de las necesidades de una VPN. Lo hace tomando el encabezado original IP y encapsulandolo dentro de la ESP, y es encriptado con el resto de los datos. Luego se incluye o agrega al resto del paquete un nuevo encabezado IP conteniendo la dirección del camino de la VPN. Haciéndolo de esta forma, IPSec no solo esconde los datos, sino también esconde la fuente original y la dirección destino para los usuarios de Internet, encriptando los datos hace que el paquete quede inmune para el análisis de ataque de tráfico. Esto si llega a ser un impedimento para quienes únicamente entran a la red a observar información que no les corresponde.

2.3.4.4 *Mecanismos de transición básicos*

Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible. Existen dos mecanismos básicos:

Dual Stack

Provee soporte completo para IPv4 e IPv6 en host y routers. La forma mas directa para los nodos IPv6 de ser compatibles con nodos IPv4-only es proveyendo una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos “IPv6/IPv4”. Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

***Tunneling*:**

Encapsula paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4. Los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Paquetes

IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone. Los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente determinados usando direcciones IPv6 IPv4-compatible.

Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de ruteo IPv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente. No obstante, IPv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con IPv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

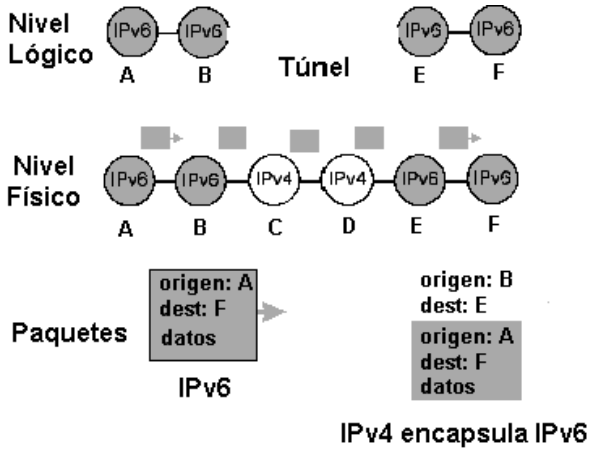


Figura. 2.10
Compatibilidad de nodos

2.3.4.5 *6 Bone?*

El 6bone es el backbone de IPv6, su función es asistir en la evolución y desarrollo del IPv6. Su creación se formalizó en marzo de 1996 en una reunión del IETF en Los Ángeles. Es una red experimental, informal y cooperativa de alcance mundial. Está supervisada por el grupo Next Generation Transition (ngtrans) del IETF y opera bajo IPv6 Testing Address Allocation [RFC 2471].

Está formada por varios 6bones regionales. Aunque la mayoría de los 6bones utilizan túneles, lentamente algunos de ellos están migrando a links nativos IPv6. Uno de ellos es el WIDE 6bone del proyecto WIDE de Japón.

Hoy en día existen otros backbones académicos y comerciales que ofrecen servicios IPv6. El objetivo inicial del 6Bone era probar los estándares e implementaciones del IPv6, hoy en día su objetivo es probar los procedimientos de transición.

2.4 Protocolos orientados a aplicación de una VPN

2.4.1 SOCKS Networks Security Protocol

El sistema SOCKS proporciona otra alternativa a los protocolos de VPN. Es un protocolo que puede utilizar un servidor proxy para aceptar consultas de los usuarios cliente en la red de la empresa, de forma que el servidor proxy puede contestarle a través de Internet. SOCKS se aloja en el nivel de *transporte* de OSI. Como SOCKS trabaja en un nivel OSI más alto que los protocolos que aquí se mencionan, permite a los administradores limitar el tráfico VPN. SOCKS utiliza sockets para representar y supervisar conexiones individuales. La parte del cliente SOCKS está integrada en ciertos exploradores web y se puede agregar la parte del servidor a un servidor próximo.

Se utilizan muchas aplicaciones para tener acceso a redes seguras públicas y privadas mediante tecnologías de seguridad de la capa de transporte como **SOCKS**, como el protocolo de transferencia de hipertexto seguro (HTTPS, *Hypertext Transfer Protocol Secure*) o nivel de sockets seguro (SSL, *Secure Sockets Layer*). La seguridad de la capa de transporte, significa que las aplicaciones basadas en TCP están escritas específicamente para utilizar estos servicios de seguridad. SOCKS V, con el que no es compatible Microsoft, se aplica a protocolos basados tanto en TCP/IP como el Protocolo de datagramas de usuario (UDP, *User Datagram Protocol*), y se presta a administración centralizada.

2.4.2 Sun.NET

Lo último en el mercado VPN por Sun Microsystems. Este interesante protocolo opera en la capa cuatro del modelo OSI que es la capa de transporte. Está basado en JAVA, lo que quiere decir que por ser virtual puede implementarse en cualquier plataforma de sistema operativo de cualquier cliente. Cuando Sun.NET permite el sitio contacta con el browser JAVA-capable, después de la autenticación un applette de Java es transferido hacia uno de los extremos de los clientes. Una vez que ha sido activado, establece una conexión VPN con el servidor. El encriptado es realizado usando un cambio DH y RCS que trabajan sobre encriptado simétrico.

Las ventajas de Sun.NET son obvias, ya que se tiene la tranquilidad de que el cliente se identifica aun teniendo una plataforma diferente. Es también una ventaja para los usuarios LAN.

2.4.3 Secure SHell

Secure SHell (SSH) es probablemente el más simple de los protocolos orientados a Aplicación de una VPN. Es un programa para acceder a otra computadora sobre una red, para ejecutar comando en una máquina remota y para mover archivos entre ellas. De alguna forma esto suena como un acceso remoto común, pero la diferencia radica en que SSH agrega seguridad mediante la autenticación y encripción, convirtiéndose así en un protocolo VPN.

SSH trabaja en lo más alto de la cadena alimenticia, la capa de aplicación en el modelo OSI. Esto limita las opciones de arquitectura de una VPN basada en SSH. Y que no puede instalarse en el firewall o router; sólo puede implantarse en el nivel usuario-servidor.

SSH intercambia llaves de sesión aleatorias utilizando cifrado de llave pública RSA. Las firmas digitales RSA también son usadas para la autenticación. La llave utilizada para cifrar la llave de sesión nunca se almacena en disco, en lugar de ello se regenera y la llave anterior es eliminada. El cliente de RSA autentica el servidor al inicio de toda conexión para prevenir que se ejecuten caballos de troya utilizando spoofing en el ruteo del DNS. El servidor autentica por SSH al cliente antes de aceptar cualquier cosa. SSH pretende ser un reemplazo en algunos casos de telnet.

Pero es importante resaltar que SSH no utiliza el proceso túnel o encapsulamiento como hemos visto en los otros protocolos para VPN como PPTP. Esto significa que, mientras los encabezados están cifrados y autenticados, la dirección IP fuente y destino son visibles para los ruteadores de Internet o de alguien utilizando un sniffer para paquetes. Esto también significa que se permite todo trafico de y para una dirección IP legal a menos que esté oculta tras un servidor proxy o se implemente algún tipo de redirección de tráfico de red.

La única seguridad es la encripción y la autenticación para prevenir el escuchar escondido. El servidor rechazará todos los paquetes que no pasen la autenticación y la sesión no podrá ser secuestrada a menos que corrompan la autenticación.

Sólo existen versiones gratuitas de SSH para Unix y OS/2 (uso no comercial). En cuanto a versiones comerciales, que incluyen licencias de uso están las implementaciones APRA Windows y Macintosh.

	Alta Vista	IPSec	L2TP	PPTP	SKIP	SOCKS V.5	SSH2	Sun.Net
Arquitecturas	C/S LAN/LAN	C/S NAS/NAS LAN/LAN	C/S, C/NAS NAS/NAS LAN/LAN	C/S, C/NAS NAS/NAS LAN/LAN	C/S LAN/LAN	C/S (req. Serv. y cliente SOCKS)	Sólo C/S	Sólo C/S
Esconde direcciones IP ilegales	SI	SI	SI	SI	SI	SI	NO	NO
Transporta paquetes no IP	NO	SI	SI	SI	NO	NO	NO	NO
Plataformas Disponibles	DEC	Windows, Unix,	Windows NT, Unix	Windows NT y no NT, Unix	SunOS, BSD, Linux, Windows NT y no NT	Windows y Windows NT	NetBSD, HP- UX, IBM AIX, Digital Unix, solaris	Servidor SUN, Cliente: cualquier aplicación Java
Acceso Remoto	BUENO	BUENO	Excelente	Excelente	BUENA	Regular	Regular	Excelente
Red a Red	BUENO	BUENO	BUENO	BUENO	BUENO	BUENO	NO	NO
Escalabilidad	BUENO	Excelente	BUENO	BUENA	BUENA	BUENA	NO	NO
Capa OSI	ENLACE Y RED	ENLACE Y RED	ENLACE	ENLACE	Entre la capa de red y enlace	SESION	APLICACIÓN	
Encripción específica	RC4 doméstico e internacional	DES-CBC 56 bits	No Especificado	Windows DES de 40, 56 y 128 bits	RC2 Y RC4, DES, 3DES, ELVIS+, SAFER	Soporta GSS- API para negociación.	3 DES	
Soporta IPSec para seguridad	NO	N/A	SI	SI	SI	SI	SI	
Soporta X.509	SI	SI	SI	SI	SI	SI	SI	

2.5 Clientes / Servidores en VPN

Un servidor VPN normalmente es un componente hardware, aunque también lo puede ser software. Puede actuar como un gateway en una red o en una computadora única. Debe estar siempre conectado y esperando a que clientes VPN se conecten a él. El software para el servidor VPN es bastante frecuente. Sistemas como Windows 2000 Server permiten alojar un servidor VPN.

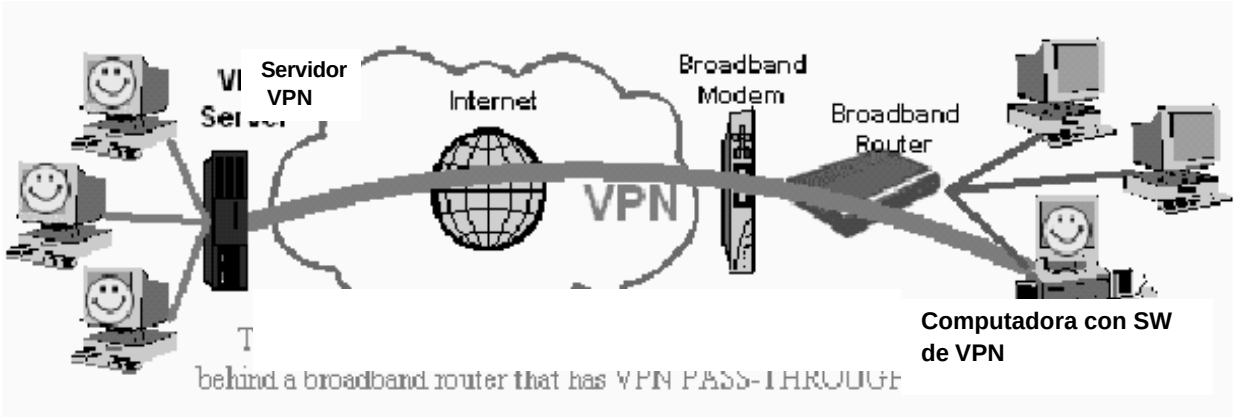


Figura 2.11
VPN detrás de un ruteador broadband

La figura 2.11 muestra una computadora corriendo en un software VPN tras un ruteador broadband que tiene una VPN PASS-THROUGH.

Un cliente VPN es en la mayoría de los casos un componente software, aunque puede ser también un componente hardware Un cliente realiza una llamada al servidor y se conecta. La computadora cliente podrá comunicarse con el servidor VPN ya que ellos se encuentran en la misma red virtual.

Como ya se mencionó, el software para un cliente VPN es bastante común y cuando se carga en la computadora este software permite crear un túnel seguro a través de Internet para poder comunicarse con el servidor VPN.

2.6 VPN Dinámicas

2.6.1 Conceptos de las VPN Dinámicas

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones comerciales. Entonces, ¿Cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperabilidad y facilidad de uso?

La respuesta apropiada se encuentra en la utilización de VPNs Dinámicas. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

Entre las principales características se encuentran las siguientes:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente a la diferencia entre usuarios.
- Permite la posibilidad de intercambio de información en diversos formatos.
- Los ajustes para cada usuario se consiguen gracias a distinntos navegadores, aplicaciones, sistemas operativos, etc...
- Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado.
- Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

2.6.2 Funcionamiento de las VPN Dinámicas

Las VPN Dinámicas constan de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad.

Siguiendo los pasos ilustrados en la figura 2.12, un usuario realiza una petición de información a un servidor, por ejemplo, pulsando con su ratón en un hipervínculo. Los pasos seguidos se pueden describir en los siguientes puntos:

Un usuario solicita información usando una aplicación tal como un navegador de Internet, desde una computadora de escritorio: El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. En el supuesto de que un usuario haya accedido a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo será seguro y solamente podrá ser accedido por usuarios autorizados.

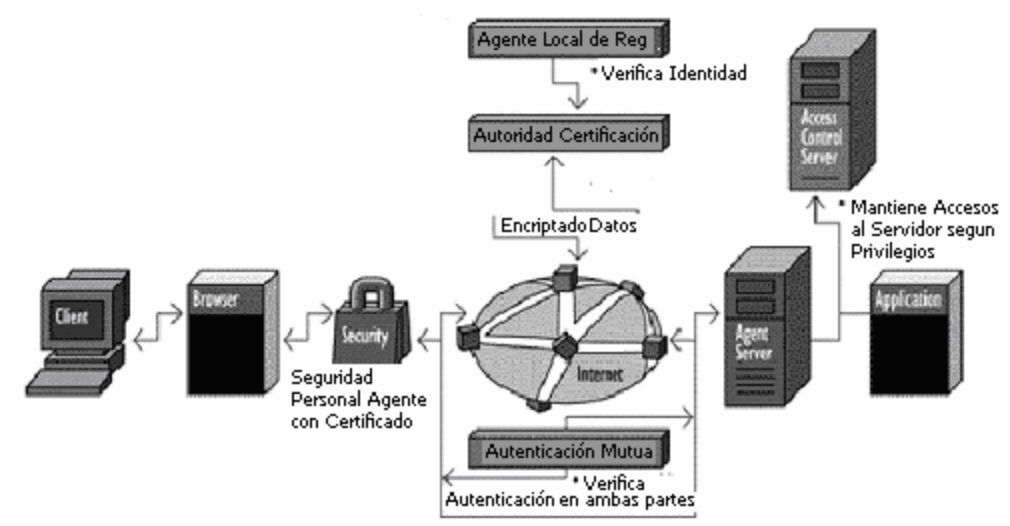


Figura 2.12
VPN Dinámicas

La aplicación envía y asegura el mensaje: Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autenticación. Este paso verifica la identidad de ambas partes antes de llevar a cabo cualquier acción. Una vez que se produce la autenticación se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario.

El mensaje se transmite a través de Internet: Para que la petición alcance el servidor debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atraviese uno o más firewalls antes de alcanzar su objetivo. Una vez atravesado el firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

El mensaje recibido debe pasar controles de seguridad: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición.

Durante la petición, se verifican los derechos de acceso de los usuarios: En una VPN dinámica, el sistema debe poder restringir qué usuarios pueden y cuáles no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el *Servidor de Control de Acceso*. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.

La petición de información es devuelta por Internet, previamente asegurada: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autenticación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

2.7 Soluciones de Software y Hardware para VPN

2.7.1 El reto de las empresas que distribuyen esta solución

Existen diferentes compañías dedicadas a la distribución de este tipo de equipos. En México la difusión de esta solución aún no está siendo tan atendida por la industria de cómputo. Los costos son representativos a la hora de dar números y aunque a la larga sean buenas inversiones este tipo de soluciones no se refleja un beneficio inmediato monetario mas bien el beneficio está en el ahorro, esto representa un reto para las empresas dedicada a implantar estas soluciones y es por ello que aun existiendo equipos bastante confiables y seguros aun el mercado de la VPN no ha sido totalmente explotado. La lucha de las empresas también está en fabricar y conseguir mejores precios.

Otro de los puntos a tratar a la hora de hablar de equipos comerciales es que para todo tipo de empresas debe haber equipos de acuerdo a sus necesidades y es que en México existe más pequeñas empresas que grandes y es por ello que los distribuidores deben de encontrar mejores soluciones a la hora de vender equipos dirigidos a este sector.

A continuación se hablará de algunas de las soluciones comerciales que se pueden conseguir actualmente, claro que también hay que considerar que con Windows que es el sistema operativo por excelencia actualmente se puede hacer una conexión de VPN.

2.7.2 Algunas de las empresas que distribuyen VPN

2.7.2.1 *Cisco Systems*

La compañía norteamericana Cisco Systems es el líder mundial de soluciones de red para el mundo Internet -según un estudio de la consultora Yankee Group, el 80% de la tecnología en la que se basa Internet es de Cisco.

En el manejo de implementaciones VPN, esta empresa tiene las siguientes soluciones:

Versión 1.0 del Cisco Security Device Manager (SDM)

Disponible en las series Cisco 830 y 3700 de *routers* de acceso para implementar y manejar los servicios de seguridad basados en el software Cisco IOS. Este administrador de dispositivo ofrece ayuda inteligente para configurar servicios de *firewall* y Seguridad IP (IPSec) en VPN. El Cisco SDM también ofrece la capacidad para cerrar, basada en una interfase gráfica de usuario y una capacidad de auditoría de seguridad para verificar y recomendar cambios a las configuraciones del *router* con base en recomendaciones de los reconocidos laboratorios ICSA Labs.

Versión 3.1 de solución CiscoWorks Security Information Management (SIMS)

Basada en la tecnología de netForensics, CiscoWorks SIMS ofrece monitoreo de eventos de seguridad y ambientes de seguridad para otras marcas. Sus opciones avanzadas incluyen puntaje de eventos, impacto de negocios y análisis de amenazas que ofrecen un juego completo de reportes y análisis para que los usuarios puedan manejar con mayor certeza las implementaciones de seguridad y mejorar su productividad.

Versión 3.0 del módulo Security Technology del Cisco IP Solution Center (ISC): Una nueva oferta de administración de seguridad basada en políticas que ofrece a los usuarios una administración robusta y escalable de VPNs de gran escala e implementaciones de *firewalls*. La plataforma ISC reduce los costos operativos de implementaciones de seguridad y evita el establecimiento de políticas de seguridad inconsistentes. Los usuarios pueden implementar y manejar con certeza y efectividad tecnologías de seguridad VPN, *firewall*, NAT (network address translation) y calidad de servicio. Módulos adicionales ISC ofrecen administración Capa 2 y MPLS para obtener mayores opciones de administración.

Versión 2.2 de CiscoWorks VPN/Security Management Solution (VMS): Ofrece administración de seguridad para el portafolio Cisco de servicios de seguridad. Las mejoras incluyen soporte administrativo integrado para el Cisco Catalyst 6500 Firewall y módulos de servicio VPN además de monitoreo integrado para soluciones Cisco IDS que operan la versión 4.0 del software.

2.7.2.2 *3Com*

Durante las décadas de 1980 y 1990, 3Com se convirtió en líder mundial en la construcción de redes que unían a las personas y a las empresas en este nuevo mundo de comercio y comunicaciones. Al tiempo que creaba el equipamiento que conectaba los equipos a la red, 3Com inventó hubs, switches y routers que interconectaban a individuos, grupos de trabajo, empresas y redes.

3Com OfficeConnect VPN Firewall

Diseñado para pequeñas empresas con delegaciones y trabajadores remotos, el firewall VPN es muy sencillo de instalar y utilizar y ayuda a hacer seguras las comunicaciones a través de Internet

3Com OfficeConnect VPN Firewall proporciona seguridad para prevenir los accesos no autorizados y bloquear los ataques de denegación de servicio y otros ataques provenientes de Internet.

- Conexión / Cantidad de usuarios: 253.
- Incorpora 4 puertos.
- Protocolo de interconexión de datos: Ethernet, Fast Ethernet.
- Red / Protocolo de transporte: TCP/IP, PPTP, UDP/IP, L2TP, IPSec, PPPoE.
- Indicadores de estado: Actividad de enlace, velocidad de transmisión del puerto, alimentación, alerta.

Características: Recortable, soporte de DHCP, soporte de NAT, VPN, soporte para PAT, enlace ascendente automático, limitación de tráfico, Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), filtrado de paquetes, servidor DNS dinámico, activable.

- Algoritmo de cifrado: DES, MPPE, AES, IKE.
- Cumple con las normas IEEE 802.3.
- Interfaces: 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 4 x nodo de red - Ethernet 10Base-T/100Base-TX - RJ-45.
- Software incluido: Controladores y utilidades.
- Sistema operativo requerido: Microsoft Windows NT 4.0, Microsoft Windows 95/98, Microsoft Windows 2000 / XP.

2.7.2.3 *Check Point*

Una de las empresas líder en soluciones VPN tiene el estándar De-facto para la Seguridad en Internet y liderazgo en el market share de VPN y Firewall (273,000+ VPN/firewalls). Es la única compañía en ofrecer Application Intelligence para protección integrada contra ataques de aplicación y de red.

VPN-1 PRO

Es una solución integrada de software que combina la seguridad de FireWall-1 con tecnología VPN. VPN-1 Pro brinda conectividad segura a redes corporativas, usuarios móviles y remotos, oficinas remotas y socios estratégicos. La solución VPN-1 está disponible en una amplia variedad de plataformas abiertas y appliances de seguridad para cumplir con los requerimientos costo / performance de cualquier organización.

- Protege la comunicación de datos con estándares de la industria para esquemas de cifrado, autenticación y administración de llaves.
- Protege recursos valiosos de la empresa con FireWall-1.
- Permite administración de seguridad centralizada, integrada y basadas en políticas.
- Soporta arquitectura de performance SecureXL, PKI y QoS integrada.

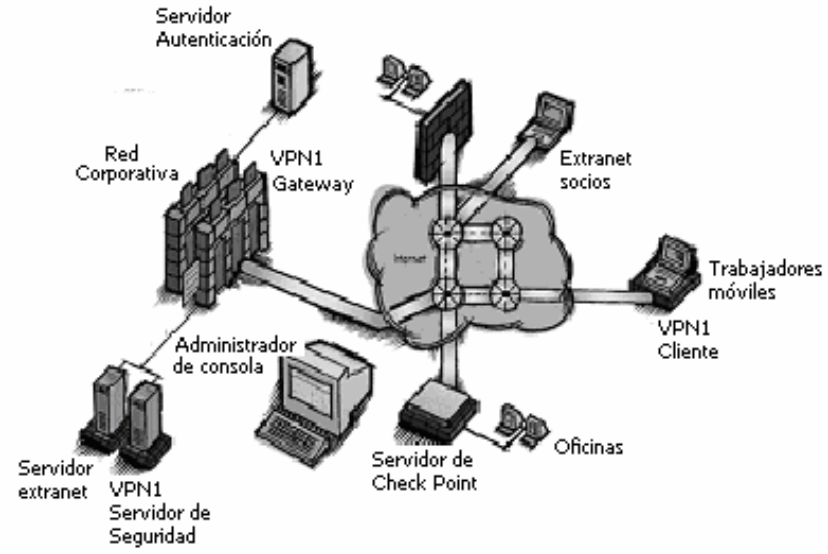


Figura 2.13
VPN-1 PRO

VPN-1 NET

Check Point VPN-1 Net es una solución dedicada de VPN que permite a las empresas conectar rápidamente múltiples oficinas a través de la Internet. Brinda una alternativa de bajo costo a los circuitos frame relay y dedicados. VPN-1 simplifica la administración de las VPN al agrupar las oficinas en comunidades VPN utilizando la tecnología One-Click VPN de CheckPoint.

- Permite administración sencilla de VPN utilizando comunidades.
- Incluye soporte de los estándares VPN de la industria y protocolos de cifrado.
- Brinda administración de seguridad centralizada y basada en políticas.
- Soporta una amplia variedad de plataformas de servidores y appliances.
- Brinda performance superior a través de SecureXL para alta disponibilidad.

2.7.2.4 *Trend Net*

Fundada en 1990 bajo la marca registrada TRENDnet, de buena calidad, bajos precios, alto rendimiento y buen servicio.

Utiliza la tecnología avanzada empresas como Intel, Broadcom, Lucent, Conexant, y Cirrus Logic convierte a TRENDware en la solución perfecta para el sector de redes.

TW100-BRV204 Enrutador Firewall VPN Cable/DSL

El ruteador Firewall VPN Cable/DSL TW100-BRV204 de TREND-net proporciona a sectores de trabajo o sucursales remotas un acceso a Internet compartido de banda ancha, mientras que al mismo tiempo proporciona seguridad avanzada Firewall y VPN contra ataques potenciales de hackers. Además de la conversión de dirección de red “Network Address Translation” (NAT), el enrutador incluye un Robusto Paquete de Inspección Firewall “Stateful Packet Inspection Firewall” (SPI) para filtrar tráfico al nivel del paquete con protección contra los populares ataques de Negación de Servicio “Denial of Service” (DOS). La encriptación VPN apoya hasta 5 túneles VPN simultáneos vía configuración client pc-to-endpoint o endpoint-to endpoint. El Wizard de instalación ayuda a que la instalación de la unidad y el montaje VPN sea rápido y fácil. La nueva familia Firewall VPN entrega seguridad avanzada para su información sensible a un precio accesible.

Figura 2.14
Ruteador TW 100-BRV204 de TRENDNET

2.7.2.5 *ANSEL Comunications*

Ansel se crea en 1996 con filiales en USA, Chile y México, con el interés de proporcionar soluciones robustas en el ámbito de la infraestructura informática y de comunicaciones de las PyME y Micro Empresas, basando sus estrategias en la Calidad del Servicio y una gama de productos clave.

Actualmente Ansel de México es la líder y propietaria de la marca, y se ostenta como una Empresa 100% mexicana que como resultado está interesada en la problemática regional y sus esfuerzos están encaminados a satisfacer las necesidades de este mercado.

ANSEL diseñó una solución integral que se basa en un poderoso firewall hardware-software (IAF), se integraron además, todos los servicios que hoy por hoy son los mas utilizados por usuarios y proveedores de acceso a Internet, sin requerir de instalaciones posteriores de software, drivers, actualizaciones, etc. no requiere de una computadora para su funcionamiento y el hardware con el cual esta construido es de nivel industrial, lo que permite su funcionamiento las 24 horas del día de todo el año. Este tipo de dispositivos, se conoce en el mercado como INTERNET APPLIANCES. Ansel ha llamado a este dispositivo ISS (Internet Secure Server) incluye entre otras muchas cosas:

- Servidores WEB, EMAIL, FTP multi-dominios
- Servidor SSH
- Servicios de WEBMAIL, FOROS, ECOMMERCE, GRUPOS,PRINT SERVER, FILE SERVER, ANTIVIRUS, VoIP, CONTESTADORA
- Servicios de seguridad como SITE FILTER, Anti SPAM, PACKET FILTER, FIREWALL, AntiHACKER, BACKUP SERVER, VPN SERVER y CLIENTE, DNS SERVER, WINS SERVER
- Servicios de control como MONITOREO DE HARDWARE, BANDWIDTH MANAGER, WEB MONITOR, PROXY CONTROL, DHCP SERVER
- Servicios de conectividad LAN y WAN a 10/100Mbps, DMZ a 10/100 mbps; soporta V-35, ISDN, Dial-Up, ADSL, Wireless, con opcion para tarjeta ruteador (para enlaces dedicados)
- Administracion local y remota mediante WEB 100% no requiere software ni drivers.

El ISS no requiere una direccion IP fija para funcionar como servidor, lo que permite que utilice los actuales enlaces ADSL para convertirse en su propio hosting con la seguridad que un firewall de alto nivel (Figura 2.15).

Figura 2.15
ISS de ANSEL

2.7.2.6 *F-Secure VPN*

Es una solución flexible y de buen costo obtener los beneficios de Internet manteniendo la seguridad en la misma. Dota a la gestión de la red de túneles entre los puntos de empresa manteniendo el acceso a puntos externos si se quiere. Es mejor usar este paquete en unión a un firewall para conseguir un control total sobre el tráfico de datos de toda la organización.

F-Secure VPN es un nuevo producto de la compañía Data Fellows que se encuentra dentro de la línea de productos enfocados a la seguridad de Internet. Usa los mecanismos de encriptación disponibles, más sofisticados y además es compatible con las arquitecturas modernas Cliente-Servidor y por supuesto Internet.

Las características principales son las siguientes:

- Fácil de instalar. Requiere pocos parámetros de instalación para el administrador, durante la instalación inicial.
- Fácil de configurar. F-Secure VPN 1.1 tiene un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.
- Configurable para asegurar las conexiones Extranet. Con el editor de red de F-Secure VPN, se puede definir la seguridad en las conexiones Extranet con tus clientes habituales.
- Rápido. En la actualidad, las redes privadas virtuales pueden aumentar la velocidad en conexiones entre puntos empresariales porque que comprimen todo el tráfico añadiéndoles encriptación.
- Seguro. Usa una extensa variedad de algoritmos de selección de usuarios, incluyendo 3DES, Blowfish, RSA, etc.
- Basado en la tecnología F-Secure SSH, el standard de hecho para conexiones entre terminales encriptados usando Internet, tecnología es usada por la NASA
- Asequible. Una pequeña red privada virtual de 2 puntos puede instalarse por 5000 dólares más el precio de los PC's dedicados.
- Disponible a nivel global, con una fuerte encriptación. Data Fellows puede enviar el software encriptado a todo el mundo, sin ningún compromiso, desde las oficinas situadas en Europa o en US. Como compañía Europea que es, no se encuentra bajo las restricciones de exportación americanas referentes a la encriptación.

Encripta paquetes TCP/IP en el transcurso de la comunicación sobre Internet o una Intranet. Trabaja con cualquier clase de base de routers y firewalls instalados. También suministra la mayoria de potentes encriptadores disponibles, incluyendo triple DES (Encriptador de Datos Standard) y Blowfish. Además, F-Secure comprime datos, autentifica otros servidores encriptados, realiza gestión de claves distribuidas.

Beneficios:

- Cualquier PC con los requerimientos mínimos puede correr el software de F-Secure VPN.

- La red VPN es dinámicamente ampliable de modo que nuevas LANs se puede añadir a VPN existente sin demasiada configuración.
- Automáticamente se encriptan y protegen contra alteraciones, todas las conexiones F-Secure VPN.
- Se integra con cualquiera de las firewalls existentes.
- Soporta conexiones Extranet seguras.

2.7.2.7 *Nokia*

Nokia ofrece una potente solución Firewall/VPN completamente integrada que extiende las redes de empresa de forma segura a Internet, permitiendo conectar rápidamente múltiples oficinas y socios. Nuestra solución VPN dedicada constituye una alternativa rentable a las líneas dedicadas.

Virtual Private Networks permite a las empresas utilizar Internet para atender todas sus necesidades de comunicación segura: conexión de oficinas remotas; acceso remoto a empleados nómadas ; incluso conexión con socios comerciales. Nokia da respuesta a todas estas necesidades al tiempo que reduce los costes asociados a la línea dedicada.

El equipo Firewall/VPN de Nokia combina tecnología de red privada virtual (VPN) y cortafuegos del líder del mercadoCheck Point con plataformas Nokia especialmente desarrolladas, preconfiguradas y probadas. Permite a las organizaciones utilizar sus plataformas de cortafuegos para lograr una conectividad de red extendida de forma económica y eficiente

2.7.2.8 *Linksys*

Inicia sus operaciones en 1985. Ofrece innovaciones tecnológicas y nuevos productos de una buena calidad y costos razonables. Cuenta con el soporte y servicio necesarios.

Router vpn de cable/dsl etherfast con switch 10/100 de 4 puertos: Conectarse a la red de su empresa para trabajar desde casa o incluso crear su propia Red virtual privada entre diferentes sedes de su empresa puede ser una gran necesidad. Con el ruteador VPN de cable/DSL EtherFast se puede establecer simultáneamente hasta 70 sesiones independientes de Red virtual privada.

El ruteador VPN es compatible prácticamente con todos los sistemas operativos y estándares, lo que facilita su instalación y utilización; por eso el ruteador VPN de cable/DSL Instant Broadband™ EtherFast es la solución para las necesidades de banda ancha.

Emplea algoritmos de encriptación DES y 3DES, algoritmos de autenticación MD5 y SHA Y gestión de claves IKE. Actúa como un servidor DHCP en su red actual, tiene compatibilidad

con otros productos VPN IPsec. Emplea NAT, PPPoE, URL Filter, IP Filter y MAC Filter para asegurar la transmision de sus datos.

Figura 2.16
Router DSL Cable MODEM (solución implantada)

Los equipos mostrados hasta este momento son los que están orientados a la pequeña y mediana empresa por los precios que maneja cada equipo dependiendo del distribuidor oscila entre los 200USD a los 500USD. Es así como estas empresas pueden introducir tecnología con pequeñas inversiones que se reflejan a largo plazo en grandes beneficios.

La solución empleada en el desarrollo de esta tesis fue ésta última que mostramos; los equipos linksys BEFVP41 conectados como se muestra en la figura 2.16 con las características ya mencionadas en tres puntos distintos, el análisis de la red así como la implantación del sistema lo hacemos más adelante.

3 HERRAMIENTAS DE SEGURIDAD

3.1 Estuche de Herramientas de Seguridad

Un estuche de herramientas de seguridad es un término global que se refiere a la protección de los recursos de una empresa. No significa necesariamente que la organización deba conocer cada uno de los puntos vulnerables que existen en Internet o alrededor de su ambiente, más bien se refiere al hecho de estar consciente que la red de la empresa es vulnerable. Y que en sí, toda organización es vulnerable a ataques; no se vive en un mundo ideal. Se han desarrollado procesos y procedimientos que ayudan a reducir el impacto de los ataques, los cuales proporcionan un marco de referencia en el que una empresa puede examinarse a sí misma y aplicar medidas a aspectos individuales.

Muchos estuches de herramientas de seguridad tienen muchas cosas en común, pero difieren en los puntos finos. Por lo tanto, un estuche de herramientas de seguridad podría definirse como aquellos componentes que hacen que su red sea más segura y, si ocurre una intrusión, le permiten saber dónde buscar ayuda.

Es importante considerar siempre que el estuche de herramientas de seguridad para una empresa representa un traje hecho a la medida, por lo que es específico para cada una. Es por esto que, el conjunto de herramientas que funcione en una no garantiza que lo haga en otra.

Los aspectos que debemos considerar a la hora de utilizar cualquier herramienta son:

- la forma de realizar los ataques.
- la variedad de sistemas operativos existentes.
- la disponibilidad que puede hacer de las mismas un potencial atacante.

A continuación explicamos estos tres puntos:

La mayor parte de las herramientas existentes en el mercado se basan en indicios de vulnerabilidades para afirmar la existencia de las mismas, sin realizar el ataque que compromete a la máquina remota a través de dicha vulnerabilidad.

Por otra parte, existen multitud de sistemas operativos que operan utilizando el protocolo TCP/IP. Aunque la base del protocolo es común, las configuraciones y los servicios que se prestan suelen variar considerablemente, y por tanto las vulnerabilidades también. Existen ocasiones donde las herramientas no están preparadas para actuar de una forma u otra en función del sistema operativo que están auditando o protegiendo.

Por último, la disponibilidad de estas herramientas es más que un inconveniente, un aspecto que debemos considerar. El hecho de que nosotros podamos auditar externamente una máquina, implica que cualquier persona con acceso a través de la Internet a la máquina puede hacerlo para explotar posteriormente las vulnerabilidades que detecte. Para solucionar esto, las nuevas versiones de algunas herramientas, avisan a la máquina remota, que están realizando una auditoría de seguridad. Para dar ejemplo de estas herramientas a continuación se presentan algunas de las más populares (ver tabla 3.1).

Categoría	Herramienta	Descripción
Administración	BCM Detect	Prueba el sistema
	Data Advisor	Diagnósticos del sistema
Seguridad del sistema	Ballista	Herramientas de auditoría de seguridad en la red
	Bo Detect	Revisa en busca de una puerta trasera en un orificio posterior
	Crypto for 95/NT	Cifrado para archivos de PC
	Desktop 98 Surveillance	Supervisa el sistema y el uso de la red
	DIRT	Herramientas de intercepción de datos, disponible sólo para las agencias gubernamentales
	METZ Lock	Nulifica la acción de la combinación de teclas CRTL+ALT+SUPR
	NT Crack	Audita las contraseñas de NT
	PWDump	Se utiliza con NT Crack
	Revelation	Guarda las contraseñas en los archivos cifrados
	OfficeLock	Asegura varios archivos de aplicación
	WinU	Funciones de administración y seguridad

Tabla 3.1
Herramientas más populares para Windows 95 y NT

3.1.1 Herramientas de control y Seguimiento de Accesos

En esta clasificación se encuentran aquellas herramientas que nos permitirán obtener información mediante archivos de bitácoras o logs de todos los intentos de conexión que se han producido sobre nuestro sistema o sobre otro que nosotros hayamos señalado, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Este tipo de herramientas nos permite tener un control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP e ICMP, o analizando paquetes a nivel de aplicaciones (TELNET, FTP, SMTP, LOGIN, SHELL, etc.). Estas herramientas pueden ser utilizadas junto con otras que nos permitan definir desde qué máquinas permitimos ciertas conexiones y cuales se prohíben. Algunas de las herramientas descritas en este apartado no necesitan estar instaladas en la máquina que se quiere controlar, ya que se puede poner en una máquina cuya interfaz de red funcione en modo promiscuo, permitiendo seleccionar la dirección IP o máquina que queremos auditar.

Algunas de las herramientas descritas en este apartado pueden tener un doble uso. Es decir, permiten protegernos ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer los sistemas. También podrán ser utilizadas para realizar seguimientos en la red cuando creamos que alguna de nuestras máquinas ha sido comprometida.

El sistema primario de defensa de una computadora son los controles de acceso, sin embargo, con estos no se asegura totalmente el no tener intrusos. Existen muchos métodos para detectar intrusos.

- Análisis de bitácoras
- Monitoreo y análisis de la actividad de los usuarios
- Reconocimiento de ataques conocidos
- Monitoreo del tráfico en la red
- Verificación de la integridad de los archivos críticos del sistema
- Auditoría de la configuración del sistema y sus vulnerabilidades

3.1.1 Sistemas detectores de Intrusos

Estas herramientas pueden ayudar en la tarea de detectar y evitar actividades relacionadas con posibles ataques.

Bitácoras

Es una de las mejores herramientas para detectar intrusiones. Se manejan en cualquier sistema serio. Pero existe la posibilidad de que el intruso modifique las bitácoras para cubrir sus huellas.

Se pueden presentar algunos problemas como el hecho que la mayoría de los análisis son automáticos y muy grandes, por lo que nadie pone la atención necesaria para detectar una intrusión. Si se pone a una persona a vigilar el contenido de las bitácoras, será muy difícil leer todo lo que se produce y aun cuando lo leyera es difícil identificar los problemas al instante. La solución es contar con herramientas inteligentes que analicen las bitácoras por nosotros y estas son los "analizadores de bitácoras".

Monitoreo y análisis de la actividad de los usuarios

Otra forma para detectar la existencia de un intruso es contar con elementos que hagan saber si existe alguna alteración en las costumbres o reglas que cada usuario tiene para operar.

En cuanto a las metas a lograr con el monitoreo del sistema tenemos las siguientes:

1. Reducir la probabilidad de un ataque sin rastros lo más cercano posible a un 0%.
2. Incrementar la probabilidad de que los ataques que queden registrados sean reconocidos como tal lo más cercano posible a un 100%.

Considerando la primera meta puede surgir la siguiente pregunta; ¿Qué causa que un ataque no sea reconocido o no deje un registro? Hay 2 posibilidades para esto:

a) El evento o ataque desconocido para la red, del cual no tiene referencia de cómo detectar o registrar.
b) Se registró el evento o se trató de registrar, pero el mecanismo fue burlado por el atacante.

El primer caso se resuelve de manera sencilla: Simplemente hay que registrar todo. En la práctica sin embargo esto es muy difícil.

En una red ideal, deberíamos registrar todo evento posible para poder analizar qué ocurrió y poder reconstruir qué sucede en un momento dado. Para esto, deberíamos registrar todo paquete, todo comando, cada transacción de disco, y tener la capacidad de recrear el estado de la red en cualquier tiempo. Esto sería un sueño hecho realidad, pero en la realidad es muy impráctico. Para lograrlo se necesitaría que el sistema de registro o bitácora fuera tan basto como la producción de la red y consumir más recursos. Cabe resaltar la importancia de hacer un buen análisis que permita determinar las actividades que deben ser monitoreadas y que este análisis debe ser periódico, dicha periodicidad será de acuerdo a las necesidades de seguridad y el análisis de riesgos que se aplique a la empresa.

Claramente, si la red registra menos eventos, pueden pasar ataques sin ser notados y puedan ser serios. Sin embargo, la debilidad depende de los mantenimientos del sistema para

mantenerlo al día en cuanto a nuevos patrones de ataque. Esto es muy difícil y en algunos casos una tarea imposible.

También es importante que se considere como ataque cualquier conducta anómala detectada en la red y registra ese inusual patrón. El intruso puede tener nuevas formas de penetrar el sistema, y una vez dentro, pueden intentar algo más que espiar el sistema.

Finalmente, se deben de considerar las computadoras comprometidas. Si el atacante posee una máquina desde la cual puede ejecutar cualquier programa como usuario de la misma, teniendo la capacidad de burlar el sistema de registro. Si la máquina fue completamente comprometida, no se puede prevenir un ataque, pero si hacerlo menos significativo avisando al sistema de registro.

Detección de ataques conocidos

La mayoría de los atacantes usan herramientas o métodos desarrollados con anterioridad, por ellos mismos o, más frecuentemente, desarrollados por otras personas. Estos ataques tienen características muy específicas que es posible detectar. Para lograr una buena detección de estos ataques es imperante registrar lo necesario para reconocerlos.

Habiendo discutido acerca de qué debe ser registrado, debemos pensar acerca de estos mecanismos para implementar el sistema de monitoreo o registro del sistema.

Syslog

El mecanismo más común en una red es el syslog de TCP/IP. Syslog corre tanto en Windows y Unix, tiene adaptadores para permitirles conectarse al sistema de syslog.

El demonio de syslog es un programa que corre en segundo plano en todas las máquinas que ocupan syslog. Una característica más es que podemos hacer que el syslog no solo reporte sobre el propio servidor donde corre el demonio, sino sobre otros servidores a través de la red. Esto se consigue iniciando el demonio de syslog para "escuchar" a otros servidores.

Si se quiere incluir los logs producidos por los sistemas Windows a partir del NT (NT, 2000, XP, 2003) puede usarse el ntsyslog (http://ntsyslog.sf.net) que es un programa libre que manda el log de Windows a un servidor syslog. Hay varios productos además de los ntsyslog que no son gratuitos como el winsyslog

Interperiscope

Monitorea la máquina, mostrando cuándo su sitio de Internet, correo o servidor de DNS puede fallar. Esta herramienta de multi-propósitos ofrece un sistema anti-intrusos extensivo en un programa amigable al usuario que puede bajarse, instalarse y activarse en minutos.

http://www.internetperiscope.com/

Desktop 98 Surveillance

Mediante este programa es posible controlar en todo momento, incluso durante nuestra ausencia, el uso que se ha hecho de la computadora: navegación por Internet, uso de chat, y cualquier otro uso indebido. El programa funciona de una manera absolutamente invisible, y sin embargo, permite conocer desde las teclas utilizadas en nuestra ausencia a la captación de imágenes de nuestro escritorio que luego pueden ser vistas través de un vídeo de vigilancia.

Sam Spade

Herramienta de consulta de redes de distribución gratuita. Provee de una interfaz de usuario gráfica (GUI) consistente y de una implementación de varias tareas de investigación de red útiles. Fue diseñada con la idea de rastrear spammers, pero puede ser útil para muchas otras tareas de exploración, administración y seguridad. Incluye herramientas como ping, nslookup, whois, dig, traceroute, finger, explorador de web crudo, transferencia de zona de DNS {"DNS zone transer"}, comprobación de "relay" de SMTP, búsqueda en sitios web, y más.

3.1.2 Herramientas de Auditoría, monitoreo y detección de vulnerabilidades

Es útil para los administradores de una red auditar los servicios de la VPN y en general del sistema. El objetivo de cualquier auditoría de seguridad es detectar las vulnerabilidades que existen en una red de computadores, para poder pasar posteriormente a su reparación.

Aunque existen varias formas de realizar estas auditorías de seguridad, en todos los casos se utilizan herramientas para la detección de las vulnerabilidades. Estas herramientas vienen caracterizadas de la siguiente manera:

1. Son imprescindibles hoy en día para realizar auditorías de seguridad.- Las auditorías de seguridad se basan en la utilización de una o más herramientas que automáticamente detectan vulnerabilidades de las máquinas que analizan. Los tiempos donde la intuición y pericia de los administradores era la forma de detectar las vulnerabilidades han quedado atrás. Es criterio del auditor verificar la existencia de las vulnerabilidades que la herramienta ha detectado e incluso realizar comprobaciones manuales con vulnerabilidades que no hayan sido detectadas y de las que existan indicios de su existencia.

2. Exigen constantes actualizaciones.- Dado que su objetivo es la detección de hoyos de seguridad, es necesario que estas herramientas se actualicen con mucha frecuencia, ya que dichos agujeros de seguridad aparecen constantemente. Una herramienta que no se haya actualizado en un año no puede presentar garantías para la detección de vulnerabilidades, ya que ignorará las reportadas durante un período de tiempo donde pueden haber aparecido un número considerable, tal como lo acreditan los archivos del CERT.

3. Son compatibles con los sistemas operativos más usuales.- Dado que las LAN actuales se suelen caracterizar por la coexistencia de sistemas operativos diferentes, estas herramientas tienen versiones para los sistemas operativos más habituales en las LAN.

ISS (Internet Security Scanner)

Es la herramienta comercial más popular del mercado. ISS salió al mercado con carácter gratuito en un principio. Actualmente la compañía que la realiza ha implementado numerosas variantes de la herramienta para ser aplicada con carácter interno (SSS - System Security Scanner). Se encuentra disponible para la mayoría de las plataformas UNIX y para Windows NT. La versión más actual de ISS es la 5.2 para Windows NT y la 4.3.3 para plataformas UNIX.

Es una herramienta que busca y corrige rápidamente las brechas de seguridad mediante un análisis de vulnerabilidad automático y completo de la seguridad de la red. Explora y detecta las vulnerabilidades, clasifica por prioridades los riesgos de seguridad y genera una amplia gama de informes significativos que van desde análisis de tendencias de nivel ejecutivo hasta instrucciones detalladas para eliminar riesgos de seguridad.

Snort

Un sistema de detección de intrusiones (IDS) libre. Snort es un sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos {"stealth port scans"}, ataques a CGI, pruebas de SMB {"SMB Probes"}, intentos de reconocimientos de sistema operativos {"OS fingerprinting"} y mucho más. Snort utiliza un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. Mucha gente también sugirió que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort.

Ballista

Es una herramienta realizada por la empresa Security Networks de características muy similares a ISS. Existen versiones de Ballista disponibles para la mayoría de los sistemas UNIX y para Windows NT. La versión más reciente de Ballista es la 2.4. Aparte de realizar auditorías de seguridad, es probablemente la herramienta más potente para la presentación de resultados, realización de mapas de red auditada, etc.

Data Advisor

Es una herramienta de diagnóstico simple pero potente que sirve para evaluar el estado del sistema. Data Advisor realiza una rápida evaluación del estado de salud de su disco duro, sus estructuras de archivos y su memoria e identifica problemas que podrían causar una pérdida

de datos. Si no consigue arrancar su sistema en Windows, no se preocupe; Data Advisor arranca por sí mismo, por lo que se ejecutará aunque su sistema no pueda hacerlo.

Esta completa herramienta de diagnóstico puede usarse para diagnosticar problemas actuales y/o como parte de un programa de mantenimiento regular para identificar posibles problemas que pudieran producir pérdidas de datos. Si se identifican posibles problemas, tendrá tiempo de realizar copias de seguridad de su valiosa información y efectuar correcciones para evitar pérdidas en el futuro.

Patchwork

Herramienta de software que automatiza el proceso de encontrar vulnerabilidades e identificar la necesidad de parches. Trabaja en los sistemas Windows NT, Windows 2000 y Windows XP. Las características son; que revisa el sistema en busca de evidencia de archivos que usualmente son utilizados por los intrusos (con base en el FBI) y que analiza el Windows server en busca de vulnerabilidades conocidas que han sido explotadas por el grupo Russian hackers. Tiene algunas limitaciones porque no es una herramienta de verificación de parches completa, solamente ayuda a mejorar la vulnerabilidad y fue diseñado con base en información proporcionada por el FBI.

Hfnetchk

Herramienta de línea de comando que se puede utilizar para evaluar un sistema o un grupo de sistemas con respecto a la falta de parches de seguridad. Identifica si el sistema carece de algún Service Pack importante, y de esta manera descargar los parches necesarios para que la seguridad y fiabilidad de éste no se vean comprometidos.

Esta herramienta freeware se comunicará con una lista constantemente actualizada de los parches almacenados en el sitio web de soporte de Microsoft, y determinará de esta forma si nuestro sistema carece de algún parche crítico. Podemos utilizar esta aplicación para verificar un sistema, un grupo de sistemas o un dominio completo.

Existe una versión sencilla, para utilizar en la consola de comandos, y otra instalable más sofisticada con numerosas opciones; ambas gratuitas. El producto da soporte a los siguientes productos de Microsoft:

- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Internet Information Server (IIS) 4.0 y 5.0
- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft Internet Explorer 5.01 y versiones posteriores
- Reproductor de Windows Media 6.4 y versiones posteriores.

Para obtener la información, la utilidad hace uso de un archivo de configuración en formato XML que contiene la relación de los diferentes boletines de seguridad de Microsoft y los productos afectados por las diferentes actualizaciones.

El archivo XML (Extensible Markup Language) contiene:

- Información acerca de qué Hotfixes están disponibles para cada producto.
- Nombre y título de los boletines de seguridad.
- Datos detallados de Hotfixes de seguridad específicos para cada producto.
- Archivos en cada paquete Hotfix, sus versiones de archivo y checksums.
- Directivas del Registry que fueron aplicadas por el paquete de instalación.
- Información de que parches reemplazan a otros.
- Número del artículo de Microsoft Knowledge Base relacionado con el Hotfix.

Cuando se ejecuta por primera vez la herramienta (sin parámetros), debe obtener una copia de este archivo XML para que pueda encontrar los Hotfixes que están disponibles para cada producto. Este archivo está disponible en el sitio Web de Microsoft Download Center es un archivo .cab digitalmente firmado.

Hfnetchk descarga el archivo .cab, verifica la firma y lo descomprime en el sistema. Después de la descompresión del archivo, Hfnetchk escanea el sistema (o sistemas) para determinar el sistema operativo, service packs y programas que se están ejecutando. Hfnetchk analiza el archivo XML e identifica los parches de seguridad que están disponibles para el software instalado en el sistema.

Los parches disponibles para el sistema pero no están instalados actualmente son desplegados como “Patch NOT Found”.

Microsoft Baseline Security Analyzer

Analiza sistemas Windows con el objeto de detectar configuraciones de seguridad erróneas. El análisis se efectúa automáticamente, sin necesidad de intervención por parte del usuario, ni de tener conocimientos de administración. Sólo se selecciona el equipo a analizar, que puede ser cualquiera de los que estén conectados a la misma red, siempre y cuando se tengan privilegios de administrador en dicha máquina.

De esta forma se pueden encontrar errores de administración y fallos de seguridad comunes, pero no por ello menos importantes, tales como falta de actualizaciones del sistema, contraseñas caducadas, existencia de más de una cuenta de administrador o de una cuenta de invitado, qué directorios se comparten y con quién, posibles fallos en Internet Explorer, Office, SQL Server, Internet Information Server, etc.

Una vez finalizado el análisis, el programa muestra los resultados en un atractivo informe en formato HTML que se puede imprimir o copiar al Portapapeles.

No sólo se debe tener privilegios de administrador para poder ejecutar la herramienta en el sistema local o remoto, además de que se tiene que estar ejecutando el servicio de Server en el sistema. Para poder operar se requiere de un interprete XML versión 3.0 así como IIS Common Files son requeridos en el sistema donde esta instalada la herramienta para realizar un escaneo remoto de sistemas IIS.

Se ejecuta en equipos basados en Windows 2000 y XP, y puede buscar revisiones que faltan y vulnerabilidades de la seguridad en equipos basados en Windows NT 4.0, 2000 y XP.

Las características de esta herramienta son las siguientes:

- Interfaz gráfica y de línea de comando para escanear sistemas Windows (locales y remotos).
- Utiliza una versión de Hfnetchk.
- Crea y almacena reportes de seguridad XML individuales para cada sistema y despliega los reportes en una interfaz de usuario gráfica en lenguaje HTML.

Este programa tiene algunas limitaciones como son: no traba con Windows 95, windows 98 y windows Me, no trabaja en sistemas operativos diferentes al inglés.

Microsft Security Configuration Editor

Permite definir plantillas de seguridad en el sistema y comparar las configuraciones del sistema con una platilla de seguridad, así como también aplicarlas al sistema. En Windows NT es necesario instalar el archivo mssce.exe[1]. Las características de esta herramienta es que permite personalizar una plantilla de seguridad y aplicarla al sistema. Se puede bajar del siguiente ftp: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/SCM/SCESP4I.EXE

Permite escoger entre distintas plantillas, dependiendo del nivel de seguridad que se desee y del tipo de sistema al cual se aplique. Se encuentra disponible como freeware para los siguientes sistemas:

- Microsoft Windows NT
- Microsoft Windows 2000 y XP

1. Una vez que se instale el archivo mssce.exe (en Windows NT solamente, en Windows 2000 y XP esta instalado), seleccione *Start, Run* y escriba *mmc (Microsoft Managemet Console)* (figura 3.1).

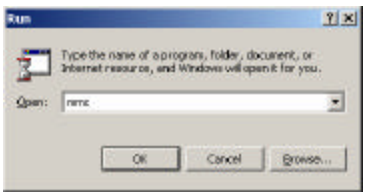


Figura 3.1
Ejecución MMC

[1] Windows 2000 y XP tienen MSCE integrados.

2. Aparecerá la ventana relativa al *MMC*, seleccione *Add/Remove Snap-in* del menú *Console*. A continuación seleccione *Security Configuration Manage,* OK y nuevamente OK.

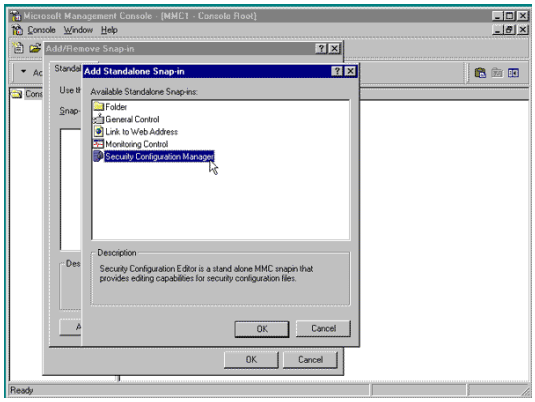


Figura 3.2
Menú console

3. Esta ventana mostrará la plantilla que esta instalada en el sistema (si existe alguna) y mostrará las posibles platillas a aplicar para el sistema, dependiendo su tipo.

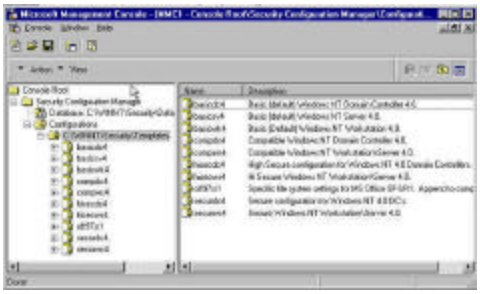


Figura 3.3
Plantilla instalada en el sistema

4. Se pueden configurar varios aspectos:

- Políticas de cuentas y locales.
- Grupos restringidos.
- Servicios del sistema.
- Compartimiento de archivos y directorios.
- Registry.
- Archivos de sistema.
- Almacenamiento en el sistema.
- Seguridad en Directorio.

Retina Network Security Scanner

Está diseñado para escanear cualquier sistema en Internet, Intranet o extranet con el objeto de identificar vulnerabilidades existentes, así como políticas de seguridad. Retina también proporciona ayuda para solucionar las vulnerabilidades encontradas, además de generar un reporte de vulnerabilidades. Se utiliza en sistemas Microsoft Windows NT, Windows 2000 y Windows XP. Esta herramienta incluye módulos de auditoría para las siguientes vulnerabilidades:

- NetBIOS
- HTTP, CGI and WinCGI
- FTP
- DNS
- Vulnerabilidades DoS
- POP, SMTP y LDAP
- TCP/IP y UDP
- Registry
- Servicios
- Usuarios, Cuentas y passwords
- Publishing extensions
- Database servers
- Firewalls y Routers
- Proxy Servers
- Interfaz gráfica
- CHAM (common hacking attack methods)
- Fix-It
- Escaner pequeño
- Auto Update
- Arquitectura abierta

Sport y Fport

Herramienta de línea de comando que reporta todos los puertos TCP/IP y UDP abiertos y los mapea con su correspondiente aplicación. Requiere utilizar el archivo psapi.dll. Es un freeware disponible para los sistemas Windows NT y Windows 2000, y sólo funciona en ellos.

En Windows NT, psapi.dll debe estar en el mismo directorio o ruta que fport. Para Windows 2000, no es el caso debido a que el sistema contiene este dll. Proporciona información sobre puertos abiertos, ID del proceso, aplicación y la ruta de la aplicación.

Sintaxis: Fport [/h] [/a] [/i] [/ap] [/ap] [/p]

Switch	Descripción
/a	Ordena la salida por aplicación.
/i	Ordena la salida por el ID del proceso.
/ap	Ordena la salida por ruta de aplicación.
/p	Ordena la salida por puerto.
/h	Ayuda

Figura 3.4
Menú comando Fport

Para utilizarlo se debe abrir una ventana de command prompt y transladarse al directorio conteniendo el archivo fport y el dll asociado. Finalmente, ejecutar fport con el parámetro deseado. El resultado será similar al siguiente:

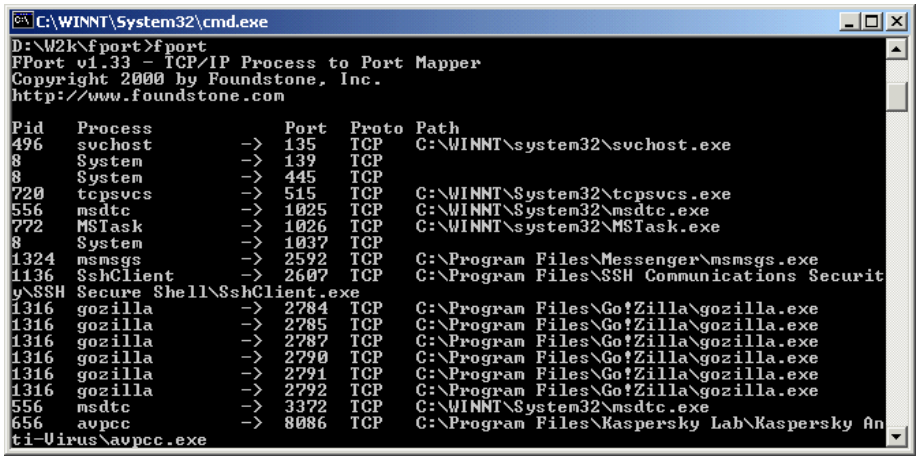


Figura 3.5
Ventana cmd

3.1.3 Herramientas Adicionales para la Seguridad del Sistema

Las herramientas adicionales para la seguridad de nuestro sistema, son indispensables para mantener la integridad y la confiabilidad de nuestro sistema en general.

Algunas herramientas que pueden ayudar son:

3.1.3.1 Herramientas de Administración y permisos de acceso a los recursos

El sistema se encuentra casi listo para salir a la red Internet, pero aun falta detallar aspectos de administración para completar la seguridad del sistema.

Los temas relacionados con la administración segura se basan en el **modelo de seguridad de Windows 2000 y Active Directory.**

La Seguridad en Windows 2000 se basa en los componentes:

- Active Directory
- GPO (Group Policy Objet)
- Sistema de Archivos NTFS V.5
- EFS y ACE
- Kerberos V.5, LM, NTLM v1, NTLM v2, IPSEC.

A continuación se describirán brevemente cada uno de los componentes:

Active Directory

Windows 2000 tiene la posibilidad de ser compatible con estaciones de trabajo y servidores con versiones anteriores.

Un *Domain Controller* puede trabajar en dos modos *Nativo o Mixto* de acuerdo a la versión de los sistemas de sus clientes.

Modo Nativo. Dominio con controladores exclusivamente Windows 2000.
Modo Mixto. Dominio con controladores de dominio Windows NT 4.0, 95/98 y 2000.

Importante: El cambio de modo mixto a nativo es irreversible, así que debe tomar en cuenta los factores anteriores para determinar cuándo se debe hacer el cambio.

EAP

El protocolo de autenticación ampliable (EAP) es una extensión de PPP, que proporciona un mecanismo de soporte estándar para los esquemas de autenticación como las tarjetas token, Kerberos, Clave Pública y Clave/S, y está totalmente soportado tanto en Windows NT Dial-up Server como en Dial-up Networking Client. EAP es un componente de tecnología crítica para las VPN's seguras, protegiéndolas de la fuerza bruta de un ataque de diccionario o que las contraseñas sean adivinadas.

EAP permite que los módulos de autenticación de terceros interactúen con la implementación de una VPN de Servicio de acceso remoto (RAS) Microsoft Windows NT. La

disponibilidad de EAP en Windows NT es una respuesta a la creciente demanda para aumentar la autenticación RAS con dispositivos de seguridad de terceros.

EAP es una extensión propuesta por IETF para PPP que permite que los mecanismos arbitrarios de autenticación se empleen para la validación de una conexión PPP. EAP se diseñó para permitir la adición dinámica de módulos de conexión de autenticación tanto del lado del cliente como del servidor de una conexión. Esto permite que los proveedores suministren un nuevo esquema de autenticación en cualquier momento. EAP proporciona la máxima flexibilidad en variedad y singularidad de autenticación. Se planea que EAP se pondrá en marcha en Microsoft Windows 2000.

GPO Policy

Group Policy Objects, proveen una poderosa forma de asegurar que todos los usuarios se apeguen a las políticas de cómputo establecidas en la empresa. Las *GPO policy* permiten las siguientes características:

- Configurar políticas centralizadas y descentralizadas.
- Asegurar que los usuarios tengan su entorno.
- Reforzar las políticas que la empresa tenga definidas.

Tipos de políticas son:

- *Local Group Policy* (Políticas Locales).
- *Active Directory Group Policy* (Políticas de Dominio).

Los contenedores hijos, heredan las configuraciones de las GPO de los contenedores padres. Para evitar que la herencia de políticas aplicadas en el Dominio afecte a los objetos se *Bloquea la herencia*.

Windows 2000 cambia las políticas de GPO a los Domain Contoller, Usuarios y Computadoras, por default los *Domain Controller* verifica cada 5 minutos las políticas cambiadas. Los *Usuarios y Computadoras* verifican los cambios cada 90 minutos por default.

Para que Windows 2000 aplique a Usuarios, Computadoras Clientes, sin tener que reiniciar la máquina, se utiliza el refresh para forzar que las GPO se modifiquen mediante el siguiente comando:

secedit refreshpolicy machine_policy /enforce

Kerberos

Kerberos es llamado así por el perro de tres cabezas que cuidaba las puertas de Hades (Infierno) en la mitología griega. Surgió en el MIT y existe una implementación gratuita y se encuentra también el código disponible. También existe en muchas versiones comerciales. Actualmente utiliza la encripción DES.

Kerberos es una herramienta interesante pues además de autenticar a los usuarios, también genera y administra las llaves de cifrado al mismo tiempo (figura 3.6)

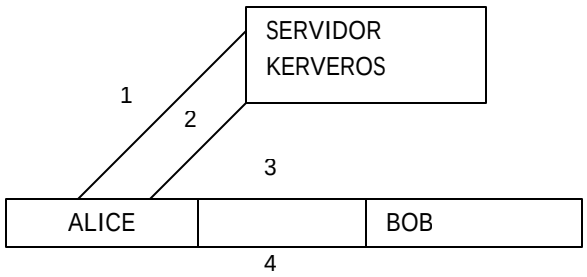


Figura 3.6
Un intercambio Kerberos, todos los intercambios son cifrados y autenticados.
1. Alice solicita aun ticket y una llave al servidor. 2. Alice recibe el ticket y la llave del servidor.
3. Alice presenta el ticket y la llave a Bob. 4. Bob verifica el ticket y le da acceso a Alice.

El Protocolo Kerberos se basa en una técnica de autenticación llamada *secretos compartidos.* Significa que yo conozco un secreto y se lo cuento sólo a usted. El secreto es lo único que compartimos.

Para poder utilizar este tipo de inicio de sesión, necesitará primero instalar un servidor de certificados Windows 2000 y después cargar en él las plantillas de certificados específicas para el inicio de sesión mediante tarjetas inteligentes.

Configuración de directivas Kerberos:

- Haga clic en inicio, barra de Tareas| Run/Ejecutar, escriba mmc haga clic en Aceptar (Ok).
- Ejecute opción Agregar/Quitar Complemento, en la pantalla nueva de clic en Agregar/Add
- En el cuadro de diálogo Agregar un complemento independiente, seleccione la Directiva de Grupo(Group Policy), de clic en Agregar.
- El cuadro de edición Objeto de directiva de grupos de clic en Examinar(Browse), de clic en Default Domain Policy (directiva de dominio predeterminada), después de Aceptar (Ok).
- De clic en Finish (Finaliza), Cerrar y Aceptar.
- Ahora que tenemos MMC configurada, podemos establecer las directivas de dominio para kerberos.

Para establecer directivas de Kerberos:

- Haga clic en **+** que hay junto a la directiva Default Domain Policy.
- Seleccione Configuración de Equipo/Configuración de Windows/Configuración de Seguridad/Políticas de Cuenta/Política Kerberos.
- De clic en política que quiera cambiar

Beneficios:

- Una autenticación más eficiente
- Autenticación mutua.
- Autenticación delegada
- Manejo simplificado de relaciones de confianza.
- Interoperabilidad con otros sistemas operativos.

Passfilt.dll

Passfilt.dll es una librería de Windows que nos obliga a utilizar contraseñas que sigan unas características específicas de seguridad. No aceptará las claves que no las cumplan. Por ejemplo, obliga a combinar mayúsculas y minúsculas, números, longitud adecuada.

Passprop

Herramienta de línea de comando que permite bloquear la cuenta de Administrador del sistema, así como también permite habilitar una política de password fuerte. Esta herramienta es de fácil manejo y permite establecer políticas de passwords fuertes.

Se necesita cargar la herramienta Passprop desde el Kit de recursos de Windows NT. Passprop, que se muestra en la figura 3.7, requiere que los usuarios creen una contraseña en la que combinen números o símbolos con letras mayúsculas y minúsculas. Al establecer estos requisitos, incrementa en gran medida el tiempo que necesita para romper las contraseñas un cracker que utiliza la fuerza bruta.

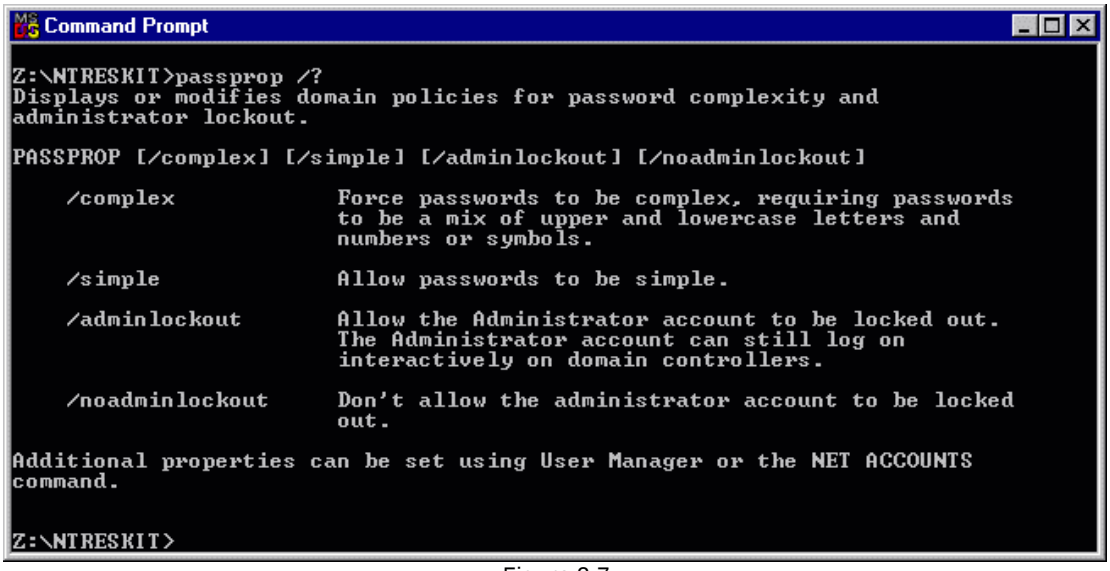


Figura 3.7
La herramienta Passprop puede incrementar en gran medida la seguridad de la red

Con tales limitaciones, algunos usuarios elegirán una contraseña como Viernes13. Cuando la contraseña caduque no podrán volver a utilizarla, porque Windows NT recuerda las contraseñas anteriores, así que pueden cambiarla a Viernes14. La herramienta Passprop comprueba si la contraseña nueva es similar a la anterior y si es así la rechaza.

La herramienta Passprop puede bloquear la cuenta administrador, si éste escribe mal la contraseña varias veces. Como característica de seguridad, el administrador puede conectarse al servidor localmente incluso si la cuenta está bloqueada.

SSH

Secure Shell permite realizar la comunicación y transferencia de información de forma cifrada proporcionando fuerte autenticación sobre el medio inseguro (red). Provee fuerte autentificación y comunicación segura sobre un canal inseguro; reemplaza comandos inseguros: telnet, ftp, rlogin, rsh y rcp; seguridad para conexiones de servicios X Windows y envío seguro de conexiones arbitrarias TCP, además utiliza algoritmos de cifrado: Blowfish, 3DES, IDEA, RSA.

Es una manera segura de acceder a computadoras remotas. Un reemplazo seguro para rlogin/rsh/rcp. OpenSSH deriva de la versión de ssh de OpenBSD, que a su vez deriva del código de ssh pero de tiempos anteriores a que la licencia de ssh se cambiara por una no libre. ssh (secure shell) es un programa para loggearse en una máquina remota y para ejecutar comandos en una máquina remota. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables {"untrusted hosts"} sobre una red insegura.

Este programa sólo está disponible, para Windows 95, 98, Me o NT (en las versiones más recientes incluyendo 2000), es decir, no existe una versión para MS-DOS o Windows 3.1 ó 3.11.

La configuración del cliente es bastante sencilla, bastará con realizar los siguientes pasos:

1. Instalación del programa.
2. Crear un directorio en el disco duro de su la computadora. Sugerimos SSH, dentro de Archivos de programa.
3. Ejecutar el programa ssh32.exe haciendo un doble clic sobre él.
4. Lo primero que le aparece es una pantalla informativa, pulse sobre el botón de OK

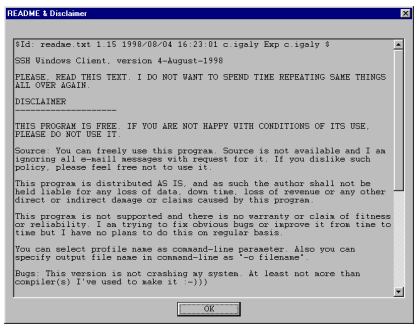


Figura 3.8
Pantalla Informativa SSH

5. Lo siguiente en aparecer es una ventana en la que se le pide que introduzca el nombre de la librería de encriptación (DLL). Si en Windows está configurado como viene por defecto (Ocultar archivos de ciertos tipos), deberá escribir crypt32.dll en la casilla correspondiente al nombre del archivo

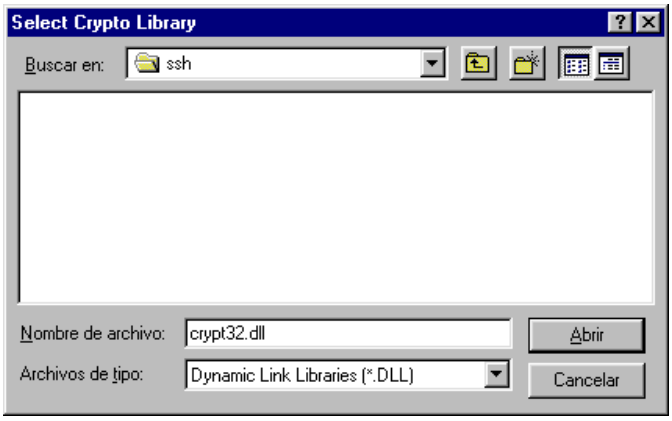


Figura 3.9
Nombre de archivo

6. Finalmente, aparece una ventana para definir una nueva conexión, pero en este caso la cerramos pulsando el botón Cancel.

Figura 3.10
Nueva Conexión

7. Lo primero que se debe realizar, antes de crear una nueva conexión, es generar una clave, para ello debe seleccionar el item Generate Key del menu Keys.

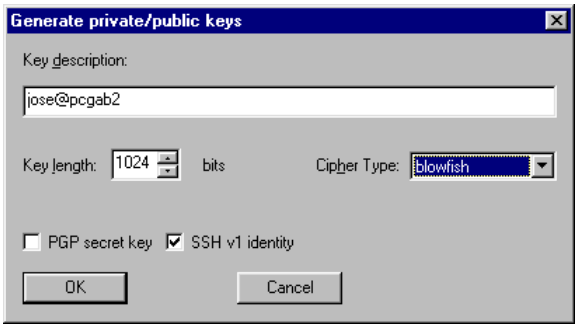


Figura 3.11
Generar una clave

En el campo Key description, se debe poner algo que identifique quien ha generado la clave, por ejemplo el usuario y el equipo en el que se ha generado.

Cuando se termine de generar la clave, se le pedirá que introduzca los passphrase o frase clave. ES mejor elegir una frase larga y complicada. Teniendo en cuenta que cuanto más larga y complicada será mejor, pues con este sistema cualquiera puede comprometer la seguridad de los datos de otras personas. Si alguien consigue entrar con una clave, generalmente tendrá la posibilidad de observar los datos de cualquier otra persona.

Figura 3.12
Definición de passphrase

8. Finalmente, pulse el botón OK y aparecerá una pantalla en la que se pide el nombre del archivo donde se almacenará la clave. Si se trata de una computadora compartido, es conveniente asignarle un nombre del tipo id usuario. Siendo usuario el nombre que uno desee. Además de este archivo se creará otro con el mismo nombre pero con la extensión .PUB

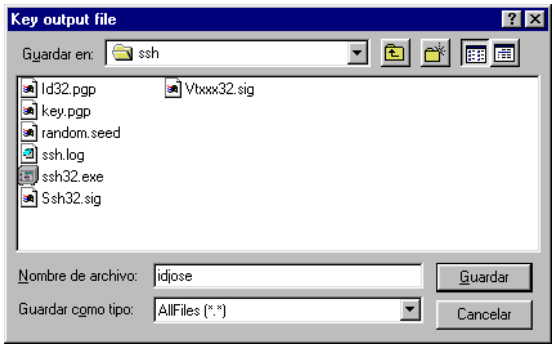


Figura 3.13
Archico .PUB

9. Una vez hecho esto, se puede definir una nueva conexión, para ello deberemos seleccionar el item Connection del menu Action.

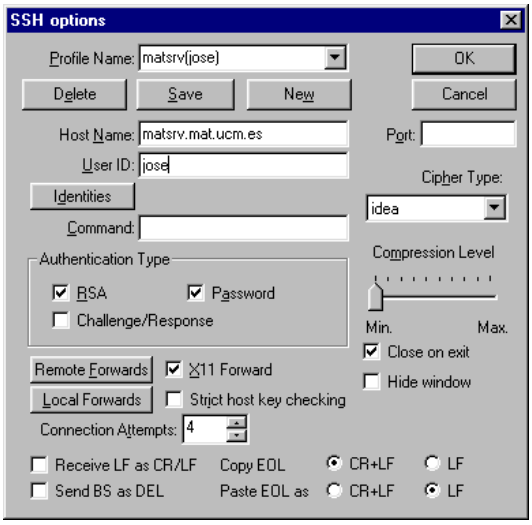


Figura 3.14
Menú Item Connection

10. Aquellos valores que no se comenten, déjelos tal y como aparecen en la pantalla. Las casillas importantes a completar son:

    Profile name. Se establecerá un nombre reconocible para la conexión. Recuerde que si trabaja con un equipo compartido, es conveniente agregarle el nombre del usuario que definió la conexión.

    Host name. Es el nombre de la máquina con la que deberá conectarse.

    User ID. Es el nombre del usuario con el que intentará conectarse a l a máquina que ha escrito en la casilla anterior.

11. Una vez que ha rellenado los campos anteriores, ahora es necesario declarar las identidades o archivos de clave, para ello, en función de la clave generada en el paso 6, seleccione el tipo de cifrado Cipher Type y a continuación pulse sobre el botón Identities. Aparecerá una ventana en la que se pide que debe pulsar sobre el botón New.

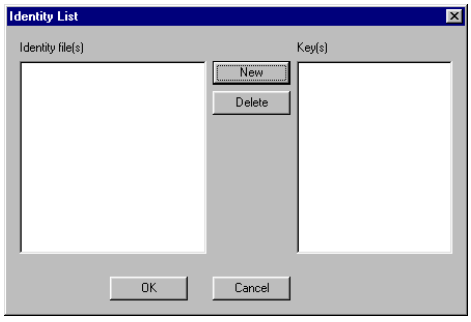


Figura 3.15
Identity list

- Aparece una ventana en la que debe seleccione el archivo en el que esta almacenada la clave. Escoja el archivo creado en el paso 8, pero el que no tiene la extensión .PUB.

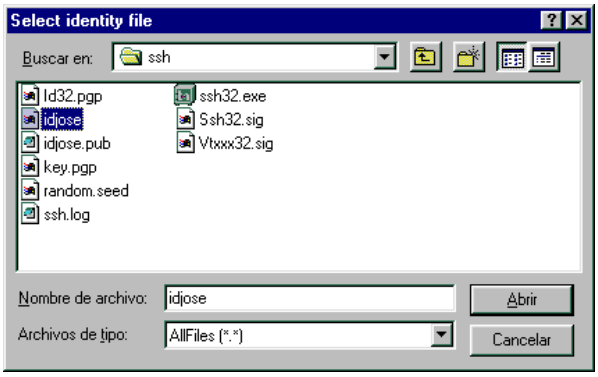


Figura 3.16
Salvar Identity file

12. Una vez seleccionado el archivo que contiene la clave, le aparecerá la siguiente ventana, en la que se indican el archivo que contiene la clave seleccionada y algunos de los datos referidos a ella. Pulse sobre el botón Ok para cerrar la ventana.

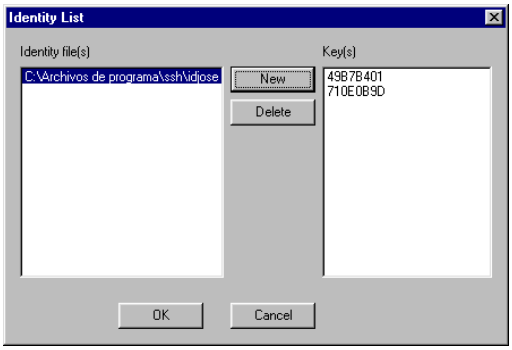


Figura 3.17
Identity list

13. Ahora deberá pulsar sobre el botón Local Forwards para definir los túneles de FTP necesarios. Le aparecerá la siguiente ventana:

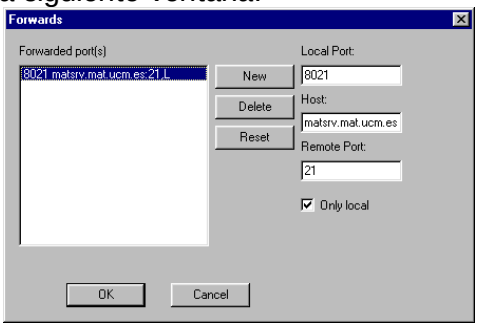


Figura 3.18
Local Forwards

14. Pulse sobre el botón New, deberá rellenar los datos Local Port y Remote Port con los valores numéricos de 8021 y 21 respectivamente y en Host deberá escribir el nombre del equipo que ha definido en el paso 9, es decir, el equipo con el que va a conectar. Active la casilla de Only Local y pulse el botón OK. Para terminar, repita el paso 13 para los valores 8020 y 20.

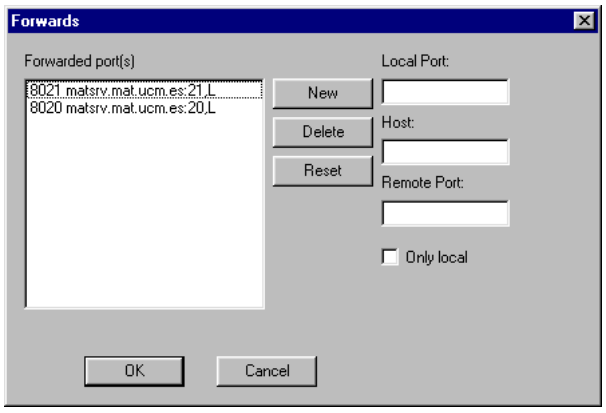


Figura 3.19
Local Forwards para valores 8020 y 20

Para terminar de configurar el programa es necesario que pulse sobre el botón Save de la ventana que aparece en pantalla, a saber, la que figura en el paso 9.

15. Ahora que ha terminado la configuración del programa ya puede conectarse con la máquina, pulsando sobre el botón OK. Le aparecerá la siguiente ventana en la que por ser la primera vez que se conecta con esta máquina se le pide confirmación para aceptar la clave del equipo al que se conecta. Acéptela pulsando sobre el botón Accept Key o sobre Accept Once si sólo desea aceptarla para esta sesión.

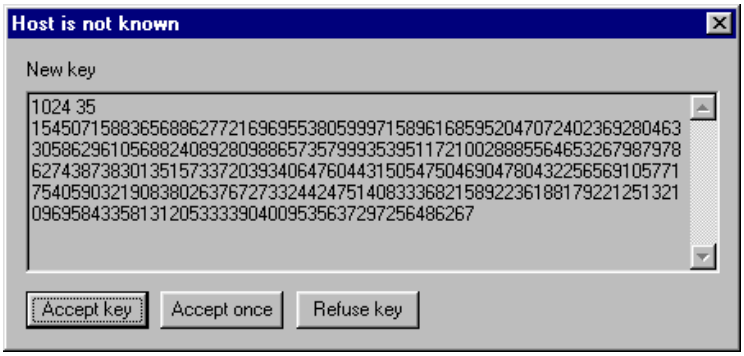


Figura 3.20
Ventana de primera conexión SSH

- Como la frase clave (passphrase) no está autorizada, pasa a un modo telnet y le pregunta por su clave unix.

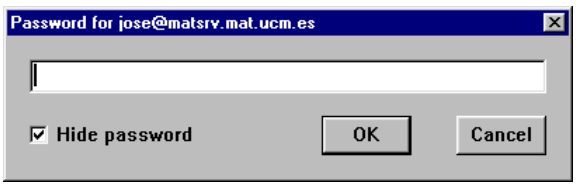


Figura 3.21
Solicitud de passphrase

Si no existe en su directorio home un directorio denominado .ssh créelo con los siguientes permisos:

```
matsrv(1):/home/ochoa/jose%mkdir.ssh
matsrv(1):/home/ochoa/jose%chmod 755 .ssh
```

Si no tenía el directorio .ssh en su directorio home, deberá crear dentro de este un archivo denominado authorized_keys y añadirle la clave pública que se ha generado en el paso 6.

```
matsrv(1):/home/ochoa/jose%cd .ssh
matsrv(1):/home/ochoa/jose%touch authorized_keys (1)
matsrv(1):/home/ochoa/jose%vi authorized_keys
```

(1) Advertencia. Si ya disponía del archivo authorized_keys, simplemente añada la clave pública, no ejecute este paso.

Para añadir la clave abra con un editor de texto de Windows (Notepad) el archivo de clave pública generado en el paso 6, el que tiene la extensión .PUB. Marque todo el texto a excepción del último carácter, que es el que corresponde con el final de línea y pulse <Control-C> (Copiar). Retorne a la ventana de la sesión ssh que tendrá en ejecución el editor vi y si el archivo a editar no tiene líneas de texto pulse la tecla <i>, si ya tiene líneas de texto, sitúese en la última línea con las teclas del cursor y pulse la tecla <o> y finalmente seleccione Paste del menú Edit, lo que pegará la ristra de números y letras que ha copiado anteriormente. Para salir grabando, pulse un par de veces la tecla <Esc> y luego teclee ":wq".

Una vez grabada la clave pública, cerramos la conexión tecleando logout o exit en nuestra ventana de conexión ssh. Volvemos a conectarnos al equipo seleccionando el item Connection del menú Action y seleccionamos el Perfil de nuestro equipo, que debiera ser el único, pues se trata de una instalación y configuración del cliente ssh para Windows. Ahora bien, si hemos hecho los pasos anteriores correctamente, la ventana que nos aparecerá será la siguiente:

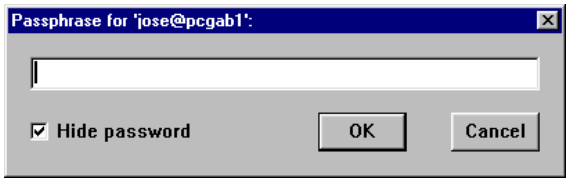


Figura 3.22
Solicitud de passphrase en equipo con perfil configurado

En la que se solicita la clave privada, passphrase o frase clave para conectarse a la máquina UNIX.

Finalmente, lo que deberemos hacer al igual que en los otros sistemas operativos es cambiar nuestra clave UNIX por otra diferente a cualquiera de las máquinas en las que tenemos cuenta que no es accesible por ssh, es decir, que no sea ninguna de las que tenemos en otras máquinas que no son accesibles mediante ssh. Un ejemplo aclaratorio, no utilizar la misma clave que en EUCMAX, EUCMOS, EMDUCM1, o cualquiera de las estaciones de Matemáticas o equipos con Linux que no dispongan del sistema ssh. El consejo final es que la clave sea lo más complicada posible. Si ya hubiera cambiado la clave, porque ha instalado otro cliente ssh, no será necesario realizar este paso.

```
matsrv(1):/home/ochoa/jose%passwd
Old password:********
New password:********
Re-enter new password:********
```

3.1.4 Herramientas para obtener muestras en la organización

Estas herramientas son útiles para evaluar las vulnerabilidades de la organización mediante la simulación de ataques a la red. La mayoría de estas herramientas se encuentran disponibles en Internet sin costo alguno y se pueden clasificar del mismo modo que clasificamos las herramientas anteriores. Las podemos englobadas como herramientas hacker pues pueden utilizarse tanto en beneficio como en contra de la organización por hackers.

Antes de proceder a hacer una evaluación de vulnerabilidades mediante ataques simulados con herramientas hacker, es recomendable seguir los siguientes pasos:

Preparar una computadora para realizar las evaluaciones o monitoreos. Es en este equipo que se instalarán las diferentes herramientas. Se recomienda que sea un equipo portátil para sondear diferentes puntos de la red de la Organización.

Evitar conectarse a sitios hacker usando direcciones del dominio de la Organización.

Hacer una lista de las pruebas a realizar, tanto internas como externas, precisando el servicio y puerto que se desea probar, así como el tipo de ataques que se simularán sobre dicho servicio. Estas listas deben incluir pruebas al top ten de las vulnerabilidades de moda.

NTcrack

Se puede utilizar sobre Internet para procurar entrar como administrador usando una base de datos de contraseñas, hasta que una contraseña se encuentre que trabajó. Para prevenir

tales ataques, debe estar seguro de inhabilitar el establecimiento de una red de SMB vía protocolo de TCP/IP (con cortafuegos o manipulando atascamientos del NT) y/o examinar periódicamente los registros del acontecimiento de la seguridad para tales ataques.

Ethereal

Es un analizador de protocolos de red para Unix y Windows, y es libre. Nos permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se quiera ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.

Netcat

La navaja multiuso para redes. Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad del tipo "back-end" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta rica en características, útil para depurar {debug} y explorar, ya que puede crear casi cualquier tipo de conexión que se pueda necesitar y tiene muchas habilidades incluídas.

TCPDump / WinDump

El sniffer clásico para monitoreo de redes y adquisición de información. Tcpdump es un conocido y querido analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red ("network interface") que concuerden con cierta expresión de búsqueda. Podemos utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión {port} para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades. Hay que tener en cuenta que muchos usuarios prefieren el sniffer más nuevo Ethereal.

DSniff

Un juego de poderosas herramientas de auditoría y pruebas de penetración de redes. Este popular y bien diseñado set hecho por Dug Song incluye varias herramientas. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy monitorean pasivamente una red en busca de datos interesantes (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante -- por ej. debido al uso de switches. sshmitm y webmitm implementan ataques del tipo monkey-in-the-middle activos hacia sesiones redirigidas de SSH y HTTPS abusando de relaciones {"bindings"} débiles en sistemas con una infraestructura de llaves públicas {PKI} improvisados.

Ettercap

Ettercap es un interceptor/sniffer/registrador para LANs con ethernet basado en terminales. Soporta disecciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También es posible la inyección de datos en una conexión establecida y filtrado al vuelo y aun manteniendo la conexión sincronizada. También soporta plugins. Tiene la habilidad para comprobar si estamos en una LAN con switches o no, y de identificar huellas de sistemas operativos (OS fingerprints) para poder conocer la geometría de la LAN.

Whisker/Libwhisker

El escáner y la biblioteca de vulnerabilidades de CGI de Rain.Forest.Puppy. Whisker es un escáner que nos permite poner a prueba servidores de HTTP con respecto a varias agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts/programas que utilicen CGI. Libwhisker es una biblioteca para perl (utilizada por Whisker) que nos permite crear escáneres de HTTP a medida.

3.1.5 Encriptación

La seguridad VPN se mejora con el uso de encriptación para proteger contraseñas además del contenido de paquetes de datos. Las claves que se utilizan para cifrar datos se derivan de las credenciales del usuario y no se transfieren por cable. Cuando se termina la autenticación se verifica la identidad del usuario, y se utiliza la clave de autenticación para la encriptación.

Tanto los protocolos de encriptación y compresión opcionales inherentes PPTP y L2TP como la seguridad adicional de encriptación, pueden agregarse implementando el protocolo IPsec. Se pueden utilizar varias tecnologías de encriptación para proporcionar seguridad de datos con las VPNs.

3.1.5.1 Encriptación Simétrica

La encriptación simétrica o de clave privada (también conocida como encriptación convencional) se basa en una clave secreta que se comparte por dos partes que están en comunicación. La parte que envía, utiliza la misma clave secreta como parte de la operación matemática para encriptar (o cifrar) el texto sencillo. La parte que recibe, utiliza la misma clave secreta para desencriptar (o descifrar) a texto sencillo. Algunos ejemplos de los esquemas de encriptación simétrica son: el algoritmo RAS RC4 (que sienta las bases para la encriptación de punto a punto de Microsoft), estándar de encripción de datos (DES), el Algoritmo Internacional de Encriptación de Datos (IDEA) y la tecnología de encriptación Skipjack propuesta por el gobierno de los estados Unidos para utilizarse en el chip Clipper o el nuevo Algoritmo Internacional AES.

3.1.5.2 Encriptación Asimétrica

La encriptación asimétrica o de clave pública utiliza dos claves diferentes para cada usuario: una es la clave privada que solo conoce el usuario, la otra es la clave pública correspondiente que puede acceder cualquier persona. Las claves privadas y públicas están relacionadas matemáticamente por el algoritmo de la encriptación. Una clave se utiliza para la encriptación, y la otra para la desencriptación, dependiendo de la naturaleza del servicio de comunicación que se esté implementando. Asimismo las tecnologías de encriptación de clave pública permiten que se coloquen firmas digitales en los mensajes; una firma digital utiliza la clave privada del emisor para encriptar una parte del mensaje. Cuando se recibe el mensaje, el receptor utiliza la clave pública del emisor para descifrar la firma digital y verificar la identidad del emisor.

Con la encriptación simétrica, tanto el emisor como el receptor tienen una clave secreta compartida. La distribución de la clave secreta debe ocurrir antes que cualquier comunicación encriptada (con protección adecuada). Sin embargo, con la encriptación asimétrica, el emisor utiliza una clave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una clave pública para descifrar estos mensajes. La clave pública puede distribuirse libremente a cualquiera que necesite recibir los mensajes encriptados o firmados digitalmente. El emisor necesita proteger cuidadosamente sólo la clave privada.

3.1.6 Firewalls

3.1.6.1 La primera línea de defensa

El firewall es un sistema diseñado para impedir los accesos no autorizados desde y hacia una red protegida.

El firewall es como la puerta principal de una casa, que se abre o cierra de acuerdo a los criterios y necesidades definidos por sus habitantes. Estas definiciones, denominadas “reglas”, son la base de la administración de los firewalls. La puerta controla la entrada y salida de la gente a la casa.

La simplicidad del concepto es lo que lo hace tan poderoso ya que aplicando las reglas adecuadas en cada lugar, podemos controlar todo el tráfico que viaja entre las redes que da servicio el firewall y así proteger la red interna.

En la vida real los firewalls se utilizan para separar y filtrar el tráfico entre las redes; por ejemplo, en el caso de un usuario de banda ancha, el firewall estaría entre su PC e Internet, protegiendo al usuario mientras está expuesto a Internet. En este caso, la red definida por el firewall es la misma PC, una red de un solo equipo.

Este lugar privilegiado que ocupan en la red los convierte en la primera línea de defensa, consolidándose como una de las herramientas fundamentales de la seguridad de la seguridad y privacidad de información.

3.1.6.2 Tipos de firewalls

Se pueden identificar tres grandes grupos, en función de los criterios de diseño y el segmento de mercado al que apuntan.

Firewalls de hardware

Son equipos que incluyen en el mismo gabinete todo el software y hardware para operar. Tradicionalmente utilizados en grandes empresas, logran los mejores rendimientos dada la integración del software y hardware.

Desde hace un tiempo han aparecido otros productos más económicos destinados al mercado de usuarios de banda ancha, que hacen hincapié en la facilidad de instalación, configuración y mantenimiento para usuarios sin experiencia. Como ejemplos podemos citar a Cisco Pix (uno de los líderes del mercado corporativo, que también ofrece versiones para pequeñas empresas) y Linksys (uno de los más atractivos para los usuarios finales, dada su relación costo-beneficio).

Firewalls de software corporativos

En esta categoría tenemos aplicaciones que corren sobre los sistemas operativos más populares: NT, Unix, Linux, etc. Hay modelos que protegen redes enteras y otros específicos para defender servidores.

Como deben convivir con el sistema operativo, son más complicados de instalar y mantener, además del hecho que necesitan personal con conocimiento del producto y el sistema operativo. Una ventaja es la flexibilidad, ya que permiten adaptarse al software y al hardware disponible.

Muchas empresas utilizan tambiés este tipo de firewalls. Como ejemplo podemos citar Checkpoint FW1 (el líder desde que apareció en el mercado por el año 1994/95, con versiones para Unix y NT). Symantec, dispone de Enterprise Firewall 7.0.

Firewalls personales

Se trata de una categoría relativamente nueva, que surgió como respuesta a las necesidades de los usuarios de PC de banda ancha y navegación en Internet. Están diseñados para brindar la máxima seguridad posible, haciendo un balance entre el nivel de protección, facilidad de uso y mantenimiento. La mayoría tienen asistente de configuración, así como también varias configuraciones predeterminadas que ayudan a mantener un alto nivel de

seguridad sin perder funcionalidad. Muchos de ellos poseen servicios de actualización automática y suman capacidades de detección de tráfico malicioso, y algunos incluso permiten bloquear los avisos pop-up tan comunes en muchos sitios de Internet.

Una característica común a todos los productos es la capacidad que tienen de "ir aprendiendo" las reglas necesarias junto con el usuario, de modo que cuando detectan un tipo de tráfico nuevo "preguntan" lo que deben hacer. Las opciones siempre son permitir o prohibir un determinado intento de conexión. Esta capacidad es muy importante, porque permite al usuario estar al tanto de todo lo que está ocurriendo en su PC con respecto a la entrada y salida de datos de su equipo.

A pesar de ser muy sencillos de operar, hay muchas consideraciones a tener en cuenta según el escenario donde se utilicen. Quizás el usuario más simple sea el de un usuario con un único PC conectado a Internet, donde el firewall protege cualquier intento de conexión proveniente de Internet que no haya sido pedido por el usuario. Pero la situación es más complicada cuando el usuario trabaja en una pequeña red, y además del acceso a Internet debe conectarse a otros equipos, impresoras, etc. Estos casos exigen un determinado conocimiento de los programas y conexiones, muchas veces más allá del usuario promedio.

Todavía los productos de firewall personal están más avanzados en plataforma Windows, aunque todas las distribuciones de Linux tienen la posibilidad de utilizar el firewall del sistema operativo, denominado "ipchains" o "iptables" dependiendo de las versiones.

Los siguientes son algunos firewalls personales (comerciales) para plataforma Windows.

- Norton Personal Firewall 2002, de Symantec
- Tiny Personal Firewall, de Tiny Software
- McAfee Personal Firewall, de McAfee
- ZoneAlarm Pro, de Zone Labs
- Sygate Personal Firewall Pro, de Sygate Technologies
- Freedom Personal Firewall, de Zero-Knowledge Systems
- Black Ice Defender, de Internet Security Systems
- Firewall para conexión a Internet de Microsoft, nativo del Windows XP

3.1.6.3 Selección de un firewall

Uno de las mayores preocupaciones que tienen las empresas hoy día es cómo llevar a cabo sus transacciones electrónicas manteniendo altos niveles de seguridad y confidencialidad. La conectividad total se ha convertido en una necesidad para poder sobrevivir en el ambiente competitivo del nuevo milenio. Esto ha traído, al mismo tiempo, serios problemas de seguridad al facilitar el acceso desde el mundo exterior a través de Internet y así exponer los recursos internos de la red.

Para impedir que personas no autorizadas penetren en la red o que accedan a más información

de la permitida, se utiliza un sistema de defensa perimetral llamado en firewall (cortafuego), el cual se coloca como una barrera de protección entre Internet y la red local de la empresa. A veces se utilizan firewalls adicionales internamente para separar distintos departamentos. A la hora de implantar un sistema de esta naturaleza, surgen preguntas como las siguientes:

- ¿Cuál tipo de firewall conviene utilizar?
- ¿Cómo debe ser configurado?
- ¿Qué pruebas se van a efectuar para verificar que el firewall se comporta cómo se esperaba?
- ¿Quién va a efectuar el mantenimiento?
- ¿Cómo se va a dar soporte y adiestramiento?

Un sistema basado en firewalls no es la panacea para la seguridad. Continuamente se descubren fallas en los productos comerciales y aparecen nuevos tipos de ataques. Y lo que es peor, la mayoría de los sistemas se configuran mal y carecen de mantenimiento.

La de Selección e Instalación de Firewalls debe garantizar que el firewall que se vaya a utilizar funcione siempre perfectamente y brinde la máxima seguridad. En caso de que el firewall ya haya sido adquirido o instalado se deben definir las reglas que se aplicarán en los firewalls.

Las reglas especifican el origen, destino, servicio y acción a realizar para cualquier transacción. También definen que eventos deben guardarse bitácoras (logs). La primera regla es usualmente no permitir cualquier acción a no ser que esté permitida expresamente, puesto que las posibles brechas de seguridad son más fácilmente identificables de esta manera. Es imprescindible que la política de seguridad esté diseñada de acuerdo a los activos de información que se quieren proteger y a las condiciones específicas de cada empresa. Se deben definir los requerimientos de comunicaciones internos y externos para así convertirlos en la base de la política de la empresa. También es importante entrevistar al personal clave de todas las áreas para garantizar que todas las variables sean consideradas.

Los pasos a seguir para implantar un firewall que brinde la seguridad esperada son en resumen los siguientes:

- Evaluación de firewalls comerciales y recomendaciones
- Estudio de costos de adquisición, implantación y mantenimiento
- Desarrollo de la política de seguridad para los activos de información del cliente
- Las reglas completas para el firewall, en forma escrita
- El firewall configurado con dichas reglas
- Pruebas bajo operación normal
- Pruebas de vulnerabilidad
- Pruebas bajo ataques de negación de servicio (DoS)
- Informe final

La mayoría de los firewalls emplean una combinación de técnicas para llevar a cabo su labor de la forma más eficiente y segura.

¿Donde se encuentran los riesgos?

Uno de los ataques favoritos de los intrusos para lograr sabotear una maquina es el uso de SYN de comunicación para inundar la maquina de peticiones que no se culminan lo que agota los recursos del sistema y no permite establecer nuevas conexiones, otro es el uso de la detección de los números de secuencia, para identificar el sistema y mas adelante manipular la comunicación por medio de un ataque de repetición.

Ahora detrás de esta estructura los ataques mas frecuentes no se realizan a través la capa de transporte, sin embargo los ataques profesionales si.

Ataques mas frecuentes

Los ataques mas frecuentas que encontramos en la red son los de las aplicaciones, en este tipo de ataque no entraremos en gran detalle debido a la la gran cantidad de estos y al numero de aplicaciones disponibles según cada sistema operativo, la importante en este punto es poder revisar el contenido de los paquetes de información que viajan sin importar si son o no encriptados (SSL HHTPS entre otros) puesto que este tipo de paquetes son los que hacen los aplicativos mas vulnerables dado que no los inspeccionan muchos Firewalls.

El filtrado de paquetes, la utilización de servidores proxy y la traducción de direcciones de red (NAT) son, en la actualidad, las técnicas más utilizadas.

Algunos protocolos, como por ejemplo Telnet y SNMP, se pueden manejar con más efectividad con filtrado de paquetes. Otros (como FTP o HTTP) se manejan con más efectividad con servidores proxy.

El firewall debe poder configurarse para bloquear todo tipo de tráfico entrante o saliente, excepto para algunos servicios en caso de ser necesarios, tales como:

TELNET	En el puerto 23, a menudo se permite sólo a algunos sistemas
FTP	FTP, en los puertos 20 y 21, se permite sólo a algunos sistemas
http	
HTTPS	
SMTP	SMTP, en el puerto 25, se permite sólo a algunos servidores de correo centrales
DNS	DNS, en el puerto 53, proporciona información sobre los hosts y que pudiera ser útil para un atacante

Los siguientes servicios son inherentemente vulnerables y no deberían autorizarse:

- TFTP (Trivial FTP)
- X Windows, en los puertos arriba de 6000
- RPC (Remote Procedure Call) en el puerto 111
- Rlogin, rsh y rexec, en los puertos 513, 514 y 512

El firewall debe permitir llevar un registro de todos los eventos y en particular de todos los accesos permitidos, así como de todos los intentos de acceso fallidos. El firewall debe poseer un sistema de gestión local y remota para facilitar su configuración y elaborar reportes de auditoría. Las sesiones de administración debe realizarse encriptadas y se requiere un mecanismo de autenticación robusto para tener acceso al firewall.

Se recomienda visitar el sitio www.icsa.net y consultar los siguientes documentos: Annual ICSA Firewall Buyer's Guide y Firewall Product Certification Criteria

3.1.6.4 Análisis de costos

A continuación se refieren algunos de los costos que deben ser considerados al momento de elegir un firewall:

- Costos no recurrentes
- Hardware
- Software
- Adiestramiento
- Certificados digitales, tokens, tarjetas inteligentes
- Sueldos del personal a cargo del firewall
- Honorarios de consultores externos
- Mantenimiento
- Seguro
- Actualizaciones y parches
- Auditoría

Con base en ellos y en las necesidades de la empresa se podrá elegir la opción más segura que se encuentre dentro del presupuesto de la organización. Según el nivel de seguridad la organización puede considerar que requiere un grado mas alto o bajo de seguridad, hay que recordar que mas siempre es mejor en seguridad pero mas significa mucho mas precio; trate de equilibrar lo que requiere su organización contra el presupuesto que dispone y los servicios a los que acceden los clientes o la misma organización.

3.1.6.5 Firewalls y VPNs

Como ya vimos los firewalls son otro método para asegurar la integridad de la red corporativa regulando estrictamente qué datos pueden entrar a la red privada desde Internet. Existen dos enfoques para la utilización de las técnicas firewall con una VPN.

Un servidor de túnel VPN puede instalarse al frente de un firewall, detrás de un firewall o en la misma máquina. La forma más lógica y comúnmente usada es utilizar para ello el estándar IPsec.

El motivo por el que se coloca el servidor de VPN en el firewall es evidente: colocarlo detrás de él haría que el tráfico cifrado entrante y saliente generado por el servidor VPN no pudiese ser inspeccionado totalmente y hubiera que obiar funciones como las de autenticación, logging, escaneo de virus, etc. sobre todo ese tráfico. Colocando el servidor VPN detrás del firewall lo hacemos vulnerable a ataques directos.

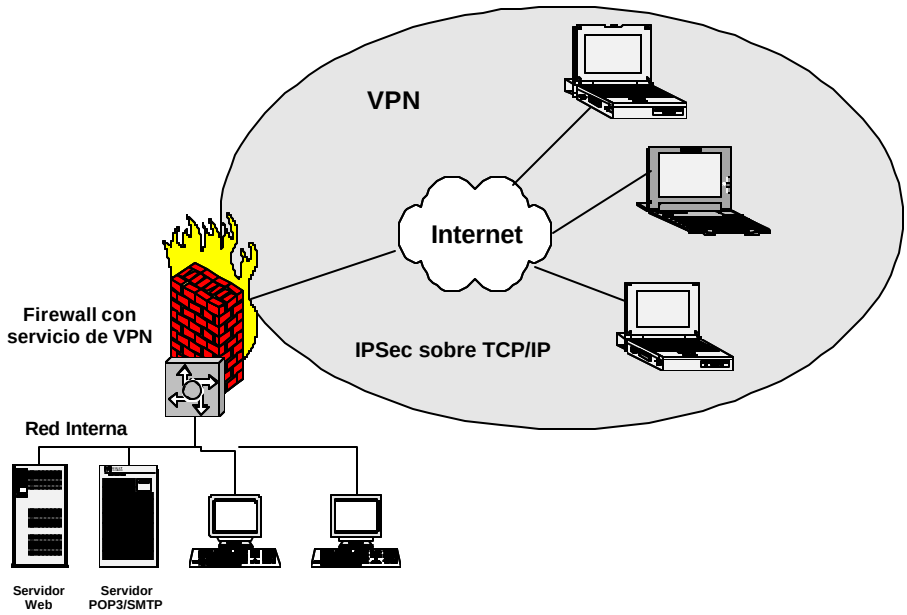


Figura 3.23
Ejemplo de una VPN con firewall integrado

Asimismo, como ya se mencionó antes, un firewall puede colocarse al frente de un servidor VPN. Esta solución aunque posible, da como resultado paquetes que son analizados por el servidor. Además existe más riesgo si se permite el paso a los paquetes basados en PPTP a través de un servidor VPN. Estos paquetes no los puede contabilizar el firewall, ya que ambos están comprimidos y cifrados. El riesgo de seguridad que conlleva dicha configuración se confina a quien posee un empleado a quien se le ha permitido el acceso remoto. El empleado que tiene acceso LAN también enfrenta cada día este riesgo interno. Esta configuración y los riesgos que implican, son suficientes para una aplicación Intranet.

Algunas organizaciones (debido a los recursos restringidos), quizá también deseen instalar un firewall en la misma máquina que el servidor VPN. Bajo estas circunstancias, una sola máquina dirige el tráfico que recibe el servidor al firewall para ser analizado. Este enfoque es el más económico y se recomienda para Intranet o comunicaciones específicas de la compañía.

http://www.creangel.com/nuke/html/modules.php?name=News&file=article&sid=174

4 ANÁLISIS DE REQUERIMIENTOS

4.1 Requerimientos del entorno de la VPN

4.1.1 Estructura de un sistema de cómputo

Antes de examinar los componentes de un sistema de cómputo seguro, es muy útil revisar la estructura de un sistema de cómputo estándar. Las partes de un sistema de cómputo pueden estar divididas en dos tipos básicos de componentes, *hardware* y *software* (para temas relacionados con seguridad, la combinación de hardware y software considerado como *firmware* deberá ser considerado en los temas concernientes tanto a hardware como software).

El *hardware* puede ser dividido en grandes grupos como dispositivos de entrada y salida (I/O), almacenamiento secundario, memoria principal y unidad central de procesamiento (CPU), tal y como se muestra en la figura 4.1. Para nuestros propósitos, el *software* estará dividido en dos categorías, el Sistema Operativo (SO) o bien software de sistema y software de aplicación.

Una computadora de un solo procesador ejecuta un programa en cualquier momento dado. Debe buscar la instrucción que será ejecutada desde la memoria, la decodifica, la ejecuta, guarda cualquier resultado y después repite el ciclo. El sistema operativo es un conjunto de programas especiales que administra los recursos y controla la operación de la computadora. En muchos aspectos, el sistema operativo sirve como un buffer entre las aplicaciones y el hardware. La relación entre cada uno de estos elementos se representa por una serie de círculos concéntricos como se describe en la figura 4.2

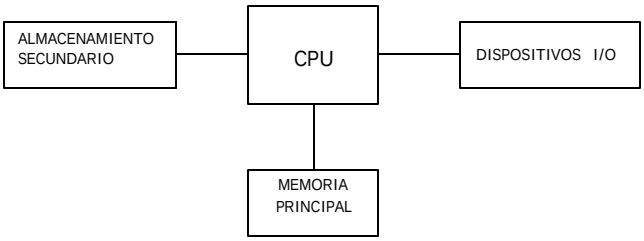


Figura 4.1
Componentes de hardware de un sistema de cómputo

El software aplicativo consiste en los programas diseñados para realizar una tarea específica utilizando los recursos del sistema. Dentro de los ejemplos de programas aplicativos podemos incluir manejadores de bases de datos, procesadores de palabra, hojas de cálculo, software de administración de proyectos, paquetes de comunicaciones y aplicaciones de negocios hechas o no a la medida.

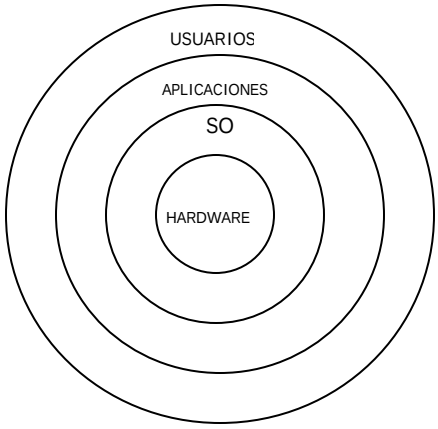


Figura 4.2
Capas en un sistema de cómputo

4.1.2 Planeación, Diseño e Instalación de la VPN

Los problemas recurrentes de una red se atribuyen a una pobre planeación, diseño e instalación. Desafortunadamente muchas redes nunca fueron planeadas o diseñadas,

simplemente sucedieron. La instalación generalmente es descuidada, con componentes de red instalados por gente con muy poca experiencia con o sin un entendimiento de redes.

Se deben conocer las bases que lo preparen para implementar la VPN. Estos pasos son críticos, cada componente que se agregue a la red debe ser tratado como dispositivo de la misma y tendrán siempre la misma importancia y el mismo trato. Ya que al agregar una pieza de equipo nueva a la infraestructura ya existente siempre aparecen problemas de interoperabilidad.

4.1.3 Componentes de red

Una red no es más que un grupo de computadoras conectadas mediante cables o algún otro medio. Sin embargo. El proceso de crear una red no tiene nada de simple. Cuando las computadoras son capaces de comunicarse entre sí, pueden trabajar juntas de varios modos: compartiendo recursos con los demás, distribuyendo el procesamiento de una tarea particular o intercambiando mensajes.

Un componente de red es un dispositivo activo que la provee de las funciones de intercomunicación de los sistemas. Podemos dividirlos en **componentes simples**, como ruteadores y concentradores de terminales y los **componentes complejos**, como servidores o estaciones de trabajo.

Un **componente simple** es un componente diseñado para manejar una sola tarea específica, como el ruteo de la red, y cuya configuración se maneja de una forma más uniforme.

Un **componente complejo** es aquel cuya función puede variar, compartirse entre distintas tareas y cuya función puede administrarse en distintos puntos y de distintas formas. Además puede variar de acuerdo a la función que se esté implementando.

Para el funcionamiento de una red local se necesitan varios componentes que realizarán determinadas tareas. A grandes rasgos son los siguientes:

4.1.3.1 Servidores y Sistemas Centrales

Es aquel equipo que permite compartir los archivos y programas que se encuentren en su(s) disco(s). Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

Debemos asegurar que estos sistemas sean instalados en áreas con la ventilación, temperatura y acondicionamiento apropiados aún en días no laborables. Por razones de seguridad es importante proteger los contactos de corriente eléctrica y controlar el acceso físico, especialmente para los servidores de archivos y de tiempo compartido, es también recomendable que el servidor principal de la VPN, el cual será el proveedor del enlace, no se ocupe también como estación de trabajo. Este servidor deberá estar siempre bloqueado y sólo el administrador de la red debe conocer la contraseña.

Cuando sea posible, se debe mantener la consistencia de estos sistemas y sus componentes. Pues la resolución de problemas es más sencilla con menores tipos de marcas de CPU's, tarjetas Lan, discos de sistema, etc.

4.1.3.2 Estaciones de trabajo

Una estación de trabajo se define como la computadora, generalmente una PC o una minicomputadora, incluyendo los componentes físicos y lógicos contenidos en el ambiente de trabajo. Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras.

A diferencia de una computadora aislada, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.

Al igual que con los servidores, mantener la consistencia hace que la resolución de problemas sea más sencilla y reduce el costo de mantenimiento. La consistencia también provee la facilidad de intercambiar estaciones de trabajo, haciendo más fácil sustituir un sistema en una emergencia.

En nuestro caso específico proponemos la arquitectura Intel para Cliente Servidor, que soporte por lo menos el sistema operativo Windows 98.

4.1.3.3 Sistema Operativo de Red y Estructuras lógicas

Es necesario que exista un sistema operativo para que administre las funciones de la red. Este sistema tiene dos partes: la del servidor de archivos y de las estaciones de trabajo.

Un sistema operativo de red para una red dedicada se ejecuta en servidores autónomos, prestando servicios de los servidores que ya habíamos mencionado antes:

- Servidor de archivos.
- Servidor o pasarela de correo electrónico.

- Servidor de comunicaciones.
- Servidor de base de datos
- Servidor de copia de seguridad y de almacenamiento.
- Servidor de fax.
- Servidor de impresión.
- Servidor de servicios de directorio.

En el caso de la VPN que queremos diseñar es importante, como se mencionó en párrafos anteriores, que el software de sistema de las computadoras del sistema se haga de una forma consistente para facilitar la detección y resolución de problemas en el sistema. Esto significa estandarizar la estructura del directorio del servidor archivos, nombres de usuario, archivos de booteo, scripts de ingreso a la red y menús. La consistencia hace más fácil la identificación de problemas pues no se tiene que aprender el funcionamiento de cada sistema enlazado en red.

Organizar directorios en un servidor de archivos en una red es distinto a cuando se organiza en una estación de trabajo. La organización lógica para un solo usuario concierne a la información de a esa única estación. En un servidor de archivos, sin embargo, debe considerar una organización lógica para múltiples usuarios, así como la seguridad y el control de acceso.

El directorio de un servidor de archivos debe tomar la mejor ventaja de la seguridad del sistema operativo en red. Además, debe ser leído por varios clientes y poder realizársele mantenimientos de una manera sencilla.

Las cuentas de los usuarios deben también ser lo más consistente posible. Utilizando, por ejemplo, un esquema estándar de nombramiento de usuarios y directorios raíz para facilitar el trabajo de mantenimiento.

Consideraciones de seguridad en el Sistema Operativo

El Sistema Operativo provee potencialmente el medio de acceso a todos los archivos y aplicaciones, es un componente intangible, que mientras se encuentra en uso, está almacenado en la memoria. Podemos considerar como el componente más importante para proteger un acceso no autorizado, ya que si alguien no autorizado penetra como un usuario privilegiado puede acceder libremente a archivos sensibles, aplicaciones y dispositivos; haciendo que cualquier otra medida de seguridad de nuestra red se vuelva ineficaz.

La seguridad de un servidor o estación de trabajo, incluyendo todos sus componentes pueden expresarse en términos de una clasificación de “niveles de seguridad”, mismos que expondremos más adelante.

4.1.3.4 Software de aplicación

Como ya mencionamos, todos los elementos anteriores, son el funcionamiento para que el usuario de cada estación, pueda utilizar sus programas y archivos específicos. Este software puede ser tan amplio como se necesite ya que puede incluir procesadores de palabra, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados por ejemplo, control de producción, correo electrónico, etc.

4.1.3.5 Sistema de Cableado

El sistema de cableado es probablemente el componente más crítico en toda la red. Un diseño o instalación pobre del sistema de cableado puede dificultar la corrección de problemas o causar tiempo fuera de servicio innecesario.

Un buen sistema de cableado es diseñado para ser fiable, administrable y de mantenimiento sencillo. La mejor guía para cableado es el C*ommercial Building Wiring Standard: ANSI/EIA/TIA-568-4966,* este documento es el resultado del esfuerzo conjunto de distintos grupos de estándares para la industria con el afán de crear una aproximación de estándar para cableado.

Para una instalación apropiada es importante encontrar a alguien con los conocimientos apropiados para instalar cableado para una red de área local. Se debe verificar que se utilicen los tipos y grados apropiados de los cables y que todas las longitudes de los cables cumplan con las especificaciones correctas. También se deben verificar que se utilicen los conectores y los bloques correctos.

Es necesario documentar el sistema de cableado. Un buen diagrama del sistema de cableado y un etiquetado apropiado de cables y placas de pared ayudarán a evitar pérdidas de tiempo en la solución de problemas.

Existe una gran cantidad de tipos de cables. Algunos fabricantes de cables publican un catálogo con más de 2.000 tipos diferentes que se pueden agrupar en tres grupos principales que conectan la mayoría de las redes:

- Cable coaxial.
- Cable de par trenzado (apantallado y no apantallado).
- Cable de fibra óptica.

Actualmente el cable de par trenzado y el de fibra óptica son los tipos de cables más comunes.

4.1.3.6 Tarjetas de red

Cada nodo de la red, o sea la estación de trabajo o servidor de archivos, debe contar con una tarjeta de red. La tarjeta de red del servidor de archivos puede ser ligeramente diferente de las utilizadas en las estaciones de trabajo.

Las tarjetas de red, también denominadas NIC (Network Interface Cards, tarjetas de interfaz de red), actúan como la interfaz o conexión física entre el equipo y el cable de red. Las tarjetas están instaladas en una ranura de expansión en cada uno de los equipos y en el servidor de la red.

Después de instalar la tarjeta de red, el cable de red se une al puerto de la tarjeta para realizar la conexión física entre el equipo y el resto de la red.

La función de la tarjeta de red es:

- Preparar los datos del equipo para el cable de red.
- Enviar los datos a otro equipo.
- Controlar el flujo de datos entre el equipo y el sistema de cableado.
- Recibir los datos que llegan por el cable y convertirlos en bytes para que puedan ser comprendidos por la unidad de procesamiento central del equipo (CPU).

En un nivel más técnico, la tarjeta de red contiene el hardware y la programación firmware (rutinas software almacenadas en la memoria de sólo lectura, ROM) que implementa las funciones de control de acceso al medio y control de enlace lógico en el nivel de enlace de datos del modelo OSI.

La tarjeta de red realiza tres funciones importantes coordinando las actividades entre el equipo y el cableado:

- Realiza la conexión física con el cable.
- Genera las señales eléctricas que circulan por el cable.
- Controla el acceso al cable siguiendo unas reglas específicas.

Para seleccionar la tarjeta de red apropiada para la red, primero es necesario determinar el tipo de cable y los conectores que tendrá. Cada tipo de cable tiene características físicas diferentes, a las que la tarjeta de red debe adaptarse. Cada tarjeta se ha construido para aceptar al menos un tipo de cable.

Si una tarjeta tiene más de un conector de interfaz y no tiene detección de interfaz predeterminada, debe realizar una selección configurando jumpers en la propia tarjeta o usando una opción seleccionable por software. La documentación de la tarjeta de red debe contener información sobre cómo se puede configurar la tarjeta de forma apropiada.

Una conexión de par trenzado utiliza un conector RJ-45. El conector RJ-45 es similar al conector telefónico RJ-11, pero tiene un tamaño mayor y tiene ocho conductores; un RJ-11 sólo tiene cuatro conductores.

4.1.4 Conceptos y preocupaciones en una Red

Las redes son una vía abierta de ataques desde diferentes lugares, por distintos lugares, por distintos medios, y por diferentes razones. En este contexto, el ámbito de preocupaciones respecto a la seguridad de las redes también es múltiple, y esto se debe, entre otras, a las siguientes razones:

- Se comparten recursos.
- Se utiliza un sistema complejo.
- Se desconoce el perímetro.
- Existen muchos puntos de ataque.
- Existe el anonimato.
- No se puede verificar la trayectoria de la información.

La seguridad en redes involucra también una serie de acciones que se pueden y deben tomar en cuenta para mejorarla. Para ello, es fundamental entender una serie de conceptos básicos esenciales para la seguridad de cualquier red o sistemas. Muchos de ellos han sido explicados a lo largo del capítulo 1 y otros serán explicados a lo largo de este capítulo. Pero a continuación se describen de forma específica para nuestra VPN.

Conocer al enemigo

Este concepto involucra a los atacantes e intrusos. Se debe considerar quién o quienes pueden querer violar las medidas de seguridad e identificar sus motivaciones. Igualmente, determinar qué es lo que pueden querer hacer y el daño que pueden causar.

Las medidas de seguridad no pueden hacer imposible a un atacante realizar acciones no autorizadas. Sólo intervienen para hacerles más difícil la tarea. El objetivo es asegurar que las medidas que se tomen estén más allá de las capacidades o motivaciones del atacante.

Calcular el Costo

Las medidas de seguridad casi siempre reducen la eficiencia del sistema, especialmente para usuarios sofisticados. Estas medidas pueden provocar el retardo de los trabajos y

encarecer la administración. Pueden requerir recursos significativos de cómputo y requerir hardware especial, etc.

Cuando se diseñan medidas de seguridad, se debe entender su costo y comparar esos costos contra los beneficios potenciales. Para lograr esto, se deben entender los costos de las medidas mismas y de posibles hoyos de seguridad. Si se obtienen costos de seguridad fuera de proporción con respecto a los daños, entonces se estaría haciendo a sí mismo un daño.

Identificar las suposiciones

Cada sistema de seguridad está soportado por una serie de suposiciones. Por ejemplo, se puede asumir que los atacantes conocen menos de lo que en realidad se hace en el sistema o red, que ellos usan software estándar, etc. Se debe estar seguro de examinar y justificar todas las suposiciones. Cualquier suposición oculta es un potencial hoyo de seguridad.

Controlar los secretos

La mayoría de medidas de seguridad se basan en secretos, tales como llaves de cifrado y passwords. Sin embargo, con frecuencia esos secretos no son todo lo secreto que deben ser. La parte más importante de mantener secretos es conocer las áreas que se deben proteger. ¿Qué conocimiento requiere un atacante para infiltrar el sistema? Se debe asegurar el no comprometer ese conocimiento y asumir que cualquier otro conocimiento es conocido por el atacante.

Lo difícil es mantener los secretos realmente secretos. Los sistemas se deben diseñar de tal manera que sólo requieran un limitado número de secretos.

Recordar el factor humano

Muchos procedimientos de seguridad fallan porque sus diseñadores no consideran cómo los usuarios reaccionan a ellos. Por ejemplo, los passwords generados automáticamente no son fáciles de recordar ya que carecen de sentido y los usuarios los escriben en papel y los dejan frente al monitor o al lado del teclado.

Por comodidad, módems no autorizados se conectan con frecuencia a Internet para evitar mensajes molestos o restricciones que imponen las medidas de seguridad.

Si las medidas de seguridad interfieren con el uso esencial del sistema, habrá resistencia para respetar tales medidas y tal vez serán evadidas. Para que se respeten las medidas de seguridad, se debe asegurar que los usuarios puedan realizar su trabajo sin problemas ni incomodidades, y tratar de que comprendan la necesidad de las medidas de seguridad.

Cualquier usuario puede comprometer la seguridad del sistema, al menos en algún grado. Por ejemplo, alguien (un atacante) se puede hacer pasar por el administrador del sistema y llamar por teléfono a algún usuario y solicitar su password. Si los usuarios comprenden los

problemas de seguridad, y comprenden las razones de las medidas de seguridad, ello hará más difícil la vida de los intrusos.

Como mínimo, los usuarios deben aprender que nunca deben revelar sus passwords u otros secretos, y menos sobre líneas telefónicas inseguras (especialmente teléfonos celulares) o correo electrónico. Algunas empresas han implementado entrenamiento en seguridad en redes seguras para sus empleados.

Conocer las debilidades

Todo sistema de seguridad tiene vulnerabilidades. Se deben conocer los puntos débiles del sistema y saber cómo pueden ser explotados por los atacantes. También se deben conocer las áreas de mayor riesgo y prevenir los accesos a ellas. Conocer los puntos débiles es el primer paso para convertir esos puntos o áreas en seguros.

Limitar el Alcance de los Accesos

Se deben de crear barreras apropiadas dentro del sistema de tal forma que si los intrusos accedan una parte del sistema, no puedan automáticamente tener acceso al resto del sistema. La seguridad de un sistema o red es solamente tan buena como el nivel de seguridad más débil de cualquiera de sus nodos.

Entender el ambiente

El comprender la forma en que el sistema funciona normalmente, conocer cuál es la conducta esperada y cuál pude ser una conducta anómala, y familiarizarse con la forma en la cual se usan los dispositivos, ayuda en mucho a detectar problemas de seguridad. El notar eventos inusuales puede ayudar a detectar intrusiones antes de que puedan dañar al sistema. Las herramientas de auditoria pueden ayudar a detectar eventos inusuales.

Limitar la confianza

Se debe conocer exactamente cuál software es confiable, y el sistema de seguridad no debe confiar en la suposición de que todo el software que usa está libre de errores.

Recordar la seguridad física

El acceso físico a las computadoras o cualquier componente sensible usualmente otorga a usuarios suficientemente sofisticados el control total sobre ese dispositivo. El acceso físico a un enlace permite espiar en ese enlace, bloquearlo, o insertar tráfico. No tiene sentido instalar software sofisticado de seguridad cuando no se controlan los accesos al hardware.

Cualquier cambio que se realice sobre el sistema puede tener efectos en la seguridad. Esto es especialmente cierto cuando se crean nuevos servicios. Los administradores, programadores, y usuarios deben considerar las implicaciones de seguridad de cambio que hagan. Entender las implicaciones de seguridad de un cambio toma alguna práctica. Requiere entender efectos colaterales y disposición para explotar cada manera en que un servicio puede ser potencialmente manipulado.

4.1.5 Necesidades de seguridad en la red

Antes de examinar como aplicar la seguridad en la red, se requiere un entendimiento mínimo de la organización en red. Hay un gran número de razones para que se conecten en una red, incluyendo el compartir recursos, la comunicación, la fiabilidad e incrementar el poder de procesamiento. La comunicación entre computadoras puede completarse en un modo punto a punto en donde cada sistema transmite a otro específico, o en un modo broadcast donde los sistemas transmiten en general a todos los medios accesibles de la red.

La figura 4.3 describe las dos topologías que encontramos en redes broadcast. La figura 4.4 describe otras dos topologías que encontramos en las redes punto a punto que son las más utilizadas. En nuestra conexión de VPN nos enfocaremos a la de topología estrella que es la más común de todas.

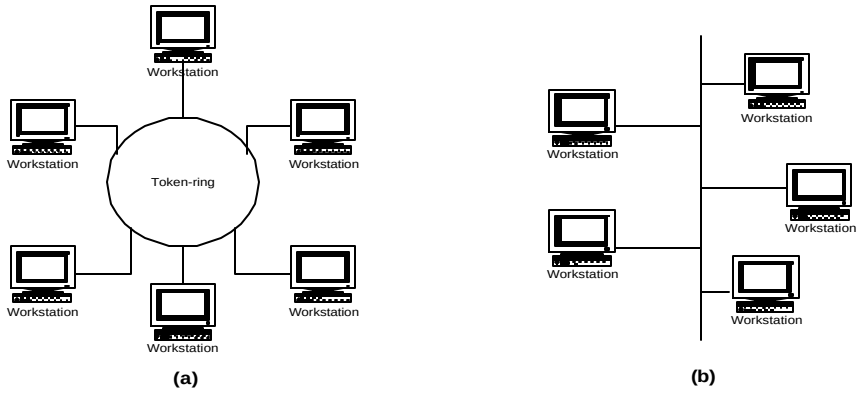


Figura 4.3
Topologías Broadcast. (a) anillo. (b) bus.

Las redes LAN generalmente usan una tecnología de transmisión que consiste en un cable sencillo, al cual se encuentran conectados todos los computadores, la velocidad tradicional de las redes de área local oscila entre 10 y 100 Mbps (Megabits por segundo), un Megabit son 1.000.000 de bits. En los últimos años se han mejorado los estándares de cableado para incrementar la velocidad de transferencia sobre cables de cobre de par trenzado, esto facilita la decisión del cable a utilizar, ya que el cable de par trenzado es más barato que el cable coaxial y ofrece una velocidad superior de transmisión.

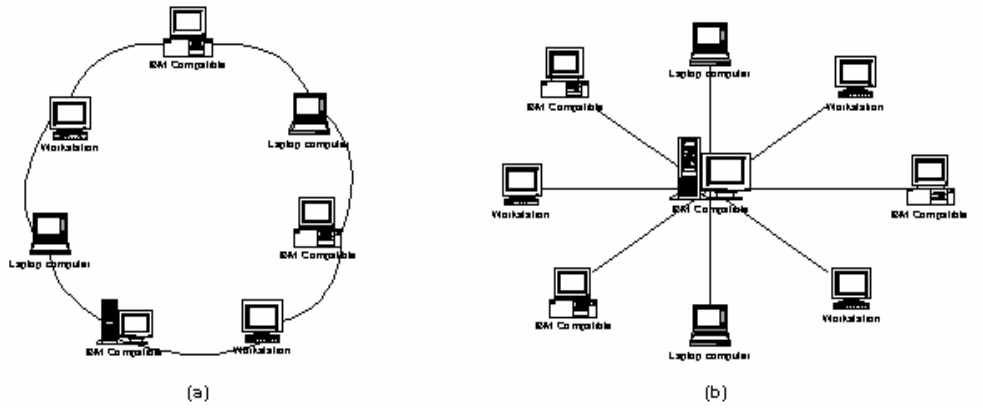


Figura 4.4
Topologías punto a punto (a) anillo, (b) estrella.

Las necesidades de seguridad dependerán de los niveles de seguridad que se quieran y se requieran manejar dentro de la red.

Primer Nivel de Seguridad

- Aislar las computadoras de la red
- Operación totalmente centralizada
- Seguridad física de los medios de transporte de la información
- Niveles de autorización, administración distribuida y cifrado de archivos
- Capacitar el personal

Segundo Nivel de Seguridad

- Colocación de barreras para aislar subredes
- Recepción de correo electrónico solamente
- Seguridad del correo (cifrado y autenticación)
- Vigilancia y análisis de uso

Tercer Nivel de Seguridad

- Colocación de barreras para permitir el acceso
- Cifrado de llaves de acceso
- Tarjetas inteligentes
- Control de ejecución de procesos remotos
- Los sistemas de autenticación varían

¿Cuál va a ser el impacto a lo largo del tiempo?

¿Qué tan flexible es migrar a otro esquema?

- Cifrado de paquetes
- Monitoreo y Análisis de uso

Cuarto Nivel de Seguridad

- Añadir el primer nivel servidores de información y de transacciones
- Autorización de transacciones
- Mantenimiento de archivos en el servidor
- Niveles de acceso
- Cifrado de llaves
- Cifrado de paquetes por origen y destino
- Monitoreo y análisis de uso

4.2 Estrategia de Seguridad

Antes de pensar en un sistema de seguridad eficaz, es primordial analizar qué es lo que se busca proteger tomando en cuenta los elementos ilustrados en la figura 4.5. En esta figura se muestra en que orden deben ser considerados dichos elementos.

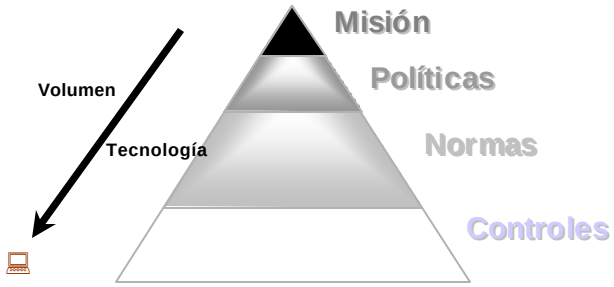


Figura 4.5
Jerarquía de valores en un análisis de un sistema de seguridad.

Como podemos apreciar en la figura 4.5 la misión es el punto más importante a considerar y cada uno de los pasos deben llevarnos a encontrar nuestra estrategia de seguridad.

Cuando se piensa establecer una estrategia de seguridad, la pregunta que se realiza, en primera instancia, es: ¿en que baso mi estrategia? La respuesta a esta pregunta es muy simple, podemos basarnos en el algoritmo Productor/Consumidor, que explicamos en el capítulo 1.

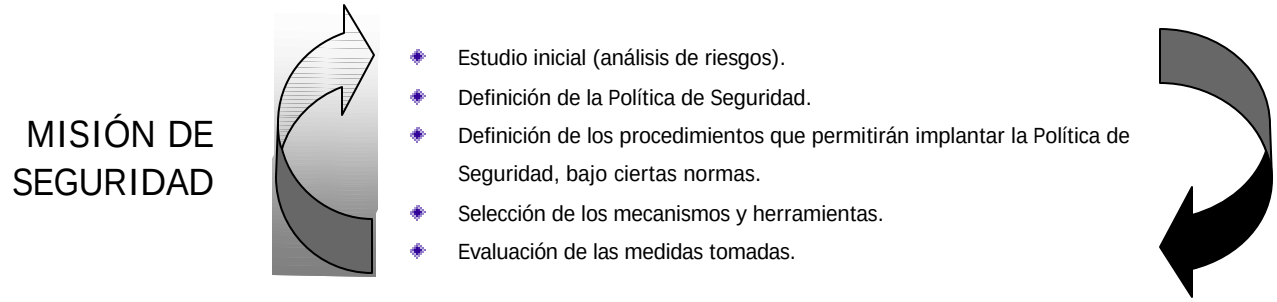


Figura 4.6
Pasos a seguir en una estrategia de seguridad

Los pasos de la figura 4.6 están contenidos, o bien, relacionados con los valores de la figura 4.5. Por ejemplo, la evaluación de las medidas tomadas y el estudio inicial forman parte del control. La selección de los mecanismos y herramientas se hará a partir de las políticas definidas. Y el punto tres, definición de procedimientos que permitirán implantar la política de Seguridad bajo ciertas normas, depende 100%, de la Normas definidas a nivel local e Internacional.

4.2.1 Misión de seguridad informática

Es el enunciado de las aspiraciones que tienen los miembros de una organización en la seguridad en el uso de la tecnología informática.

En el proceso de adquirir un sistema de información es necesario tomar la decisión de que confiabilidad debe tener para cumplir con su misión de seguridad. La misión debe definirse en términos de los cuatro requerimientos que ya conocemos:

Preservar la confiabilidad, la integridad, la autenticidad y la disponibilidad

Concebir y redactar la misión y las políticas de una organización recae sobre los responsables del buen funcionamiento de la misma. Por ejemplo los dueños de una empresa, los principales administradores de una corporación o los directores de alguna dependencia. El elemento fundamental de estos documentos es que expresan el consenso de quienes conocen mejor que nadie los principios operativos, económicos y éticos que conducirán al éxito colectivo.

Al hacer este trabajo es necesario consultar a los expertos en diversos tipos de actividad, para que los directivos sepan cómo afectarán las políticas que emitan la capacidad de acción de las diferentes secciones de la organización. La forma más eficiente de realizar ésta consulta es mediante una encuesta preparada por expertos en seguridad informática que planteen las

preguntas en forma tal que conduzcan a párrafos precisos en la redacción de la misión, cada uno de los cuales pueda plasmarse en una o más políticas de seguridad.

Todas las disciplinas de seguridad (personal, física, informática, etc.) trabajan en forma conjunta para establecer una infraestructura de seguridad que sirva a toda la organización. Definen cuál es el comportamiento aceptable y cuáles son los riesgos aceptables, y determinan cómo se mitigan los riesgos que no son aceptables aplicando garantías medibles que hacen manejables y aceptables los riesgos. Las palabras "medibles" y "aceptables" son fundamentales. Garantías tales como controles de accesos físicos, o la confiabilidad del personal, o algoritmos de cifrado son herramientas importantes para controlar los riesgos en algunos entornos. Medir la efectividad de los controles de acceso físico para evitar intrusos, la confiabilidad de un empleado analizando su biografía para detectar si ha cometido fraudes o medir un servicio de cifrado para saber hasta que grado de confidencialidad de la información es básico para poder tomar decisiones sobre qué riesgos son aceptables. (Ferris J.M.,1994).

4.2.1.1 Objetivos de seguridad

Los objetivos de seguridad deben de enfocarse a alcanzar la misión de seguridad. Y son simplemente una lista detallada de los puntos que se desean alcanzar, que se encuentran englobados en la misión de seguridad.

Para fijar estos objetivos y buscar la forma de alcanzarlos específicamente en un sistema de red, necesita elaborarse un esquema de Seguridad en Red.

Método para alcanzar los objetivos

Los métodos para alcanzar los objetivos de seguridad no siempre son claros. Involucran conceptos y acciones tales como las siguientes:

*Confinar sujetos***.-** Los sujetos deben ser confinados a un componente sencillo. El concepto de una pareja (proceso, dominio) para un sujeto, limita a los objetos al mismo componente:

- Asegurar que los objetos de un dominio no comprendan los de otro componente.
- El resultado de un proceso remoto en la creación de un nuevo sujeto en un componente remoto.

Si son objetos de un componente local

- Los sujetos pueden accesar objetos en forma directa sólo dentro del componente al que esté asociado el sujeto.
- ¿Qué sucede con la información que está siendo transmitida entre los componentes?
    1. La información "en movimiento" no es tratada como un objeto.

2. Si no es tratada como un objeto, entonces no puede ser accesada hasta que "esté inmóvil".

Si los componentes contienen un monitor de referencia de componentes, entonces:

- En algunos componentes un monitor de referencia de componentes corrompido puede bastar.
- Esto significa que si el componente es de nivel sencillo, el monitor de referencia es corrompido.
- Los no accesos necesitan ser revisados por:
  1. Todos los objetos tienen la misma etiqueta.
  2. Todos los sujetos tienen la misma clase.
- Se debe recordar siempre que cada monitor de referencia de componente necesita reforzar únicamente la política perteneciente a los accesos locales particulares del componente.

4.2.2 Políticas

Como se expuso anteriormente (Capítulo 1, Antecedentes de seguridad) las políticas de seguridad deben hacerse en base a los resultados del análisis de riesgos. La forma en la que se debe realizar este análisis explicará en puntos subsecuentes, pero a continuación enunciamos algunas de la cuales no deben faltar y a las que se agregarán las que sean necesarias para alcanzar la misión de seguridad.

4.2.2.1 Políticas de seguridad básicas para VPN's

- Sólo a las partes autorizadas se les permite el acceso a aplicaciones y servidores corporativos.
- Todo usuario de la Organización debe contar con un mecanismo único y personal que le permita autentificarse. El usuario no deberá de comprometer de forma alguna ese mecanismo de autentificación.
- La organización debe asegurarse de que los datos estén seguros y no puedan ser leídos por otros, así como tener algún mecanismo para corroborar la integridad de los mismos.
- La VPN debe de funcionar para todas las plataformas o sistemas operativos, es decir, debe de ser interoperable.

- El dispositivo de la VPN debe proporcionar una administración fácil, la configuración debe ser directa, y su mantenimiento y actualización debe estar asegurada.
- Todos los sistemas deben de contar con programas de antivirus y ser revisados periódicamente. También se deberán hacer respaldos periódicos de la información del sistema central.
- Cualquier tráfico de Internet deberá de pasar por el Firewall. No podrán conectarse líneas directas a Internet o redes externas, por ejemplo modems.
- Los usuarios deben tener distintos niveles de accesos. Los usuarios individuales deben tener un distinto nivel de acceso cuando entren al sitio desde redes no internas.
- Por cada componente de la red es necesario un monitor de referencia. Cada monitor de referencia debe tener un modelo formal de política de seguridad.
- Deberán actualizarse continuamente los parches de seguridad a los servidores del sistema.
- Deberán realizarse auditorias a los sistemas de seguridad, para detectar si es necesario hacer alguna modificación, a mecanismos o políticas.

4.2.3 Normas

Las normativas de seguridad empezaron a desarrollarse a finales de los años setenta cuando surgió la necesidad de proteger ciertas comunicaciones que no pertenecían a los restringidos ambientes militares y diplomáticos, hasta entonces únicos usuarios de comunicaciones seguras. Bancos y multinacionales fueron promotores y primeros beneficiarios de la normalización de los métodos de protección de la información y las comunicaciones. Dicha normalización, además de permitir una comunicación cifrada entre distintas entidades y distintos equipos, incrementa el nivel de seguridad de los algoritmos al hacerlos públicos, lo que facilita su estudio y la posibilidad de analizarlos detalladamente.

Las organizaciones internacionales dedicadas a la elaboración de normativas han generado varios documentos relativos a los distintos aspectos de seguridad, como vamos a ver a continuación. En estas normas se tratan aspectos muy genéricos de la seguridad, como la situación de los elementos de protección en los distintos puntos de la red, sin entrar en detalles de algoritmos concretos. Así ocurre, por ejemplo, en la norma ISO 7498.2, en distintas recomendaciones de las series X.2xx, X.4xx, X.5xx, X.7xx y X.8xx dadas por la Unión Internacional de Telecomunicaciones (ITU), en los trabajos realizados por el Subcomité 27 (SC27) dependiente de la Organización Internacional de Estándares (ISO) y en los de la Comisión Electrotécnica Internacional (IEC).

Por otra parte. El Instituto Nacional Americano de Estándares (ANSI), en sus series X3 y X9, describe con detalle el cifrado, la integridad, la autenticación y la administración de claves. En la serie X12 está contemplada la seguridad para el intercambio de datos electrónicos (EDI). Muchas normas de la ANSI han sido posteriormente modificadas y adoptadas por ISO.

Existen otros grupos y otras comisiones, entre ellos el Instituto Europeo de Estándares de Telecomunicaciones (ETSI) y la Asociación Europea de Fabricantes de Computadoras (ECMA), que están trabajando en cuestiones de normativa de seguridad, aunque sus resultados aún no son definitivos.

Por otra parte, en la década de los 80's el NCSC (National Computer Security Center) emitió una serie de libros clasificados por colores, los cuales abordaban diferentes problemáticas de seguridad. El libro naranja (Orange Book) llamado oficialmente: Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) contiene requerimientos básicos en cuatro categorías para sistemas operativos confiables: política de seguridad, responsabilidad, garantía y documentación. Posteriormente se emitió el libro rojo (Red Book) llamado oficialmente: Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC), el cual contiene una interpretación del libro naranja con respecto a los requerimientos para redes, y un sumario de servicios específicos de red: integridad de comunicaciones, negación de servicio, y protección del compromiso.

En esta serie de libros se definen las distintas categorías con relación a las necesidades de las fuerzas armadas de los EUA y por su disponibilidad su uso se ha generalizado quizás excesivamente. A lo largo de los años se han categorizado de esta manera los elementos que conforman los sistemas de información destinados al mercado no militar, y se ha publicado esta categorización. La descripción de la confiabilidad que se desea tenga un sistema que se piensa adquirir se ha basado en muchos casos en esta categorización preestablecida.

Los Criterios Comunes ofrecen una metodología para llevar a cabo una descripción de la confiabilidad deseada de un sistema que no es motivada por un punto de vista militar, y además constituyen un lenguaje común para los fabricantes, proveedores y consumidores que es preciso y fácil de usar.

4.2.4 Control

En este punto se controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la Organización y/o la Dirección Informática, así como los requerimientos legales.

Su misión es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas, actuales y válidas.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.

- Colaborar y apoyar el trabajo de auditoria informática, así como de las auditorias externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los niveles adecuados del servicio informática, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control, si no también en cada responsable de objetivos y recursos, así como de la implantación de medios de medida adecuados.
- Mantener el nivel definido de seguridad para el sistema, haciendo análisis de la red, así como de vulnerabilidades y bitácoras. Esto implica mantener actualizadas las herramientas de seguridad, aplicaciones y sistemas operativos.

Los grandes grupos de controles son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación:

- Controles **directivos**, que son los que establecen las bases, como las políticas, o la creación de comités relacionados o de funciones: de administración de seguridad o auditoria de sistemas de información interna
- Controles **preventivos**, antes del hecho como la identificación de visitas (seguridad física) o las contraseñas (seguridad lógica).
- Controles de **detección**, como determinadas revisiones de accesos producidos o la detección de incendios.
- Controles **correctivos**, para rectificar errores, negligencias o acciones intencionadas, como la recuperación de un archivo dañado a partir de una copia.
- Controles de **recuperación**, que facilitan la vuelta a la normalidad después de accidentes o contingencias, como puede ser un plan de continuidad adecuado.

Podemos hablar de *Objetivos de Control* respecto a la seguridad, que vienen a ser declaraciones sobre el resultado final deseado o propósito a ser alcanzado mediante las protecciones y los procedimientos de control, objetivos como los recogidos en la publicación COBIT (Control Objectives for Information and Related Technologies) de ISACA (Information Systems audit. And Control Association/Foundation).

Cada entidad ha de definir sus propios objetivos de control, en cuanto a seguridad y otras áreas, y crear y mantener un Sistema de Control Interno (funciones, procesos, actividades, dispositivos...) que pueden garantizar que se cumplen los objetivos de control.

En los informes se recomendará la implantación o refuerzo de controles, y en ocasiones incluso que se considere la supresión de algún control, si es redundante o ya no es necesario.

El *sistema de control interno* ha de basarse en las políticas, y se implanta con apoyo de las herramientas, si bien encontramos a menudo en las auditorias que lo que existe es más bien la implantación parcial de controles de acceso lógico a través de paquetes o sistemas basada en el criterio de los técnicos, pero no sustentada en normativa, o bien habiendo partido ésta de los propios técnicos, sin aprobaciones de otro nivel.

La realidad es que el control interno no está generalizado en México fuera de los procesos que implican gastos, y especialmente pagos, pero existen otros riesgos importantes o más que las pérdidas monetarias directas, relacionados con la gestión adecuada de los recursos informáticos o con la propia protección de la información, que podrían suponer responsabilidades y pérdidas muy importantes para la entidad.

Cuando existe un sistema de control interno adecuado, los procesos de auditoria, especialmente si son periódicos, son revisiones necesarias pero más rápidas, con informes más breves; si el sistema de control interno es débil, la auditoria llevará más tiempo y esfuerzo, su costo sería mayor, y las garantías de que se pongan en marcha las recomendaciones son mucho menores; en ocasiones la situación dista tanto de la ideal como la del paciente que se somete a un chequeo después de varios años sin control.

4.2.4.1 Herramientas de control interno

En la tecnología de la seguridad informática que se ve envuelta en los controles, existe tecnología hardware (como las herramientas de cifrado) y software. Las herramientas de control de tecnología de software que por sus características funcionales permiten vertebrar un control de una manera más actual y automatizada. Sin olvidar que la herramienta en sí misma no es nada. El control se define en todo un proceso metodológico, y en un punto del mismo se analiza si existe una herramienta que automatice o mejore el control existente, para más tarde definirlo con la herramienta incluida, y al final documentar los procedimientos de las distintas áreas involucradas para que éstas; los cumplan y sean auditados. O sea, comprar una herramienta sin más y ver qué podemos hacer con ella es un error grave que no conduce a nada.

Las herramientas de control (software) más comunes son:

- Seguridad lógica del sistema
- Seguridad lógica complementaria al sistema (desarrollado a medida)
- Seguridad lógica para entornos distribuidos
- Control de acceso físico. Control de presencia
- Control de copias
- Gestión de soportes magnéticos
- Gestión de soportes magnéticos
- Gestión y control de impresión y envío de listados por red
- Control de proyectos
- Control de versiones
- Control y gestión de incidencias
- Control de cambios

Todas estas herramientas están inmersas en controles nacidos de unos objetivos de control y que regularán la actuación de las distintas áreas involucradas.

En las herramientas de seguridad lógicas están inmersas todas aquellas que nos garanticen la confidencialidad y la integridad de la información; podemos encontrar firewalls, herramientas de cifrado y de dispersión. Con estas herramientas podemos también apoyarnos para conseguir otros dos tipos de control para mantener la seguridad del sistema.

4.2.4.2 Monitoreo del sistema

Además de preocuparse acerca de usuarios no autorizados, los usuarios autorizados a veces se equivocan, o cometen actos maliciosos. Si esto sucede es necesario determinar qué se hizo, quién lo hizo y qué fue afectado. La única forma de lograr esto es tener un registro inexpugnable de la actividad que sucede en el sistema e identifica en forma no ambigua a todos los actores y acciones. En alguna aplicaciones criticas las trazas de auditoria y monitoreo pueden ser tan extensas que permiten deshacer las operaciones realizadas para ayudar a restablecer el sistema a su estado correcto.

El monitoreo y la auditoria están ampliamente relacionadas como herramientas de control del sistema. En el monitoreo podemos estar analizando en tiempo real los acontecimientos del sistema, y en caso de que por la cantidad de procesos sea muy grande se guardan son los registros en la bitácora del sistema, para que posteriormente ser revisados como parte de la auditoria.

Otra de las ventajas de mantener un monitoreo del sistema, es poder reaccionar ante un ataque en cuanto es detectado y no esperar a que las consecuencias sean graves.

Podemos apoyarnos de distintas herramientas hacker como las que vimos en el capítulo 3 para llevar a cabo este monitoreo del sistema y estar enterados del comportamiento del sistema.

4.2.4.3 Auditoria informática

Conceptualmente la auditoria, toda y cualquier auditoria, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple con las condiciones que le han sido presentadas.

La auditoria informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo sustenta y confirma el éxito de los objetivos tradicionales de la auditoria.

- Objetivos de protección de activos e integridad de datos.

- Objetivos de gestión que abarcan, no solamente los de protección de activos, si no también los de eficacia y eficiencia.

El responsable de realizar esta auditoria evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoria, incluyendo el uso de software, tal como mencionamos anteriormente. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear el software de auditoria y otras técnicas asistidas por computador.

Se pueden establecer tres grupos de funciones a realizar por el auditor de información designado:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.

- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.

- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

Para muchos la seguridad sigue siendo el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoria informática para revisar la seguridad, aunque después se hayan ido ampliando los objetivos.

No puede haber seguridad sin auditoria, puede existir auditoria de otras áreas, y queda un espacio de encuentro: la auditoria de la seguridad (figura 4.7), y cuya área puede ser mayor o menor según la entidad y el momento. La auditoria viene a ser el control del control.

Figura 4.7
Encuentro entre seguridad y auditoria.

Debe evaluarse en la auditoria de seguridad si los modelos de seguridad están en consonancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones, porque no se puede auditar con conceptos, técnicas o recomendaciones de hace algunos años (que en realidad no son tantos).

En cuanto a la justificación de porque es importante la auditoria, que no parece necesaria en una obra de este tipo, sólo decir que tanto la normativa como la auditoria son necesarias: una auditoria no basada en políticas de la entidad auditada (además de las normas para realizar la auditoria) sería subjetiva y hasta peligrosa, aunque en sistemas de información es una situación habitual.

4.2.4.3.1 *Áreas que puede cubrir la auditoria de la seguridad*

Se incluyen las que con carácter general pueden formar parte de los objetivos de una revisión de la seguridad, si bien ésta puede abarcar sólo parte de ellas si así se ha determinado de antemano.

En una auditoria de otros aspectos pueden también surgir revisiones solapadas con la seguridad; así, a la hora de revisar los desarrollos, normalmente se verá si se realizan en un entorno seguro y protegido, y lo mismo a la hora de revisar la explotación, o el área de técnica de sistemas, las redes, la informática de usuario final, las bases de datos... y en general cualquier área, salvo que expresamente se quiera pasar por alto la seguridad y concentrarse en otros aspectos como pueden ser la gestión, costos, nivel de servicio, cumplimiento de procedimientos generales, calidad o cualquier otro.

Volviendo a las áreas, las que se citan pueden ser objeto de la auditoria de seguridad, si bien cada caso se habrán fijado los objetivos que más interesen, no considerando o por lo menos no con el mismo énfasis otros, si bien debiendo quedar claro y por escrito cuáles son esos objetivos, tanto cuando se trate de una auditoria interna como externa, en cuyo caso puede mediar un contrato o al menos una propuesta y carta de aceptación.

Las áreas son:

- Lo que se puede denominar como controles directivos, es decir, los fundamentos de la seguridad: políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como que existen sistemas y métodos de evaluación periódica de riesgos.

- El desarrollo de las políticas: procedimientos, posibles estándares, normas y guías, sin ser suficiente que existan estas últimas.

- Que para los grupos anteriores se han considerado el marco jurídico aplicable, aspecto tratado en otros capítulos de esta obra, así como las regulaciones o los requerimientos aplicables a cada entidad. Otro aspecto es el cumplimiento de los contratos.

- Amenazas físicas externas: inundaciones, incendios, explosiones, corte de líneas o de suministros, terremotos, terrorismo, huelgas...

- Control de acceso adecuado, tanto físicos como los denominados lógicos, para que cada usuario pueda acceder a los recursos a que esté autorizado y realizar sólo las funciones permitidas: lectura, variación, borrado, copia... y quedando las pistas necesarias para control

y auditoria, tanto de accesos producidos al menos a los recursos más críticos como los intentos en determinados casos.

- Protección de datos: lo que fije la ley en cuanto a los datos de carácter personal bajo tratamiento automatizado, y otros controles en cuanto a los datos en general, según la clasificación que exista, la designación de *propietarios* y los riesgos a que estén sometidos.

- Comunicaciones y redes: topología y tipo de comunicaciones, posible uso de cifrado, protecciones ante virus, éstas también en sistemas aislados aunque el impacto será menor que en una red.

- El entorno de Producción, entendiendo como tal Explotación más Técnica de Sistemas, y con especial énfasis en el cumplimiento de contratos en lo que se refiera a protecciones, tanto respecto a terceros cuando se trata de una entidad que presta servicios, como el servicio recibido de otros, y de forma especial en el caso de la subcontratación total o *outsourcing*.

- El desarrollo de aplicaciones en un entorno seguro, y que se incorporen controles en los productos desarrollados y que éstos resulten auditables.

- La continuidad de las operaciones.

No se trata de áreas no relacionadas, sino que *casi todas tienen puntos de enlace y partes comunes:* comunicaciones con control de accesos, cifrado con comunicaciones y soportes, datos con soportes y con comunicaciones, explotación con varias de ellas y así en otros casos.

En el capítulo 6 en donde hablemos del mantenimiento del sistema que se implemente se hablará de la auditoria seguridad, de la red y en específico de la auditoria orientada a la PyME.

4.3 Análisis de Riesgos

En una primera aproximación, para determinar cuál es la seguridad adecuada en un sistema habrá que estudiar cuáles son los riesgos a los que está expuesto teniendo en cuenta el valor de la información que contiene, los costos de recuperación ante un hipotético desastre y, por supuesto, evaluar lo que costaría la protección.

Se trata de identificar los riesgos, cuantificar su *probabilidad* e *impacto,* y analizar medidas que los eliminen o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

El *riesgo* es la probabilidad que se materialice una amenaza. Hacer un análisis de riesgos, requiere estudiar las amenazas a las que un sistema está expuesto, el grado en el que lo está,

así como las posibles consecuencias. La forma más sencilla de hacer este estudio sería anotar en una columna todas las amenazas posibles y al lado, como un valor numérico de dentro de una escala, el grado en el que se considera que el sistema está expuesto.

Realizar un análisis de riesgos es el primer paso para determinar en qué dirección deben dirigirse los esfuerzos para conseguir la seguridad adecuada y que permitirá detectar cuáles son los puntos débiles sobre los que hay que aplicar o reforzar las medidas de seguridad.

En cada caso particular el riesgo frente a cada amenaza puede ser muy distinto. Lógicamente, no corre el mismo riesgo de una infección por virus una computadora en el que únicamente se introducen programas originales y sólo trabaja una sola persona en él, que otro utilizado por múltiples usuarios y en el que no hay ningún control sobre los programas que entran. Factores como las condiciones meteorológicas de la zona determinan el riesgo que se corre ante desastres como inundaciones y fuego.

Es necesario revisar si se han considerado las *amenazas* de todo tipo, o bien evaluarlas si es el objetivo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a personas, datos, programas, redes, instalaciones u otros activos, y llegar a suponer un peor servicio a usuarios internos y externos, imagen degradada u otros difícilmente cuantificables, e incluso pérdida irreversible de datos, y hasta el fin de la actividad de la entidad en los casos más graves.

Para ello es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles, que serán los que preferentemente intentarán usar quienes quieran acceder de forma no autorizada.

Debemos pensar que las medidas deben considerarse como *inversiones en seguridad,* aunque en algunos casos se nos ha dicho que no es fácil reflejarlas como activos contables ni saber cuál es su *rentabilidad.* Esa rentabilidad la podemos determinar si los dispositivos o controles han servido para evitar la agresión, y a veces habrá constituido simplemente una medida para lograr disuadirla, sobre todo en seguridad lógica, y no llegaremos a conocer su efecto positivo.

Durante el proceso de análisis deben contestarse las siguientes preguntas, muchas de las cuales son contestadas con los antecedentes del capítulo 1:

- ¿Qué es un riesgo?
- ¿Qué impacto tiene la materialización de un riesgo en las metas de la organización?
- ¿Qué riesgos son aceptables?
- ¿Cuál es la dependencia de la organización en sus recursos de información?
- ¿Qué medidas de defensa existen para eliminar los riesgos no aceptables y cuánto cuestan?
- ¿Qué medidas de protección resultan tener más beneficios por determinado costo?
- ¿Quién se responsabiliza de las medidas de protección?
- ¿Cómo y cuándo se implementarán esas medidas de protección?

4.3.1 Elaborando el Análisis de Riesgos

Las siguientes preguntas definen el proceso de análisis de riesgos:

- ¿Qué puede suceder? (amenaza)
- Si sucede, ¿qué tanto daño causará? (impacto)
- ¿Cada cuánto sucederá? (frecuencia)
- ¿Estamos seguros de lo anterior? (incertidumbre)
- ¿Qué se puede hacer? (mitigación)
- ¿Cuánto tiempo, dinero y esfuerzo se está dispuesto a invertir para obtener una protección adecuada? (erogación económica)
- ¿Vale la pena hacerlo? (costo/beneficio)

El proceso de análisis de riesgos tiene varias fases:

- *Identificación de los activos.*
  - I Valoración de los activos.
- *Identificación de los riesgos.*
  - II Análisis de vulnerabilidad.
  - III Correlación de vulnerabilidad y riesgo.
  - IV Identificación de los mecanismos de reducción de vulnerabilidades.
  - V Valoración de los mecanismos.
- *Calculo de los riesgos.*
  - VI Análisis del beneficio logrado con el costo estimado.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

La información no es lo único que está en juego; también lo están los equipos y además de ambos, algo puede llegar a ser tan o más valioso: la disponibilidad del sistema. El hecho de que el sistema no pueda ser utilizado supone pérdida de tiempo de los usuarios y puede comportar retrasos en la entrega de trabajos, lo que podría desembocar en pérdida de negocios o de la confianza del cliente.

Por lo tanto, al hacer una estimación de costos de lo que se arriesga, habría que considerar tanto el valor de la información como el precio de los equipos, sin olvidarse de lo que costaría la no disponibilidad del sistema. También se deberán tener en cuenta los posibles costos de recuperación para que el sistema volviese a estar operativo tras un desastre.

Existen muchas maneras de efectuar este proceso. Un método que ha resultado exitoso es llevar a cabo una serie de talleres. Se invita a una gama de usuarios, administradores y directivos de toda la organización. A lo largo de varias semanas se completan las listas de activos y amenazas. Este proceso no sólo permite obtener un conjunto de listas más completo sino que también promueve la concientización de todos los que asisten.

4.3.2 Identificación de los activos

Esta etapa normalmente se cumple mediante un análisis de la misión de seguridad, pues allí se indica qué es lo que se desea proteger. Sin embargo, este análisis puede ser complicado, pues los sistemas de información cada día son más complejos. El uso de redes de computadoras, particularmente en forma de intranets y redes externas, y los procesos de adquisición, fusión y fragmentación de organizaciones, frecuentemente resultan en la inexistencia de un inventario completo de los bienes informáticos de una organización. Además, la proliferación de la información interna disponible a los miembros de una organización dificulta aún más la realización de inventarios completos.

El primer paso es hacer una lista de todo lo que debe ser protegido, así como la dependencia entre ellos. Debe basarse en el plan de negocios y en el sentido común. El proceso puede requerir conocimientos de la legislación local vigente, un completo entendimiento del equipo y locales, y un buen conocimiento del plan de seguros que se ha contratado. Esta lista debe ser regularmente actualizada por ejemplo con la llegada de nuevo equipo, cambios de infraestructura, cambios en los aplicativos, etc.

Entre otras cosas se debe considerar: hardware, software, datos, documentación, servicios u operación. A continuación los definimos con ejemplos:

Hardware: CPU's, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de discos, líneas de comunicación, servidores, ruteadores, conmutadores, módems, unidades de respaldo, hubs.

Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas para comunicaciones, programas de oficina, en general todas las aplicaciones creadas fuera y dentro de la empresa.

Datos: almacenados en línea o fuera de línea, en procesamiento, en respaldos, bases de datos, circulando en algún medio de comunicación, desplegado o impreso.

Documentación: sobre sistemas, equipos, aplicaciones, programas, procedimientos de operación y administrativos, planes de contingencia, etc.

Servicios u operación: Son las funciones administrativas y operacionales propias del negocio. Servicios al cliente, etc.

Accesorios: papel, formularios, cintas, información grabada.

En términos generales, una metodología práctica es establecer perímetros que se puedan definir bien y llevar a cabo el inventario dentro de esos perímetros. Posiblemente el único análisis de riesgos factible será el que se haga perímetro por perímetro.

La temporalidad es un factor determinante en el análisis de riesgos. La vida útil de los equipos, de los programas, de los datos y de los mecanismos de protección dominan el estudio de los beneficios y de los costos. Por ejemplo, un mecanismo de protección cuya vida útil es mucho más corta que la del sistema de información que está protegiendo, deberá ser reemplazado varias veces, y el costo por lo tanto no es sólo el del mecanismo inicial.

Otro factor temporal esta indicado por la variación en el tiempo del valor de la información. Si sólo se considera el valor actual en el análisis de costo/beneficio, olvidando por ejemplo que la información no tendrá valor después de un periodo dado, se puede sobreestimar el beneficio que ofrece un mecanismo de protección. Por esto, el trabajo de análisis normalmente se hace sobre la base de cifras anuales.

Para definir la importancia de un cierto activo, así como el riesgo asociado a éste, es necesario contar con el apoyo de las áreas que crean, procesan o administran la información. Este apoyo es necesario concertarlo a través de varias reuniones.

4.3.2.1 Valoración de los activos

Podemos dividir los activos en dos grandes rubros:

- TANGIBLES:
  - Computadoras
  - Respaldos y acervos
  - Manuales, guías y libros
  - Listados
  - Medios de distribución de programas comerciales
  - Equipo y cableado de comunicaciones
  - Registros de personal

- Registros de auditoria
- Ruteadores
- Cableados

- Intangibles

  - Datos privados
  - Salud y seguridad del personal
  - Privacidad de los usuarios
  - Contraseñas personales
  - Imagen pública y reputación
  - Buena voluntad de los clientes y compradores
  - Disponibilidad del proceso
  - Información sobre la configuración

Los activos tangibles se valoran de acuerdo a las normas contables que tenga la empresa en el sentido de calcular valores de reposición. Debe incluirse en esta valoración el costo del trabajo necesario para hacer una reposición funcional. Por ejemplo el costo de la configuración, o de la programación en caso de ser necesario.

Se puede considerar que el valor contable es una fuente objetiva de valuación monetaria. Se llama a veces valoración basada en costos, y tiende a producir valores conservadores. Los costos pueden ser el precio de adquisición de la información (compra de una lista de clientes) o el costo de generar la información, como podría ser una encuesta en la que se usó personal, materiales, instrumentos de comunicación, etc., cada uno de los cuales se pagó.

Aparte del recurso en sí (algo tangible, como un router) hemos de considerar la visión intangible de cada uno de estos recursos (por ejemplo la capacidad para seguir trabajando sin ese router). Es difícil generar estos aspectos intangibles de los recursos, ya que es algo que va a depender de cada organización, su funcionamiento, sus seguros, sus normas...No obstante, siempre hemos de tener en cuenta algunos aspectos comunes: privacidad de los usuarios, imagen pública de la organización, reputación, satisfacción del personal y de los clientes, en el caso de una universidad, de los alumnos, capacidad de procesamiento ante un fallo...

Con los recursos correctamente identificados se ha de generar una lista final, que ya incluirá todo lo que necesitamos proteger en nuestra organización.

Lo más valioso que hay en la mayor parte de los sistemas es, por supuesto, la información que contienen. En general, no es tarea sencilla calcular su valor puesto que no sólo hay que

tener en cuenta el costo de haberla generado o de tener que volver a introducirla, sino también el costo de no poder disponer de ella en un momento determinado.

En el valor de la información puede influir incluso el tiempo de reacción con el que se cuenta para recuperarse en caso de pérdida; es decir, para que el sistema vuelva a ser operativo y la información vuelva a estar accesible por los usuarios. Por ejemplo, es mucho más perjudicial que se pierda información de las nóminas de una empresa el día anterior a emitirlas que tres días antes cuando el tiempo para reaccionar es todavía suficiente.

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Cuando hablamos del valor de la información nos referimos, por ejemplo, a qué tan peligroso es enviar la información de mi tarjeta de crédito a través de Internet para hacer una compra, en una red gigantesca donde viajan no únicamente los 16 dígitos de mi tarjeta de crédito sino millones de datos más, gráficas, voz y video.

El peligro más grande radica, no en enviar la información sino una vez que esta información, unida a la de miles de clientes más, reposa en una base de datos de la compañía con las que se concretó el negocio. Con un único acceso no autorizado a esta base de datos, es posible que alguien obtenga no únicamente mis datos y los de mi tarjeta, sino que tendrá acceso a los datos y tarjetas de todos los clientes de esta compañía.

En efecto, el tema no está restringido únicamente a Internet. Aunque no se esté conectada a Internet una red está expuesta a distintos tipos de ataques electrónicos, incluidos los virus.

4.3.2.2 Métodos para valorar la información

a) Orden superior, política general, legislación

Los dueños de la información pueden asignar un valor a un cuerpo de información o a varios cuerpos de información en términos no monetarios. Pueden existir reglas impuestas interna o externamente que determinen el valor no monetario de algunos tipos de información. Esto permite desarrollar consideraciones que indiquen su valor monetario. Estas aseveraciones o reglas frecuentemente son generales y pueden no ajustarse al caso en cuestión, ser no realistas o estar sujetas a interpretaciones distintas. Sin embargo, hay que aceptarlas, pero no sin verificar sus implicaciones. El valor monetario resultante puede ser tan extraordinario que sea inaceptable. En ese caso, hay que procurar cambiar el requerimiento o rehusarse a aceptarlo.

b) Entrevistas con Listas de Verificación

Los usuarios y los dueños de la información son quienes pueden tener la mejor apreciación del valor de la información. Para obtener esta apreciación se realizan entrevistas estructuradas con los individuos seleccionados para ello y se redactan listas de verificación de las preguntas que se les harán o de los temas que se discutirán. Las listas permiten estandarizar lo más posible las entrevistas y evitan la dispersión de las ideas.

c) Cuestionarios

En lugar de entrevistar a los usuarios o dueños, se pueden preparar cuestionarios y emplear las respuestas como base para la valoración.

d) Consenso (Delphi)

Cuando hay grupos identificables de usuarios de la misma información, se puede usar el método delphi numérico modificado, para obtener un consenso sobre el valor de la información.

e) Valor en libros

Se puede considerar que el valor contable es una fuente objetiva de valuación monetaria. Se llama a veces valoración basada en costos, y tiende a producir valores conservadores. Los costos pueden ser el precio de adquisición de la información (compra un lista de clientes) o el costo de generar la información, como podría ser una encuesta en la que se usó personal, materiales, instrumentos de comunicación, etc., cada uno de los cuales se pagó.

f) Análisis estadístico

Cuando se tienen que valuar grandes cantidades de activos de información y resulta imposible valuarlos en forma individual se puede acudir a técnicas de muestreo estadístico. Este muestreo se apoya en alguna de las técnicas anteriores para asignar el valor monetario correspondiente. Este método es de particular utilidad cuando se tienen muchos registros de calidad (y por tanto de valor) no homogénea. Por ejemplo en una lista de compradores potenciales un registro que contenga, pero el que contenga un ingreso disponible confirmado por otros campos del registro tendrá aún más valor. Ante la imposibilidad de analizar todos los registros se toma una muestra estadísticamente adecuada, se hace el análisis, y de allí se infiere el valor de toda la lista.

Hay que seleccionar, si es posible, dos o más métodos para obtener un valor de la información que sea útil para el análisis de riesgos (Tabla 4.1). Cada método tiene características distintas y aplicaciones diferentes.

	Cualitativo		Cuantitativo	
	0		100	
Legislación	XXXX			
Entrevistas		XXXXXX		
Cuestionarios		XXXXXX		
Consenso		XXXX	XXXX	
Valor en libros			XXXX	XXXXXX
Estadística				XXXXXX

Tabla 4.1
Ejemplo de valoración de información

Se debe adoptar una estrategia para expresar esta valoración que concluya tanto el valor como los costos de mantenimiento (respaldos por ejemplo) y operación (verificación de la integridad por ejemplo). El valor debe expresarse en términos de algún periodo de tiempo, por ejemplo en forma anualizada, para que sea posible compararlo con el costo de las salvaguardas.

Una vez concluida la lista, se debe ponderar el riesgo contra el impacto que provocaría a la Organización que uno de sus activos estratégicos fuese afectado. En este punto también se recomienda el uso de herramientas hacker para evaluar, de forma más precisa, qué tanto riesgo tiene asociado un activo particular.

4.3.3 Identificación de amenazas

Una vez que conocemos los recursos que debemos proteger es la hora de identificar las vulnerabilidades y amenazas que se ciernen contra ellos. Como podemos recordar del capítulo 1, una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que puede aprovechar una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Cabe destacar que un cuanto hablamos de riesgo nos referimos a las amenazas que son aplicables en nuestro entorno de red en particular y ataque es cuando esa amenaza o riesgo se hace tangible. Otra subdivisión de éstos puede ser la siguiente:

Accidentales: Negligencia, ignorancia, confianza, falta de capacitación.

Intencionales: Vandalismo, espionaje, guerras, fraude, desagravio, represalias. Los usuarios internos con conocimiento representan un mayor riesgo.

Y además de las clasificaciones de amenazas que se describieron en el Capítulo 1 y en el párrafo anterior, suelen dividirse en tres grandes grupos, en función del ámbito o la forma en que se pueden producir:

a) Desastres del entorno

Dentro de este grupo se incluyen todos los posibles problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Por ejemplo, se han de tener en cuenta desastres naturales (terremotos, inundaciones...), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

b) Amenazas en el sistema

Bajo esta denominación se contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad, etc.. como ejemplo tenemos lo siguiente:

Errores y Omisiones: Pueden ser causados por el personal de sistemas y usuarios

- Errores en los programas que pueden ser benignos o catastróficos.
- Incluyen errores de instalación y mantenimiento.
- Una causa común es el mal control de calidad.
- La concientización y capacitación ayudan a la solución.
- Hay que evitar los dedos inexpertos.

c) Amenazas en la red

Como ya hemos comentado, cada día es menos común que una máquina trabaje aislada de todas las demás; se tiende a comunicar equipos mediante redes locales, intranets o la propia Internet, y esta interconexión acarrea nuevas - y peligrosas - amenazas a la seguridad de los equipos, peligros que hasta el momento de la conexión no se suelen tener en cuenta. Por ejemplo, es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos que necesitan acceder a ciertos recursos internos a la organización (como un investigador que conecta desde su casa a través de un módem).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad. Es algo normal que a la hora de hablar de atacantes todo el mundo piense en crackers, en piratas informáticos mal llamados hackers. No obstante, esto no es más que el fruto de la repercusión que en todos los medios tienen estos individuos y sus acciones; en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada, así como piratas externos a la entidad que aprovechan la habitualmente mala protección de los sistemas para acceder a ellos y conseguir así cierto status social dentro de un grupo de piratas. Los conocimientos de estas personas en materias de

sistemas operativos, redes o seguridad informática suelen ser muy limitados, y sus actividades no suelen entrañar muchos riesgos a no ser que se utilicen nuestros equipos para atacar a otras organizaciones, en cuyo caso a los posibles problemas legales hay que sumar la mala imagen que nuestras organizaciones adquieren.

Debido a la orientación de este trabajo de tesis, nos enfocaremos al análisis de estas amenazas en la red.

La naturaleza distribuida y la posibilidad de interconexión creciente de las redes ha dado como resultado que sean más vulnerables que los sistemas monolíticos o centralizados.

El análisis de las posibles amenazas en un ambiente de red implica tomar en consideración múltiples conceptos y componentes, entre los cuales los más importantes son los siguientes:

- Nodos locales
- Enlaces locales
- Redes locales
- Almacenamiento local de datos
- Procesos locales
- Compuertas a la red
- Enlaces de red externos
- Recursos de control de las redes
- Ruteadores en la red
- Recursos de la red

La exposición de los puntos anteriores a posibles intrusiones, malos usos, y abusos, trae como consecuencia las siguientes amenazas reales en un sistema de red:

- Intercepción de datos en tránsito
- Acceso a programas o datos en host remotos
- Modificación de programas o datos en host remotos
- Suplantación de un usuario para añadir información
- Inserción de una repetición de una secuencia
- Bloqueo de tráfico selecto
- Negación del servicio
- Ejecución de un programa en un host remoto

No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema: muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación; decir "no lo hice a propósito" no ayuda nada en estos casos. Por supuesto, tampoco tenemos que reducirnos a los accesos no autorizados al sistema: un usuario de nuestras máquinas puede intentar conseguir privilegios que no le corresponden, una persona externa a la organización puede lanzar un ataque de negación de servicio contra la misma sin necesidad de conocer ni siquiera un login y una contraseña, etc.

d) Ataques típicos en una red

Análisis de Tráfico

Las redes constituyen una fuente inagotable de información para cualquier atacante pasivo que monitoree el canal público y se dedique a registrar información, el atacante, posteriormente, puede, en general, inferir información mediante el exámen de los tributos de los mensajes en lugar de sus contenidos y, a partir de ello, montar un ataque activo. Este análisis involucra, entre otros, los siguientes aspectos:

- Frecuencia del tráfico
- Direcciones de origen
- Direcciones de destino
- Tráfico mixto

Negación de Servicio

El hecho de que un atacante pueda inhabilitar el uso de los recursos de una red o de un sistema por parte de los usuarios legítimos, constituye una de las principales amenazas a la seguridad en red. Esta amenaza aglutina un conjunto muy extenso y variado de ataques conocidos en la literatura como DoS ("Denegation of Service") y varían, en nombre de los ataques de acuerdo a la plataforma que atacan y al tipo de ataques pasa por evitar el uso de recursos físicos, robo o alteración, mediante el estricto control de acceso. También el retraso en los accesos de tiempo crítico es una forma de negación de servicio.

Otras formas de ataques de negación de servicio son las siguientes:

- Inundar la red con tráfico
- Bloqueo de transmisiones basado en direcciones
- Réplica de mensajes

Suplantación ("Spoofing")

La capacidad de un atacante para registrar, retener, modificar, sustituir, y reenviar información es lo que comúnmente se conoce como ataques por "spoofing" y constituye otras de las grandes amenazas a la seguridad en redes.

En general, este tipo de ataques hace uso de servicios bajo identidad falsa. Puede obtener acceso no autorizado a la información, o puede modificarla maliciosamente. Algunas de las manifestaciones de esta amenaza se refleja, entre otras, en las siguientes acciones:

- Réplica de passwords
- Modificación de direcciones de origen
- Comprometer passwords
- Réplica de mensajes

Monitoreo (Espionaje)

Esta amenaza consiste en la captura lícita de información mientras se transfiere entre las partes que se comunican. Este tipo de amenaza se diferencia del análisis de tráfico en que para realizarlo se requiere equipo especial y un conocimiento profundo de los protocolos de comunicación. El análisis de tráfico no requiere nada de esto, ya que el atacante sólo tiene que observar lo que fluye por la red sin equipo ni conocimiento especial. Algunas de estas amenazas son las siguientes:

- Intercepciones en enlaces de radio
- Intervención de canales (wiretaping)
- Emisiones desde equipos de comunicaciones
- Toma de paquetes ethernet desprotegidos en una LAN

Canales Secretos

Otra de las grandes amenazas a la seguridad en redes son los canales secretos o encubiertos, que consisten fundamentalmente en el uso de los mecanismos del sistema en forma inesperada, lo cual ocasiona fuga de información violando la política de seguridad del sistema. Un ejemplo de este ataque se ilustra en la figura 4.8.

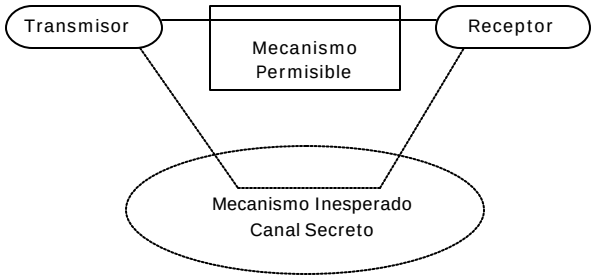


Figura 4.8
Canales Secretos

4.3.4 Medidas de protección

Tras identificar todos los recursos que deseamos proteger, así como las posibles vulnerabilidades y amenazas a que nos exponemos y los potenciales atacantes que pueden intentar violar nuestra seguridad, hemos de estudiar cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos). Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en nuestra organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale dicho recurso o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total. Por ejemplo, podemos seguir un análisis similar en algunos aspectos al problema de la mochila: llamamos al riesgo de perder un recurso *i* (a la probabilidad de que se produzca un ataque), y le asignamos un valor de 0 a 10 (valores más altos implican más probabilidad); de la misma forma, definimos también de 0 a 10 la importancia de cada recurso, , siendo 10 la importancia más alta. La evaluación del riesgo es entonces el producto de ambos valores, llamado peso o riesgo evaluado de un recurso, y medido en dinero perdido por unidad de tiempo (generalmente, por año).

De esta forma podemos utilizar hojas de trabajo en las que, para cada recurso, se muestre su nombre y el número asignado, así como los tres valores anteriores. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que esto significa que es probable que sean atacados, y que además el ataque puede causar pérdidas importantes. Es especialmente importante un grupo de riesgos denominados *inaceptables*, aquellos cuyo peso supera un cierto umbral; se trata de problemas que no nos podemos permitir en nuestros sistemas, por lo que su prevención es crucial para que todo funcione correctamente.

Una vez que conocemos el riesgo evaluado de cada recurso es necesario efectuar lo que se llama el análisis de costos y beneficios. Básicamente consiste en comparar el costo asociado a cada problema (calculado anteriormente) con el costo de prevenir dicho problema. El cálculo de este último no suele ser complejo si conocemos las posibles medidas de prevención que tenemos a nuestra disposición: por ejemplo, para saber lo que nos cuesta prevenir los efectos de un incendio en la sala de operaciones, no tenemos más que consultar los precios de sistemas de extinción de fuego, o para saber lo que nos cuesta proteger nuestra red sólo hemos de ver los precios de productos como *routers* que bloqueen paquetes o cortafuegos completos. No sólo hemos de tener en cuenta el costo de cierta protección, sino también lo que nos puede suponer su implementación y su mantenimiento; en muchos casos existen soluciones gratuitas para prevenir ciertas amenazas, pero estas soluciones tienen un costo asociado relativo a la dificultad de hacerlas funcionar correctamente de una forma continua en el tiempo, por ejemplo dedicando a un empleado a su implementación y mantenimiento.

Cuando ya hemos realizado este análisis no tenemos más que presentar nuestras cuentas a los responsables de la organización (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hemos de tener siempre presente que los riesgos se pueden minimizar, pero *nunca* eliminarlos completamente, por lo que será recomendable planificar no sólo la prevención ante de un problema sino también la recuperación si el mismo se produce; se suele hablar de medidas *proactivas* (aquellas que se toman para prevenir un problema) y medidas *reactivas* (aquellas que se toman cuando el daño se produce, para minimizar sus efectos).

4.3.5 Presupuesto

Las compañías por lo general intentan implementar productos de distintos proveedores para sus diferentes necesidades de seguridad. Muchas organizaciones recurren a entre tres y ocho proveedores distintos para implementar los diferentes procedimientos de seguridad, dependiendo de sus preocupaciones. La figura 4.9 muestra la forma en que un presupuesto de seguridad podría dividirse para una organización cliente/servidor. El porcentaje podría cambiar en distintos entornos. Sin embargo en un entorno basado principalmente en un mainframe, el porcentaje de la seguridad destinado al mainframe probablemente sería mayor.

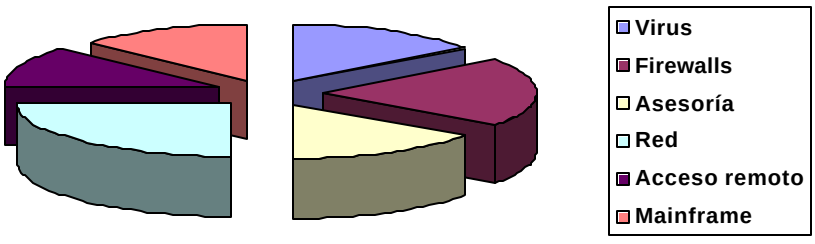


Figura 4.9
Ejemplo de inversión presupuesto de seguridad

En este ejemplo, el presupuesto de seguridad se divide en: el acceso remoto, el mainframe, la red, los virus, los firewalls y la consultoría. Este presupuesto de seguridad puede cambiar dependiendo de las necesidades de la compañía, pero da la idea de que la seguridad está dividida en niveles y que puede ser desglosado. Le corresponde a la administración decidir qué tipos de datos son importantes y qué datos no lo son. La referencia que los datos no son importantes, no implica que los datos mismos son prescindibles. La referencia es a la sensibilidad, por ejemplo, si ocurre una violación a la seguridad y los datos son modificados, ¿se podrían usar para dañar a la organización? Si no es así, entonces sólo será suficiente una copia de respaldo para este tipo de datos.

4.4 Cómo decidir un plan de acción

Cuando se decide por un plan de acción, hay que tomarlo con calma. Primero hay que poner las piezas en su lugar e intentar esquematizar el flujo del tráfico. Quizá aún no se haya decidido por la infraestructura, pero ahora puede saber con mayor certeza cuáles son los dispositivos con los que dispone. Dibuje la configuración de una topología. Es probable que ya tenga una; entonces sólo introduzca estos dispositivos en el dibujo e intente examinar el flujo de los datos. Cuando haga el dibujo, pregúntese cosas como ¿cómo autenticar a los usuarios?, ¿En que subredes serán admitidos?, ¿en qué momento ocurre el proceso de cifrado? Después de considerar este flujo de ideas, comience a procesar esta información y en el flujo de ideas, no es necesario plantearse una solución, lo que necesita plantear es un conjunto muy extenso de preguntas para hacerle a los proveedores potenciales o su área de sistemas. Estas respuestas determinarán la configuración óptima.

Al plantearse estas preguntas, es importante que recuerde que debe pensar en la problemática como si se tratara de un sistema. Observe la figura 4.10 y piense cuántos aspectos debe considerar.

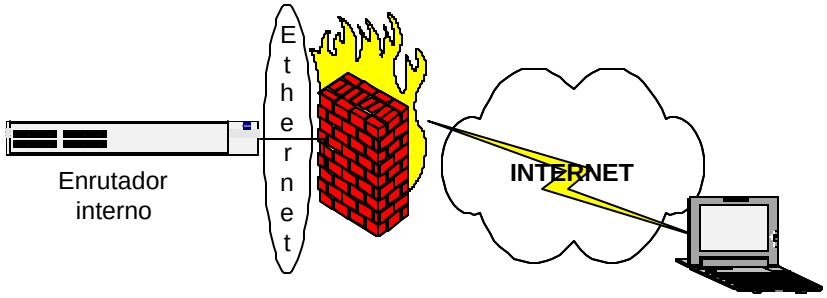


Figura 4.10
Propuesta del sistema para implementar una VPN

Probablemente éste es el concepto de túnel de VPN más sencillo en el que pueda pensar, un equipo remoto conectado a un firewall/VPN. El procedimiento debería ser directo, la configuración debería simplificarse y la conexión de datos tendría que estar automatizada. Sin embargo, si piensa así, puede cometer varios errores y dar cosas por hechas, lo cual provocará problemas posteriores.

A continuación listamos algunos de los aspectos que deben tomarse en cuenta antes de la implementación.

Espacio para la dirección IP

En cualquier escenario de VPN, necesitará espacio para la dirección IP. Es probable que decida utilizar una traducción de dirección de red pero, aún así, necesita una dirección IP válida para crear el túnel, o tendrá que determinar con el túnel un punto de acceso del límite con Internet, por ejemplo en un firewall.

Aspectos del DNS

Debe preocuparse por quién hará su DNS. Si obtiene un nuevo espacio para direcciones IP, necesitará configurar un servidor DNS en algún lado para que sus usuarios de Internet puedan encontrar los servidores de la red. Si utiliza un servicio de VPN administrado, entonces es probable que su proveedor proporcione este servicio.

Aspectos del enrutamiento

Deberá prever qué tablas de enrutamiento serán necesarias para la empresa. Las VPN son IP a IP; por lo tanto, deberá tener un algoritmo de enrutamiento para mantener el tráfico en su red local.

Traducción de direcciones de red

NAT ofrece la capacidad para establecer una conexión a Internet. Además ofrece la capacidad para ocultar la dirección interna de una compañía detrás de varias direcciones IP. Estas direcciones normalmente se implementan de un firewall, lo cual significa que cada paquete que llega se termina en el firewall y sólo éste lo reenvía.

Cifrado

Si es como la mayoría de los usuarios de VPN, no sabe ni siquiera cuál es el tipo de cifrado que utilizará, desde luego, el fabricante le dirá qué tipo de productos soporta, pero probablemente utilice el algoritmo de cifrado que viene con el producto. Además ¿Cuántos equipos portátiles utilizarán la VPN? También necesitará cargar en esos equipos el mismo software para cifrado.

4.4.1 Ubicación de la arquitectura VPN

Después de decidir que tipo de dispositivo utilizará, debe decidir dónde lo colocará. En el capítulo 2 se describieron los distintos tipos de arquitecturas y de topologías de VPN, las cuales deberían darle una idea de dónde colocar el dispositivo VPN. Se debe colocar cerca del punto de conexión a Internet. Por consiguiente es necesario preguntarse, ¿hay un ruteador, firewall o una subred independiente que quiera utilizar?

Una de las primeras preguntas que debe hacerse es ¿dónde colocar este dispositivo? Observe la figura 4.11; la empresa tiene dos departamentos en distintos puntos geográficos. Si quisiera, podría colocar dos dispositivos de VPN pero eso puede aumentar el trabajo y los gastos. Así que debe establecer un lugar adecuado. Desde luego. Un buen punto podría estar donde se localiza el personal capacitado, puesto que el tiempo de inactividad es crítico y es imprescindible que las cosas se resuelvan rápidamente.

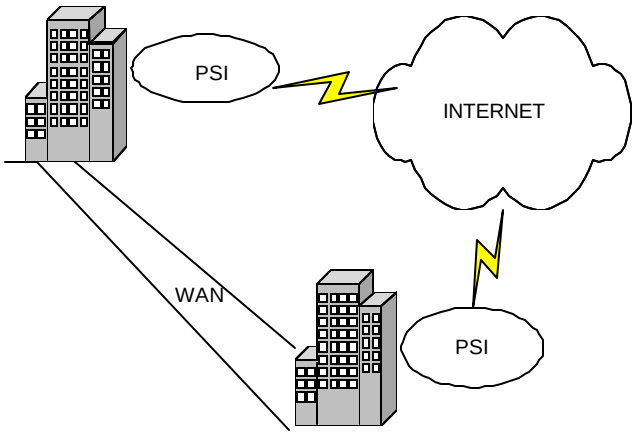


Figura 4.11
Sitios de VPN geográficamente distintos

4.4.2 Problemas de enrutamiento

Suponiendo que se decida colocar el dispositivo en una ciudad, pero también va a dejar ambas ciudades con sus respectivos proveedores de Internet, el siguiente problema con el que se enfrenta es con el enrutamiento. Eso puede solucionarse utilizando nombres de dominio para cada una de las entidades, o bien, para la entidad principal.

En el caso de los accesos remotos, por ejemplo de una computadora portátil, cuya dirección pudiera ser 220.220.220.10:

1. El equipo portátil utilizando su configuración de conexión a la red, establece una conexión PPP a un PSI local y se le asigna una dirección pública enrutable de red.

2. El software cargado en el equipo establece una conexión con el firewall/VPN de la Ciudad de México. Esto puede hacerse manualmente o por un proceso automático en el equipo.

3. El Firewall de la Ciudad de México responde con la clave apropiada. Otra pieza de información que se envía al equipo portátil es el dominio de la VPN, el cual consiste en la dirección del servidor de Puebla.

4. El equipo portátil ahora intenta conectarse al servidor de Puebla en la red 220.220.220.10.

5. Conforme la solicitud desciende en la pila OSI, el software del equipo portátil sabe que la dirección IP 220.220.220.10 es parte del dominio de la VPN. Por lo tanto cifra y encapsula todo el paquete con una nueva dirección IP. La nueva dirección IP es la dirección pública del Firewall de la Ciudad de México.

6. El Firewall desenvuelve la IP y descifra el paquete. Sabe que la solicitud es para un servidor válido en el dominio de la VPN. De acuerdo con los procesos de autenticación de usuarios establecidos, el Firewall solicitará la autenticación para el equipo portátil.
7. Una vez que el equipo portátil se autentica, el Firewall revisa los permisos para ver si el usuario puede acceder al servidor de Puebla. Si es así, el Firewall envía los datos en texto simple por la red interna hasta el servidor de Puebla.

8. El servidor ve la solicitud y responde (si los permisos apropiados se establecen) al dispositivo de destino, el cual es el Firewall.

El software de cifrado del equipo portátil sabe qué redes están en su dominio de VPN. Para un administrador esto significa que tiene que configurar la VPN para que le "indique" al equipo remoto de qué dominio será parte. Éste también es un aspecto de configuración; algunas VPN sólo permiten un dominio, mientras que otras permiten varios.

4.4.3 Ubicación de la topología

Después de estudiar la ubicación de la arquitectura y ver los posibles problemas de enrutamiento, se debe considerar la ubicación real del equipo en la red local. Como con todo lo demás en la tecnología de la VPN, existen distintas formas de ubicar este equipo. Distintos tipos de arquitectura pueden colocarse de manera diferente. Conforme la empresa necesite más servicios, estos se colocarán cerca del dispositivo de la VPN.

Es importante recalcar que la ubicación de la topología siempre irá en base del análisis de tráfico y del tipo de VPN que se quiera implantar, aunque siempre recae en la proximidad de la conexión a Internet. En la siguiente figura se pone el ejemplo con una VPN basada en Firewall.

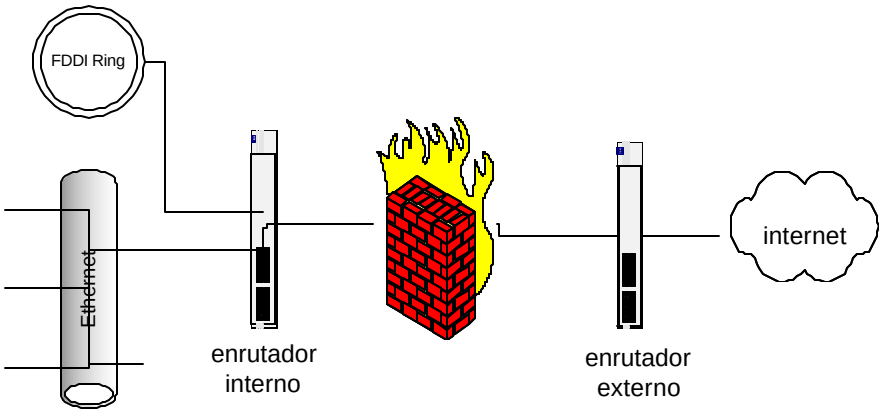


Figura 4.12
Ubicación del Firewall/VPN

En este capítulo se dieron las bases para implementar una VPN más que nada orientado a un dispositivo de Firewall, que actualmente es la configuración más común. Aunque dependiendo de los requerimientos de la empresa, esta configuración puede ser diferente. La razón para elegir una configuración de Firewall es que ésta contiene todos los pasos necesarios para implementar la seguridad y una VPN. Si la empresa ya cuenta con un Firewall y sólo está agregando la VPN independiente, entonces puede ser tan sencillo como conectar y usar. Si no necesita todos los pasos desarrollados a lo largo del capítulo.

5 IMPLANTANDO LA VPN

5.1 El escenario

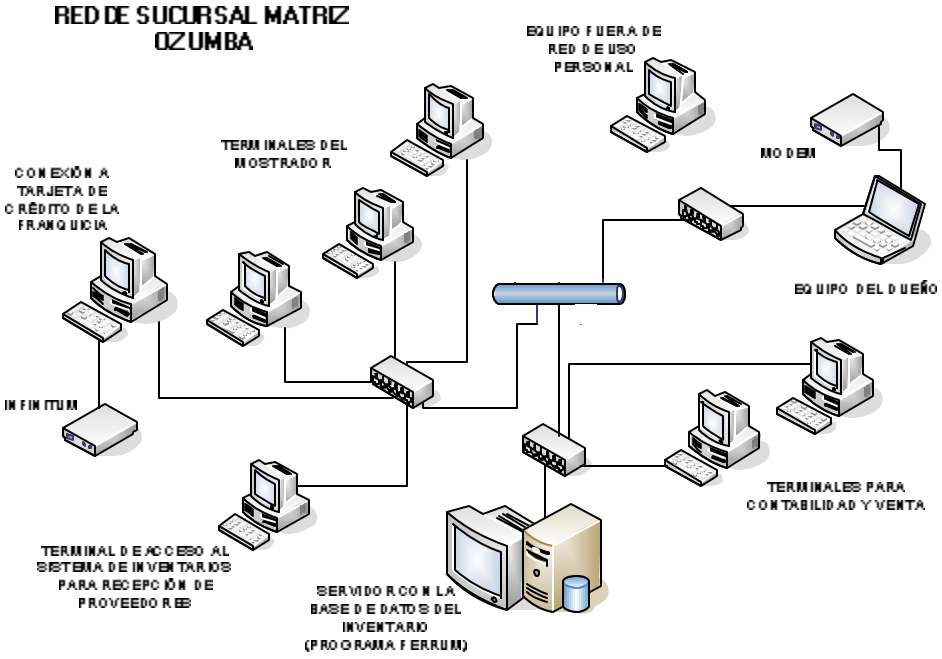
Se aplicaron algunos de los conceptos y recomendaciones tratados a lo largo de esta tesis en la conexión de tres sucursales de tres franquicias de una importante ferretería. Cada una de ellas localizadas en tres poblaciones distintas del Estado de México. La tienda principal se localiza en Ozumba, otra más en Tepetlixpa y por último una más en Amecameca.

Estas tres sucursales pertenecen a un pequeño empresario del Estado de México, y que gracias a su esfuerzo logró crecer con estas tres sucursales, pero debido a ello y a la inseguridad que atraviesa actualmente nuestro país fue secuestrado por lo que para él es importante no tener que hacer viajes frecuentes a sus sucursales por miedo a que suceda nuevamente.

Distribución de las redes de la empresa:

1. Sucursal Matriz, OZUMBA. Esta Sucursal tiene la tienda, la caseta de recepción, una pequeña oficina en la parte posterior y en la parte superior de las mismas la oficina y domicilio del dueño. En la figura 5.1 vemos como estaban conectadas estas sucursales bajo un pequeño grupo de trabajo con el nombre de "FORTALEZA". En el mostrador tienen 3 máquinas cliente y en la caja se encuentra la de la tarjeta de crédito de la franquicia, que tiene conexión a la base de datos, pero que no comparte recursos y se encuentra conectada a Internet.

   En la caseta de recepción de material y proveedores se encuentra una Terminal tonta con conexión a la Base de Datos. En la oficina de la parte posterior se encuentran dos máquinas de trabajo para las contadoras y el servidor con la bases de datos que cuando hay mucha carga de trabajo también funciona para ventas de mostrador.



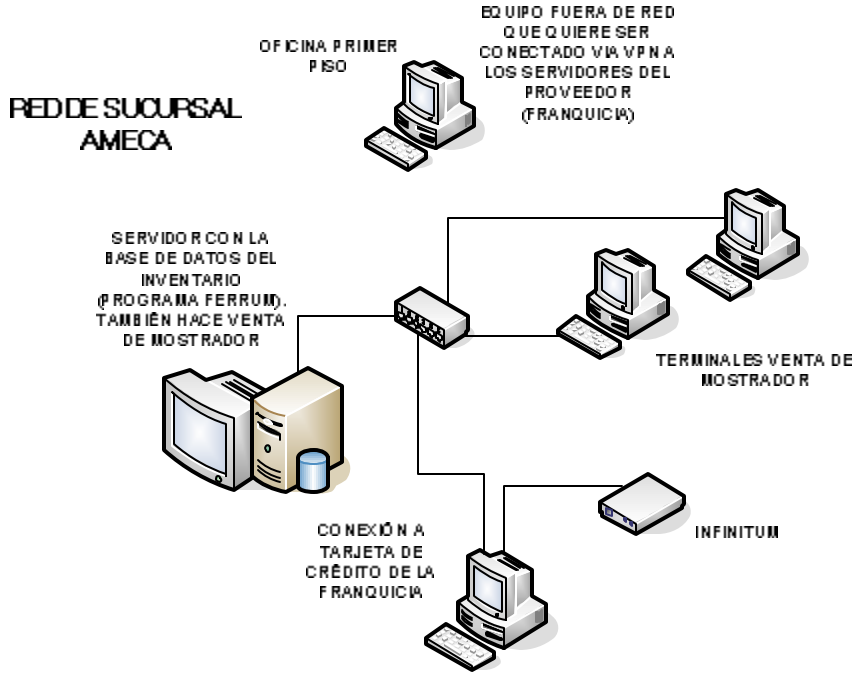


Figura 5.2
Red original Ameca (Sucursal)

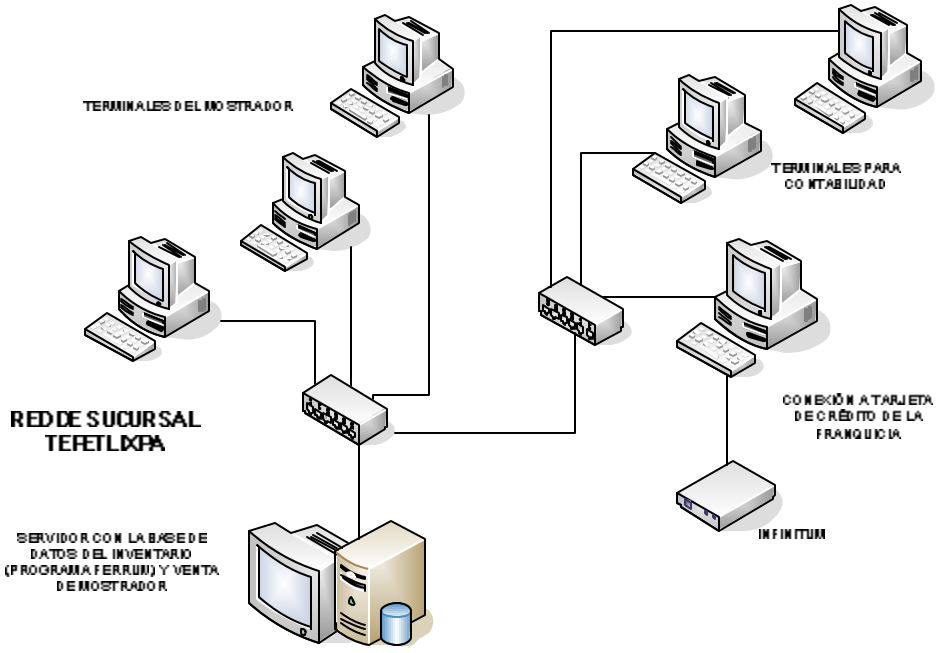


Figura 5.3
Red original Tepetlixpa (Sucursal)

5.1.1. Requerimientos del cliente

El dueño nos requiere lo siguiente; conectar sus tres sucursales y tener acceso desde un equipo móvil que la mayoría de los días se encuentra en una oficina en la parte superior de la tienda matriz, pero con la facilidad de poder seguir teniendo el control cuando sale de viaje.

Hay otros pequeños requerimientos adicionales:

1) Sólo las máquinas de caja propias de la tarjeta de crédito de la franquicia tienen conexión a Internet, por medio de un ADSL de 128 mbps, por lo que se pretende compartir dicha conexión a la red para que tanto el dueño como la máquina personal y las oficinas de contabilidad tuvieran accesos.

2) Aunque las oficinas de contabilidad deben acceder a Internet pero sólo a las páginas de Bancos o proveedores, por lo que debía restringirse el acceso.

3) Se debe conectar la máquina de uso personal de la sucursal matriz a la red pero nadie debe accesarla.

4) En una oficina del primer piso de la sucursal Ameca se encuentra una máquina recién adquirida que pretende se conectada a la BD del sistema para revisar inventarios y lo más importante es que se conectaría también vía VPN con un software propietario del proveedor.

Como estamos hablando de un pequeño empresario, que aunque si cuenta con cierto presupuesto, no puede gastar en soluciones costosas. Algo muy bueno de este ejemplo es que se trata también de un empresario interesado no sólo en la seguridad física de su negocio, si no también en la seguridad de su información.

Se eligieron equipos de marca Lynksys, en específico el modelo BEFVP41 debido a varias de las ventajas que presentamos en el Capítulo 4. En general lo que nos motivó fue el hecho de que es un ruteador con VPN que tiene su propio Firewall, que además es de un precio bastante accesible. Otra ventaja sobre otros proveedores es que tiene capacidad para triangular las redes, es decir, puedo conectarme con 10 redes al mismo tiempo. Con esto estamos dándole al pequeño empresario una opción que le permitirá conectarse aún si aumenta el número de sus sucursales a 10. Se adquirió un equipo para cada una de las sucursales.

5.2 Instalación de los equipos VPN

Antes de la instalación se verificaron que las condiciones de la red fueran las adecuadas para aceptar la implantación de la red virtual privada. Por esta razón lo primero que se hizo fue una revisión física de los equipos para validar las condiciones y capacidades de los mismos; para recordar lo que debe evaluarse se puede apoyar en los conceptos que se revisaron en el capítulo 4.

Después del el análisis y considerando que las máquinas que queremos introducir a la red virtual privada cuentan con los elementos necesarios para hacerlo, es decir, tarjeta de red, capacidad de procesamiento y sistema operativo compatible; se hicieron los siguientes pasos para conectarlas a Internet:

1) Los equipos routers BEFVP41 se instalaron en los servidores de cada sucursal. La manera de conectarlos se describe en la figura 5.4 para cada punto.

2) El servidor se conectó al router y éste a su vez al hub en donde se encontraban conectadas todas las máquinas de la red. Las características de estos equipos ADSL es que distribuyen el Internet configurando la conexión del enlace en ellos.

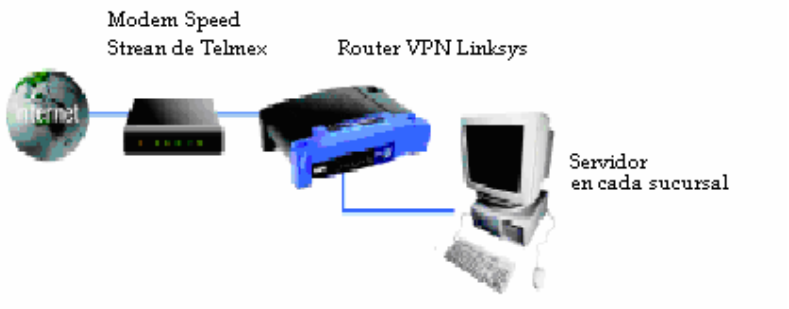


Figura 5.4
Forma de conectar el router VPN al servidor

Para cada sucursal con su respectivo servidor se conectó de la misma forma.

La configuración de los tres routers BEFVP41 se hizo de acuerdo a las especificaciones que el equipo debe tener en cada punto y como se detallará más adelante. Es importante hacer notar que las tres redes deben estar en tres diferentes nubes de Internet para poder establecer la conexión. Lo que queremos decir con esto es que las direcciones IP de cada red deben estar en un segmento distinto para poder identificarlos tanto para los servidores como para los nodos. La dirección que tiene asignada de fábrica es la 192.168.1.1, por lo que por cuestiones prácticas se asignaron de la siguiente manera:

- ozumba 192.168.1.1
- tepe.ath.cx 192.168.2.1
- ameca.ath.cx 192.168.3.1

Para tener un acceso rápido y eficiente a los equipos se pueden dar de alta dominios. Una manera sencilla sugerida para tener este servicio es ingresar a la página www.dyndns.org.

Para este proyecto se dieron de alta los siguientes dominios:

- ameca.ath.cx
- tepe.ath.cx
- ozumba.ath.cx

Lo que resolvemos con esto es que se fijan estos dominios y ya no importa que las direcciones de Internet sean dinámicas porque el dominio se encarga de reconocer la IP con la cual se está trabajando en ese momento. Es decir, si no se hiciera por medio de dominios, cada vez que se entablara conexión con el proveedor de Internet se tendría que dar de alta la nueva dirección que nos asigne.

Para ingresar a los equipos se debe de hacer con el Explorador de Windows a través de su dirección IP.

Es importante hacer notar que el tráfico en los túneles debe ser con protocolo TCP/IP para las características que tienen estos equipos, sin embargo para este proyecto nos encontramos que en las tres sucursales se trabaja con una aplicación que opera en una red de protocolo Lantastic llamado FERRUM el cual solo se ejecutará desde otra sucursal instalando un programa que permita el acceso de un servidor a otro. Se eligió PcAnywhare que tiene la característica de poder establecer conexiones a través de túneles con otra máquina que tenga instalado de igual forma este software con una configuración VPN. La importancia de que tenga dicha configuración VPN es que la conexión pase por un medio seguro, ya que el empleo de este tipo de software hace que la información pueda ser interceptada en Internet.

5.3 Configuración de los equipos

Las ventajas que se tienen al conectar este tipo de equipos es que son compatibles con diversos sistemas operativos. Los equipos Linksys BEFVP41 son compatibles con sistemas operativos como Win 95, 98, 2000, Me y tienen la característica de compartir la señal ADSL.

Podemos tener varias formas de conectar dependiendo de las características que se tengan en la red, los equipos BEFVP41 cuentan con cuatro puertos RJ45 y un puerto INTERNET

que es en donde llega la señal ADSL, podríamos decir que podemos conectar cuatro computadoras en red que estarían compartiendo el Internet. Estos cuatro puertos no limitan la conexión de red a 4 equipos (figura 5.5), podemos hacer la red tan grande como se quiera, esto se puede lograr conectando switches en cascada partiendo del router de la VPN (Fig. 5.6) Existen switches y hubs que contienen infinidad de puertos y que repiten la señal a todos los que se conecten a ellos.

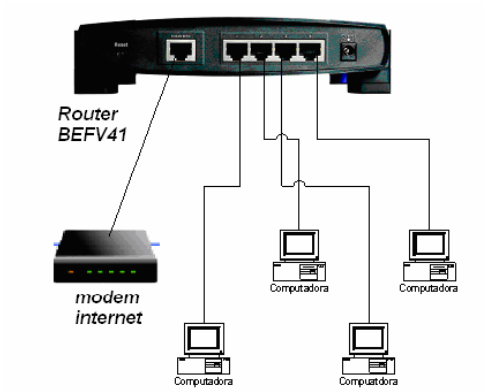


Figura 5.5
Conexión de una red de 4 computadoras

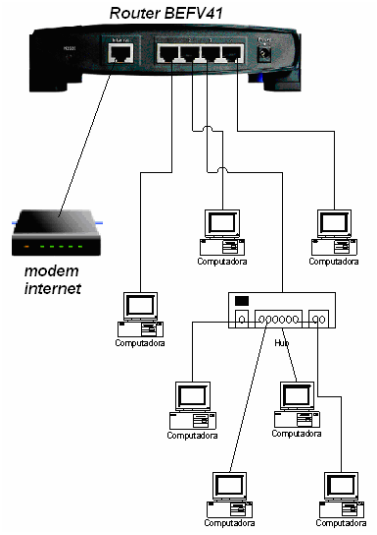


Figura 5.6
Red extendida conectando un hub al router

5.3.3 Configuración final de la red para cumplir requerimientos del empresario

En atención a los requerimientos del empresario se hicieron algunas modificaciones a la red, antes de continuar con la configuración. Quedando de la siguiente manera:

Sucursal Ozumba:

Se dio de alta en la red el equipo de uso personal y además se movió de lugar la conexión ADSL hacia el servidor principal ya que en la caja cortan la corriente al cierre de la sucursal, impidiendo que se conecten tanto los usuarios de la casa como de las oficinas. (Ver figura 5.7)

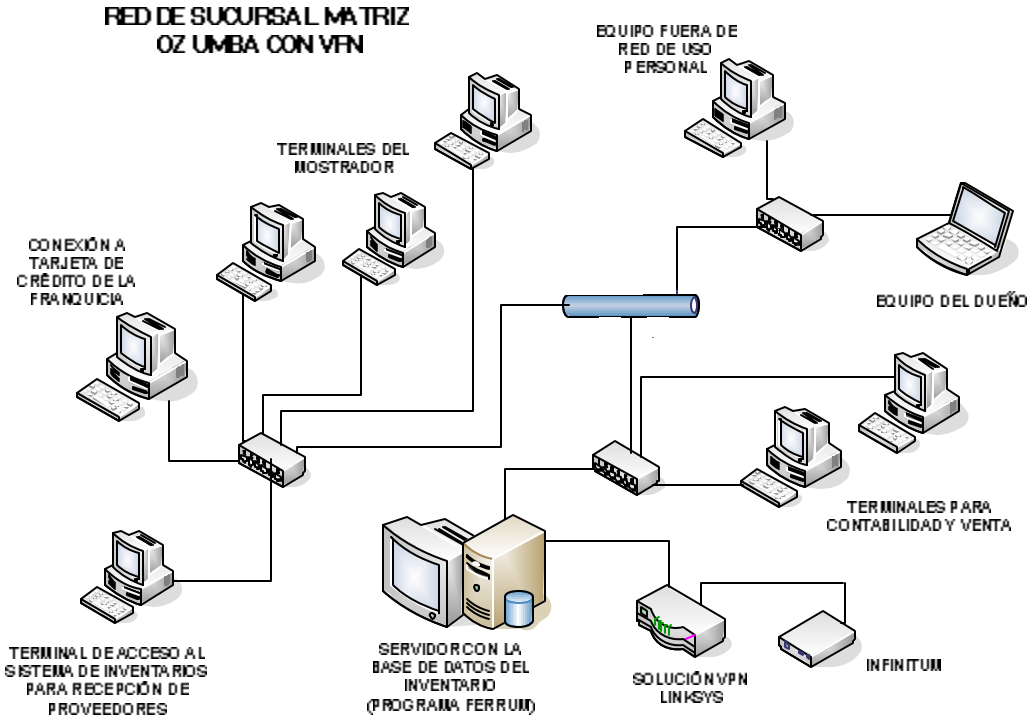


Figura 5.7
Red modificada Ozumba (Matrizl)

Sucursal Ameca:

Se conectó la máquina de la oficina superior, pero no apoyamos con la instalación del software propietario de la franquicia para conectar su VPN, sin embargo se aprovechó la configuración de la red y el Routeador de VPN para conseguir dicho acceso. Para conectar dicha máquina lo único que fue necesario hacer fue un cable de red suficientemente largo para conectar el switch con la máquina en el primer piso. Cuando se hacen este tipo de conexiones con cables largos de red es importante no pasar el largo máximo especificado para el tipo de cable que estemos utilizando. Se incluyó dentro del segmento de red y grupo de trabajo a la máquina de tarjeta de crédito de la franquicia. (Ver figura 5.8)

Sucursal Tepetlixpa:

Básicamente se dejó la misma configuración sólo se conecto el ADSL directo al switch de la caja para poder configurar el Internet. Se incluyó dentro del segmento de red y grupo de trabajo a la máquina de tarjeta de crédito de la franquicia. (Ver figura 5.9)

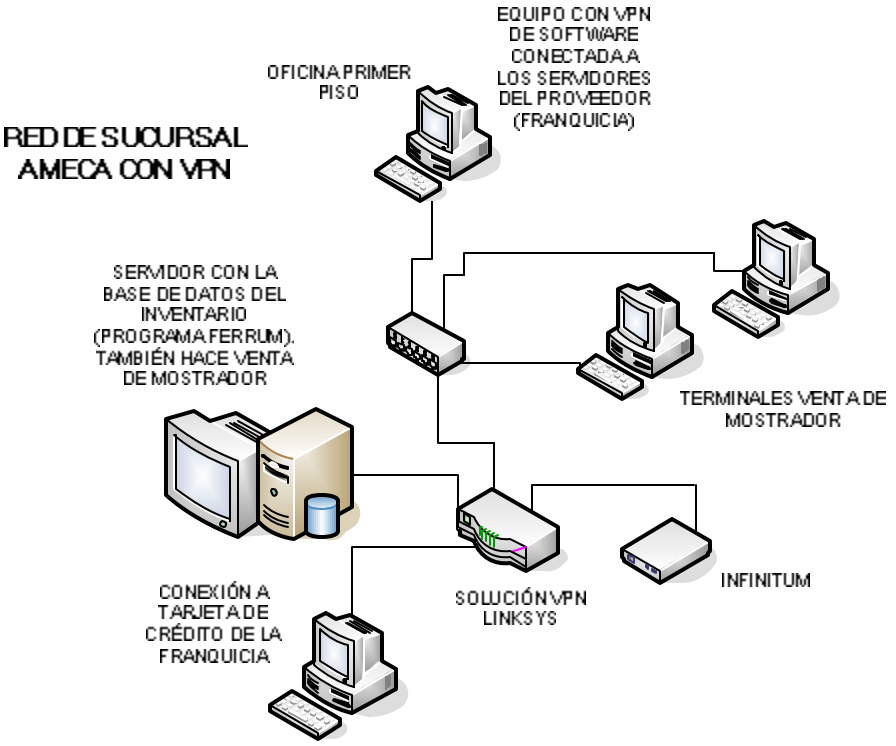


Figura 5.8
Red finall Ameca (Sucursal)

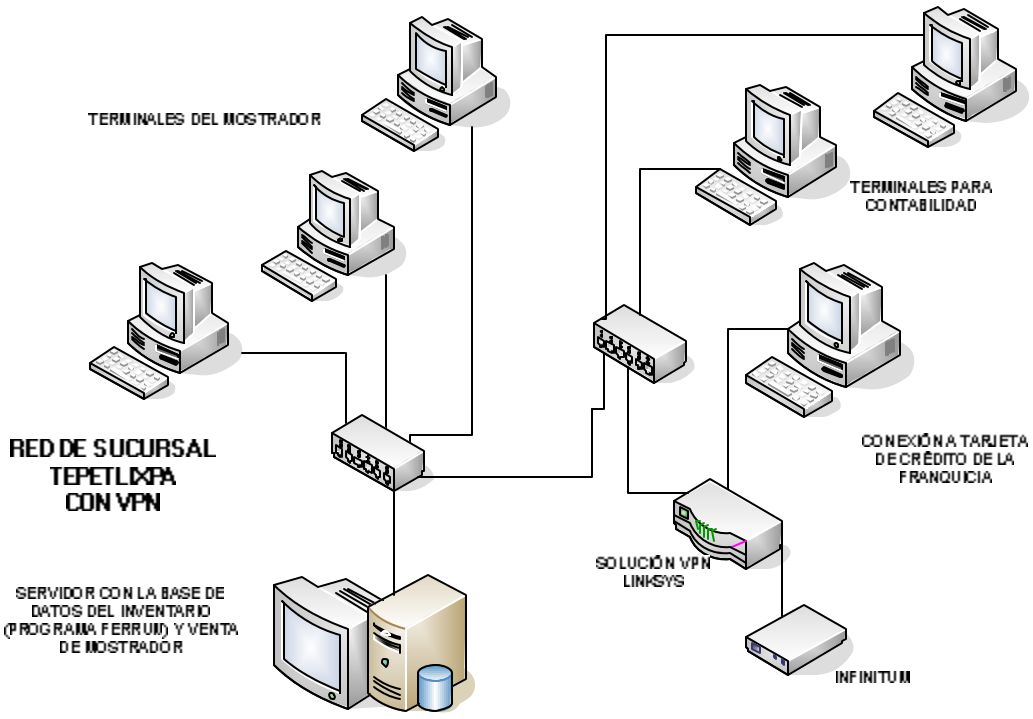


Figura 5.9
Red final Tepetlixpa (Sucursal)

5.3.2 Pasos de la configuración del equipo BEFVP41

La configuración del equipo fue la siguiente (Primero se configuraron los equipos Router Linksys BEFVP41):

En la figura 5.10 se muestra la pantalla para la configuración del Router BEFVP41 de Linksys a continuación se muestran las partes a configurar en esta pantalla para una mejor comprensión y apreciación. Como mencionamos antes el acceso a la pantalla de configuración debe ser por medio de Internet Explorer ya sea llamando al dominio o a la red local, por ejemplo para Ozumba sería 192.168.1.1.

Figura 5.10
Configuración del router para establecer el túnel

SETUP

Internet Setup

Conection Type: PPPoE

Como se trabaja con Internet Infinitum debemos tener este protocolo.

PPPoE Settings

User Name: 5979761432
Password: ****
Service Name: Prodigy Infinitum
Connection: Keep Alive

Nota: Esta última opción es muy importante porque es la que reestablece la conexión de los túneles aun cuando se apague el equipo. Cuando se encienden nuevamente se levantan los túneles automáticamente.

Optional Settings

Host name: BEFVP41
Domain Name:

MTU:

MTU: Manual
Size: 1400

Internet Setup

Router Setup

Local IP Adress: 192.168.1.1
Subset Mask: 255.255.255.0

Network Adress Server Settings

Local DHCP Server: Enable
Start IP Adress: 192.168.1.100
Number of Adress: 50

Estos son los datos generales en la pestaña de setup que definen las direcciones de las que se va a disponer en esa localidad así como la dirección en el lugar en el que nos encontramos.

Una vez que llenamos esta información, salvamos los cambios.

5.3.3 Configuración VPN

En las siguientes líneas veremos cómo se hizo la configuración de la VPN recordando las direcciones establecidas en cada punto son las siguientes:

- 192.168.1.1 Ozumba (Matriz)
- 192.168.2.1 Tepetlixpa (Sucursal)
- 192.168.3.1 Amecameca (Sucursal)

Es importante recordar estas direcciones porque las emplearemos para hacer los enlaces a través de los túneles a configurar en cada router como vemos en la figura 5.11:

Figura 5.11
Configuración del Túnel

Security
VPN

VPN Passthroug

IPSEC Pass-through: Disable
PPTP Pass.Through: Disable

VPN Tunnel

Select tunnel entry: Tunel 1, Tunel 2, Tunel 3.....Tunel 50 (segun sea el caso)
VPN Tunnel: Selected

Tunel Name: Nombre del tunnel

Local Secure Group:
Subnet
IP: 192.168.1.0
Mask: 255.255.255.0

Remote Secure Group
IP: 192.168.2.0
Mask: 255.255.255.0

Remote Secure Gateway
Any

Encryption
DES
Autentication: MD5

Key Management
Auto IKE
PPS: Disable
Pre-Shared Key: la determinada
Key Lifetime: 3600

Status
Mostrará el status en el que se encuentran los túneles si son conectados o desconectados

De esta forma es como se configura el túnel VPN, el tráfico que pase a través de él será con la encripción que se asigna al equipo o con las que opere. Ya en el capítulo anterior se habló sobre encripción.

Los equipos soportan hasta 50 túneles, y se recomienda que si se van a utilizar más de 10 se cuente con un buen ancho de banda ya que el tráfico sería más pesado.

El tener un buen ancho de banda garantiza que el tráfico del túnel llegue de manera transparente al otro lado del túnel, como si se estuviera en tiempo real. Las encripciones pueden ser las causantes del defase en el envío y entrega de información.

Para que el tráfico de información sea confiable y fluido es muy importante contar con un enlace estable, de manera que no existan perdidas de paquetes de información y mucho menos la caída de los túneles. El no contar con un buen enlace puede originar en una VPN problemas como una conexión inapropiada, perdida de información, retrasos u operación muy lenta del lugar remoto.

5.4 Conexión y configuración de los clientes móviles

En este apartado se explica como se hace la instalación de clientes móviles. La forma de conectar es como se muestra en la figura 5.12. La instalación de la red en cada sucursal es como se explicó anteriormente, es conectando el router BEFV41 directamente al ADSL que da el enlace y al servidor de cada sucursal. Ahora bien, un cliente móvil como es de suponerse debe de contar con conexión a Internet para poder conectarse a su Red Virtual Privada.

Figura 5.12
Conexión de clientes móviles

Pensando que la computadora cliente que en este proyecto en específico se encuentra en otra oficina o cabe la posibilidad de se encuentre en otra ciudad de donde vacacione el empresario. Se instala un software para clientes VPN, para este proyecto se utiliza el software GREENBOW. Este software tiene la característica de ser compatible con equipos de diferentes marcas y hace la conexión VPN a una red remota.

La instalación del software es sencilla comprando la licencia correspondiente. La configuración se detallará en el siguiente punto. La licencia la pueden adquirir en la página de Internet www.thegreenbow.fr.

5.4.1 Configuración del Software Greenbow para clientes móviles

Como mencionamos anteriormente en los clientes móviles instalamos un software llamado **greenbow**, éste tiene la característica de que es compatible con el equipo BEFVP41 de Linksys y otros equipos.

La configuración del software para la conexión VPN es similar a la de los equipos que mostramos anteriormente.

http://www.thegreenbow.fr/doc/tgbvpn20x_en.pdf

El cliente VPN de The Greenbow es una solución completa de clientes IPsec para todas las versiones de Windows. Este cliente provee encripción DES, 3DES y AES y autenticación MD5 y SHA.

5.4.1.1 Instalación del software

Para la instalación del software no requerimos de información compleja pues es una instalación clásica de Windows, al final de la instalación el software pedirá el reinicio de la máquina.

Una vez que la máquina ha reiniciado se abrirá una ventana solicitando el número de licencia (figura 5.13).

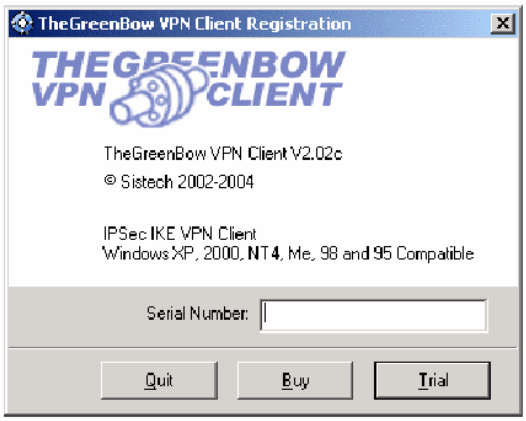


Figura 5.13
Ventana de solicitud de licencia

Si el número de licencia es correcto el cliente VPN se activará (figura 5.14). En la barra de tareas se activará un icono azul verdoso para iniciar la configuración.

El cliente VPN consiste de dos unidades:

- de interfase de configuración
- demonio IKE

Figura 5.14
Icono en la barra de tareas

Este icono es el que aparece en la barra de tareas una vez que el túnel VPN está habilitado. Haciendo clic en el botón izquierdo se abre el menú de configuración (figura 5.15). Y haciendo clic en el botón derecho se abre el menú del programa.

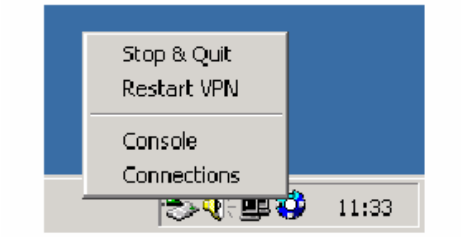


Figura 5.15
Menú de configuración

"Stop and Quit" cierra o establece los túneles VPN, detiene el servicio IKE y la interface de configuración.

Cuando se vuelve a cargar el cliente VPN , se da clic en el cilente VPN de Greenbow o bien en el menú "Start > Programs > TheGreenBow > VPN > TheGreenBow VPN".

- "Rerstart VPN" reinicia el túnel
- "Console" muestra el registro de windows
- "Connections" abre la interface de configuración con las listas o con el tunel VPN establecido.

Para salir del software:

Si se desea salir del software se tiene que seleccionar "stop & Quit" del menú del sistema. Se debe dejar algunos segundos para que el demonio IKE cierre apropiadamente y que los tuneles sigan trabajando.

5.4.1.2 La ventana Main

La ventana de Main (fig. 5.16) está compuesta por:

- Tres componentes en la columna izquierda que contienen toda la configuración de IKE e IPsec.
- Tres botones “Console”, “Parameters”, “Connections”.
- Una ventana de configuración que muestra los tres niveles elegidos.

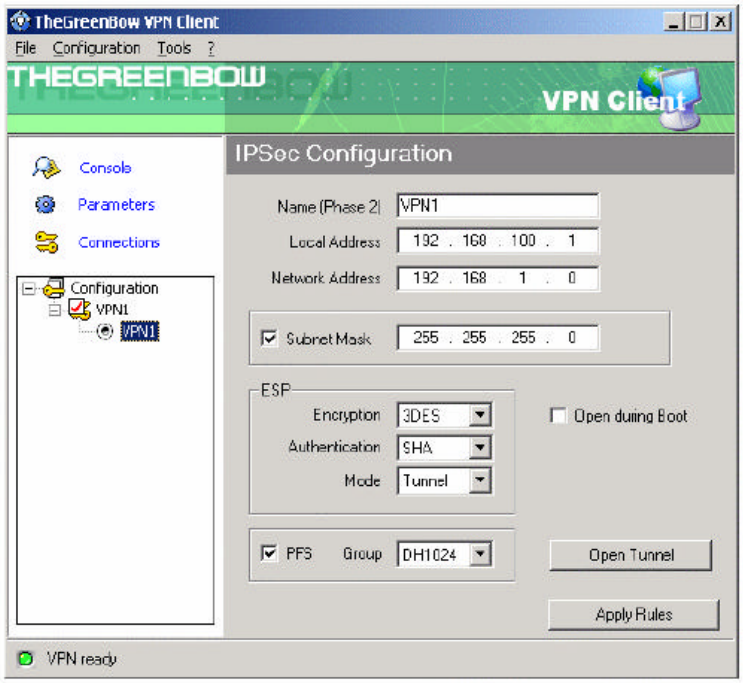


Figura 5.16
Ventana Main

El menú de Main

- El menú “File” es usado para cargar y salvar la configuración. Con esta característica se podrá importar y exportar la configuración VPN.
- El menú “Configuration” contiene todas las acciones del árbol de control haciendo clic derecho.
- También el menú de configuración da el acceso al asistente para configuración.
- El menú “Tools” contiene a las opciones “Console” y “Conections”.
- El menú “?” da el acceso en línea a la ayuda de Windows.

La barra de status

El botón izquierdo muestra el status con:

- “VPN Ready”: el demonio IKE (o servicio activo). Esto no necesariamente quiere decir que existe un túnel establecido.
- 'Configuration VPN update': El demonio IKE es reiniciado y se encarga de leer la configuración. Este mensaje aparece cada vez que se hace clic en el “Apply rules”.
- 'VPN tunnel active': quiere decir que una VPN está activa (el LED debe de estar en color rojo).
- 'Wait for VPN is ready...': este mensaje indica que el demonio no esta cargado o hay hay problemas de comunicación entre la interfaz de usuario y el demonio IKE (El color de LED es gris)

Si se tiene que trabajar con Windows 95,98, Me:

- Detenga el proceso "TgbStarter.exe"
- Se debe volver a ejecutar haciendo doble clic en: C:\Windows\System\tgbstarter.exe
- Se ejecuta la aplicación VPN

Si se tiene como sistema operativo Windows NT4, 2000, XP:

- Salga de la interfase VPN
- En el shell hacer "**net stop "tgbike starter"** "
- Hacer "**net start "tgbike starter"** "
- Ejecutar la interface VPN

Ventana “About”

La ventana “About” (figura 5.17)da la versión de la interfaz del software del cliente VPN y el demonio IKE. También proporciona un sitio en INTERNET URL para los usuarios.

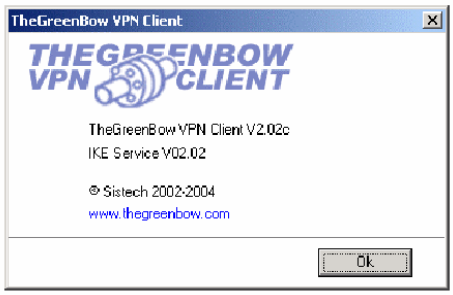


Figura 5.17
Ventana about (acerca de)

5.4.1.3 Configuración del Túnel (Asistente)

El cliente VPN integra un asistente que permite la creación de la configuración VPN en un árbol de pasos. Este asistente esta diseñado para computadoras que necesitan conectarse a una LAN corporativa a través de un pasaje VPN.

Nota: La configuración del cliente VPN con algunos gateways está disponible en el sitio web siguiente:

http://www.thegreenbow.com/vpn_doc.html.

La figura 5.1 muestra todo el contenido de la conexión VPN de nuestra conexión:

- La computadora remota tiene una IP publica dinámica por lo que se dio de alta el DNS
- Trata de conectarse a la red LAN a través del túnel VPN que tiene un DNS ozumba.ath.cx.
- En la LAN remota, se tendrá una dirección IP fija 192.168.100.1
- Se hace el acceso remoto con los recursos compartidos en la LAN como el servidor con la dirección IP 192.168.1.10.

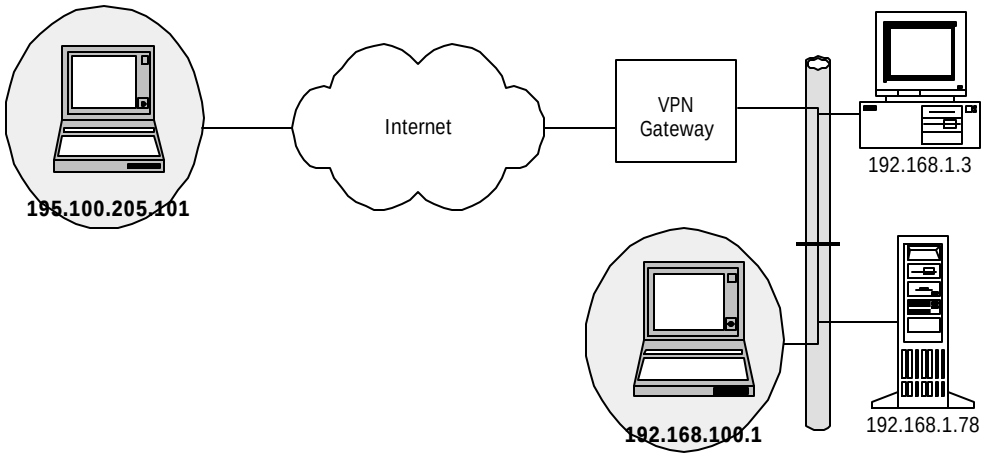


Figura 5.18
Contenido de la conexión

Para configurar esta conexión, se abre la ventana del asistente y se selecciona en menú "Configuration > Wizard"

Como primer paso puede configurar:

- El nombre de la conexión, en nuestro caso, FORTALEZA
- El DNS o la dirección IP para el túnel VPN. Para nuestro caso ozumba.ath.cx (Figura 5.19)

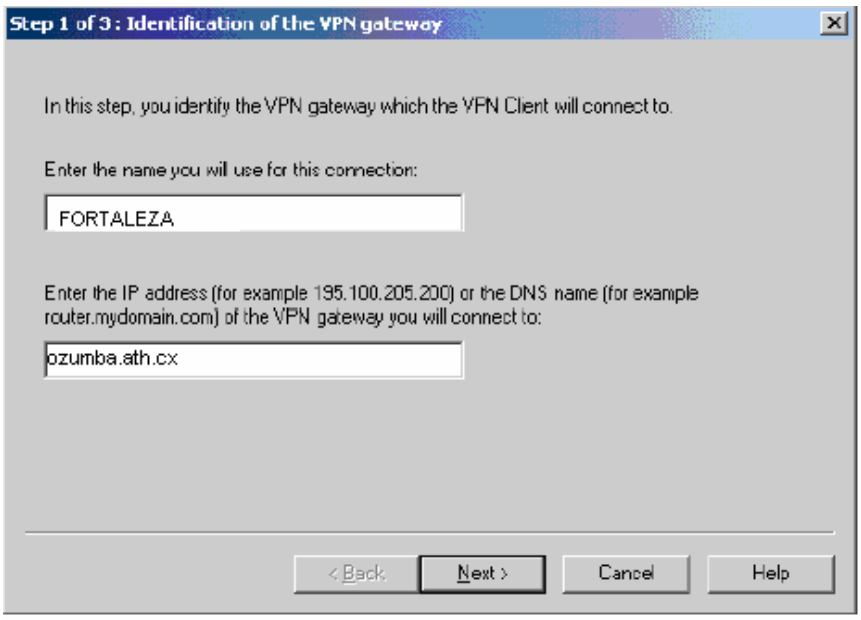


Figura 5.19
Configuración de dominio

Como Segundo paso puede escoger el método de autenticación el cual será usado entre el Cliente VPN Greenbow y el gateway (figura 5.20).

- La autenticación se basa en una llave predeterminada: la llave predeterminada debe ser dada en el archivo apropiado.

- La autenticación que se basa en el certificado X509: el usuario debe de importar los certificados y dar más información en "Advanced Window".

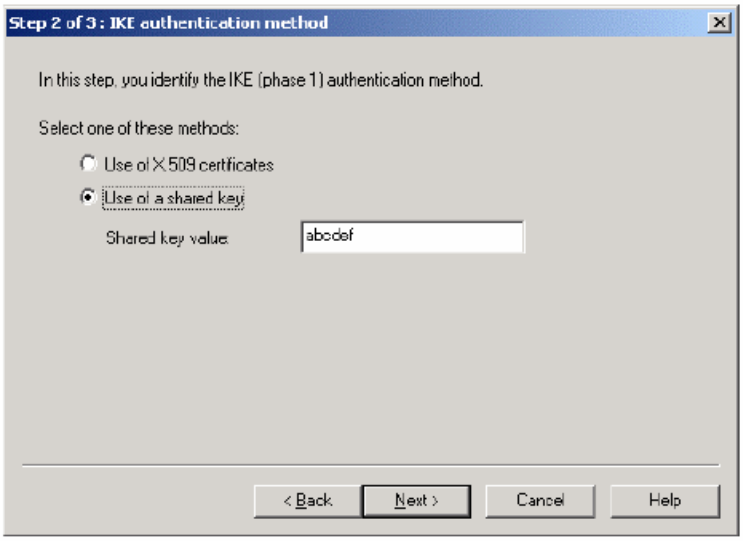


Figura 5.20
Método de autenticación

Como tercer paso, la dirección IP del cliente VPN en la LAN remota y la dirección de red de esta LAN (dirección IP de red y la mascara de subred) debe de ser en el mismo rango. Es importante que la dirección IP del cliente no sea mas larga que la de la LAN remota.

Si la dirección de la red remota es dada, toda computadora de la LAN puede creer que el cliente esta conectándose a su LAN. Tendrán que responder a un cuestionario ARP en el orden que las direcciones MAC son encontradas y tendrán que enviar las respuestas. Si el cliente no se conecta a la LAN, debe de enviar un paquete a través del gateway que será procesado y hecho con IPSec. Como ejemplo tenemos la figura 5.20

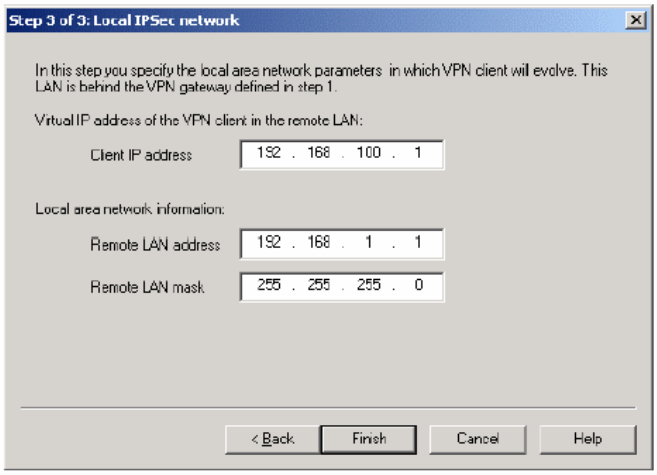


Figura 5.20
Red IPSec local

Después de terminado el tercer paso, la nueva configuración VPN será mostrada en el árbol de control de la ventana de main. Es posible cambiarla otra vez.

5.4.1.4 Configuración del Túnel (Ventana Main)

Para crear un túnel VPN a través de la ventana de Main (sin usar el asistente de configuración):

1. Clic derecho en “Configuration” en el árbol de control y seleccione “New Phase 1” (figura 5.21)

2. Configurar la autenticación fase (phase 1)

Figura 5.21
New Phase 1

3. Clic derecho en la nueva Phase 1 en el árbol de control y seleccionar "Add Phase 2" (figura 5.22)

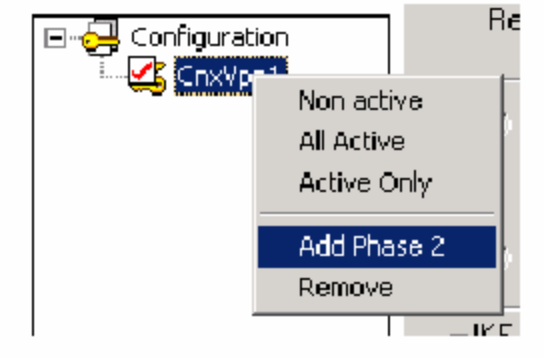


Figura 5.22
Add Phase 2

4. Configurar IPSec (Phase 2)

5. Clic en "Apply rules" para registrar la nueva configuración por el demonio IKE.

6. Hacer clic "Open Tunnel" para establecer el túnel VPN (solo en la ventana de "IPSec Configuration")

Nota: Las fases de autenticación severas puedan ser configuradas. Una computadora puede entonces establecer la conexión VPN con un túnel de fuerte autenticación.

De la misma forma una configuración severa de IPSec (fase 2) puede ser creada por la misma fase de autenticación (fase 1)

Fase Activa/no Activa

Una fase puede ser activa o no activa también. Si una fase esta no activa, los cambios no serán aplicados. Esta característica puede ser usada en una severa configuración compuesta de túneles VPN que no necesitan estar habilitados simultáneamente.

Para cambiar el estado activo o no activo de una fase puede ser salvado por un clic derecho en la fase:

- Activo (o no Activo) Habilitado o deshabilitado la fase
- Todas las fases activas
- Activo solo desactivo cada fase excepto el seleccionado por el mouse.

5.5 Cuestiones adicionales

Como lo planteamos a lo largo de este trabajo de este trabajo de tesis hay puntos muy importantes para considerar dentro de un esquema de implantación seguro de VPN. Por lo que se tuvieron que hacer los siguientes ajustes, que cerramos a políticas de seguridad al negocio para cuidar que la VPN sea seguro.

5.5.1 Políticas de seguridad para el negocio

- Las contraseñas deberían ser cambiadas cada 30 días.
- Nunca se deben apuntar las contraseñas.
- Se debe actualizar antivirus manualmente cada semana en cada máquina.
- Deben bloquear las estaciones de trabajo cuando se muevan de lugar
- Tenemos acceso al proveedor por medio de la VPN, pero nadie tiene acceso al interior de nuestra red.
- El acceso de Internet está restringido de la siguiente manera:
  - Mostrador y recepción de materiabs – SIN ACCESO
  - Oficina de contabilidad – Acceso sólo a las páginas de proveedores y bancos en los que manejan sus cuentas
  - Propietario - Sin restricción de acceso.

6 MANTENIMIENTO Y RECOMENDACIONES

6.1. Importancia del mantenimiento

Una VPN que no está funcionando cuando se necesita es peor que no tenerla. Una vez que uno empieza a depender de esa facilidad de conexión, si algo pasa y la deja inactiva nos daremos cuenta que parte de nuestra operación queda fuera.

Al igual que otro dispositivo de red las VPN necesitan mantenimiento pero, a diferencia de los otros dispositivos de red, éstas no deben considerarse como un solo dispositivo aislado. Aún si se está utilizando un dispositivo de hardware independiente, la VPN requiere mucho más mantenimiento que otros dispositivos. Mantener trabajando a una VPN involucra algo más que mantener los cables conectados. Cuando se instala una VPN, como hemos visto, se establecen túneles, se crean bases de datos de acceso para los usuarios y se instalan esquemas de cifrado y de administración de claves. Probablemente también se instalará un tipo de software de supervisión y alertas.

Un dispositivo VPN puede averiarse y desconectarlo de Internet, si ésta es su única manera de ir al exterior; no obstante, con los dispositivos de alta tecnología actuales se busca un tiempo promedio de reparación en cuestión de años y no de meses. Por lo tanto, sus

requisitos de la VPN caerán dentro de la infraestructura de soporte, la seguridad, la administración de claves y usuarios, etc.

Conforme crece una organización, el tráfico de Internet se incrementará más rápido de lo que la infraestructura de red física puede soportar. Cuando el tráfico de Internet empiece a crecer sin límite necesitarán manejar estas nuevas necesidades de conectividad en red. ¿Qué hay acerca del número de túneles que se pueden establecer en el presente y del número de licencias que están en vigencia actualmente? Mientras que pueden ser suficientes por ahora, pueden no serlo en el futuro. ¿Se puede actualizar fácilmente una licencia para permitir más usuarios y añadir más capacidad de túnel a sus dispositivos VPN? ¿Se puede añadir otro dispositivo en paralelo para manejar esta nueva carga? o ¿La empresa estará delimitada por el hardware existente y requerirá actualizar todo? Todo esto debe plantearse al momento de la compra o la elección de la solución de VPN y de este modo sepamos que tan complejo será el mantenimiento del sistema. Es importante que de estos puntos se considere la ampliación de licencias y la capacidad para soportar el crecimiento de la carga de la red, pues no será conveniente adquirir o seleccionar un sistema que en un corto plazo tenga que ser reemplazado o reforzado con otra solución.

Algunos de los puntos importantes que se deben tratar en el mantenimiento se listarán a continuación, son los que podemos considerar más importantes y deben realizarse siempre de manera oportuna, periódica y eficiente para asegurar que el sistema que se haya elegido siga siendo seguro y efectivo.

6.1.1 Supervisión

La supervisión es un elemento crítico del proceso de VPN general y puede causar dificultades en la implantación. Sólo cabe imaginar la cantidad de tráfico que va a pasar por este dispositivo. Al estudiar la ubicación se puede ver el flujo de tráfico que es probable se requiera supervisar. Se debe considerar qué tipo de tráfico se desea supervisar: ¿solo el tráfico VPN o todo el tráfico que fluye a través del dispositivo? Todos los dispositivos VPN que hemos visto ofrecen capacidades de supervisión, pero algunos ofrecen “el registro de todo el tráfico” y otros ofrecen “sin registro de tráfico”. Si se implementa una característica con la cual se puede supervisar sólo algunos tipos de tráfico, esto significa que el dispositivo tendrá que observar todo el tráfico y examinarlo, lo cual implica que todo el tráfico, incluyendo SMTP, DNS, HTTP y VPN, se supervisará y almacenará en alguna parte. Tal vez no se requiera una aplicación de procesos intensivos en el dispositivo VPN y, si existe un servidor al cual lo está enviando, el servidor necesitará espacio en disco.

6.1.2 Registro

Mientras que la emisión de alertas es importante para cualquier organización, el registro es la característica más importante que se puede instalar. Sólo hay que pensar: ¿cómo saber que uno de nuestros servidores está siendo penetrado por un intruso o si el servidor de correo está siendo utilizado para retransmitir el correo? La respuesta es simple, no lo sabemos, al menos no directamente. Si algo está saliendo mal (si no estamos llegando al exterior o no estamos obteniendo ningún correo) lo más conveniente es investigar. Si hacemos que las alertas sean demasiado sensibles, el administrador recibirá muchas de ellas, así que de inmediato las cerrará o minimizará la ventana en la que se presenten. Por lo tanto, los registros son los que se cuentan la historia: quién, qué, dónde, cuándo, pero no por qué (excepto en el correo basura cuando es bastante obvio). Con el registro se puede regresar y ver que ha sucedido, quién pude ver los horarios, por qué dirección IP entraron y qué servidor fue al que intentaron atacar. Aún si falsificaron su dirección IP, puede decir de cuál PSI viene y al menos el PSI puede intentar ayudarle. La intrusión a menudo puede rastrearse hacia un individuo sin experiencia.

6.1.3 Actualización de la seguridad

La seguridad indudablemente será el principal elemento de mantenimiento que se tenga que manejar con las VPN. No se debe simplemente colocar las medidas en su lugar y olvidarse de ellas; debe mantenerse actualizado sobre las últimas alertas de seguridad, los boletines de los proveedores, las acciones correctivas sugeridas y lo que está sucediendo en el mundo real. Algo bueno respecto de la seguridad y una gran cantidad de listas de correo. Cuando ocurre un evento de seguridad, se anuncia inmediatamente en los medios y en las listas de correo, para que las personas puedan estar concientes de ellos rápidamente. El problema puede residir en la aplicación más antigua que se esté ejecutando o en el hecho de no tener actualizados sus sistemas operativos, servidores web, etc., siempre debe mantenerse actualizado respecto a la seguridad debido a que ésta cambia constantemente.

La seguridad es como un sistema de tuberías agujeradas. Una vez que se tapa un agujero, otro se descubre.

6.1.4 Protocolos para establecimiento de túneles

Como ya se mencionó en capítulos anteriores, actualmente existen tres protocolos principales para establecimiento de túneles: IPSec, PPTP y L2TP. ¿Por cuál decidirse y cuándo usar cada uno?, ¿Se desea obtener una implementación que combine los distintos tipos

disponibles? ¿Qué nivel de soporte tendrán los productos de un proveedor para cada protocolo para el establecimiento de túneles? y, cuando se terminen las normas, ¿el equipo será actualizable? Los tres protocolos ofrecen seguridad para la organización; algunos ofrecen más seguridad que otros. En cualquier caso, es necesario asegurarse de que si se utiliza PPTP en los equipos de escritorio, el dispositivo VPN puede pasar el paquete, cifrarlo o encapsular un paquete de seguridad alrededor de él.

También es necesario asegurarse de que la política de cifrado permita distintos tipos de tecnología de cifrado. IPSec es un marco de referencia, PPTP es cifrado y no ofrece encapsulamiento, y 3DES ofrece autenticación y seguridad sólida. No todos estos protocolos y tecnologías interoperan, así que antes de elegir alguno asegúrese que sabe cuáles serán sus requisitos.

6.1.5 Dispositivos de administración

Es aconsejable contar con la capacidad de administrar la VPN desde una ubicación central. No obstante no todos los productos VPN soportan características de administración centralizada. Por ejemplo, podemos considerar la forma en que actualmente configuramos y enviamos una VPN a un edificio de oficinas distinto; es probable que incluya instrucciones sobre cómo instalarlo o que lo configure en forma manual y transporte el dispositivo a ubicaciones geográficamente distintas dentro de la organización.

Normalmente tenemos una o dos formas en las cuales podemos modificar y resolver los problemas de la VPN. Podemos crear un túnel a través de la red pública para configurarlo lo cual implica que el proveedor le ha dado la opción de instalar un túnel de administración con base en algún algoritmo de cifrado estándar. O debe ser capaz de conectar un módem al puerto de consola de ese dispositivo para administrarlo. En ese caso se ha abierto un problema de seguridad al añadir un módem en un dispositivo de seguridad por lo que será necesario considerar el tipo de módem a utilizar, un modelo estándar listo para configurarse o algún tipo de módem de seguridad que cifra los datos entre los módems. ¿Estos módems son seguros? ¿Se han probado? ¿Son confiables? ¿Qué otra opción tenemos? Si no podemos crear un túnel de administración su única otra opción es el módem.

6.1.6 Rendimiento

La organización debe definir *rendimiento*. Al igual que con un automóvil, ¿es el consumo de gasolina por cada kilómetro o la aceleración lo que definen el rendimiento? ¿Cómo se define el rendimiento, por el tiempo de inactividad, la latencia, la utilización, el número de túneles creados? En algunas estadísticas, el desempeño es el número de ciclos por segundo que la VPN

puede proporcionar; esto puede pensarse como el número de conexiones de túnel simultáneos, o la cantidad de procesamiento, medido por el número de usuarios por segundo. Para poder colocar una medida precisa en el rendimiento al menos se cuenta con una prueba de evaluación comparativa para juzgarlo. Probablemente se puede obtener estadísticas sobre el rendimiento de la VPN pero, ¿son comprensibles? ¿Cómo se relacionan con el número real de usuarios que pasa a través de la VPN, conducto, túnel, etc.? si se define, por ejemplo, que 100 usuarios pasan de forma simultánea dentro y fuera de la conexión a Internet, al menos puede utilizar eso como una prueba de evaluación comparativa.

6.1.7 Calidad de servicio

La calidad en el servicio se define por la latencia, el tiempo de inactividad de la red y el ancho de banda. Se pueden obtener garantías en el ancho de banda por parte del proveedor de Internet. Se requiere ancho de banda disponible para la VPN, es importante considerarlo dependiendo de las necesidades que tendrá la red.

6.2. Actualizaciones de VPN basadas en Software

Las actualizaciones de software pueden ser un proceso de múltiples pasos que probablemente necesiten soporte del fabricante.

Es bien sabido que todos los sistemas operativos, en alguna ocasión, presentan un problema con los aspectos de seguridad, pero simplemente es importante estar al tanto. El proveedor de la VPN probablemente será responsable de su propio software, pero no puede ser responsable del sistema operativo de la empresa.

Es necesario considerar todas las capas de software e imaginar todos los aspectos de seguridad y comunicación posibles que conciernen a cada una, asimismo será necesario considerar todos los puntos vulnerables que cada una de estas capas pudiera presentar. Como lo ilustra la figura 6.1, cada aplicación se encuentra encima de la anterior, por consiguiente, si se actualiza una aplicación debe pensarse en la que se encuentra inmediatamente arriba, ya que por ejemplo con un servidor típico, si existe incompatibilidad se puede dar marcha atrás de la actualización, llevar al sistema fuera de línea, etc.; pero con los servidores de seguridad, debe enterarse inmediatamente de esto, a menos que se desee darle a alguien una oportunidad para introducirse a la red.

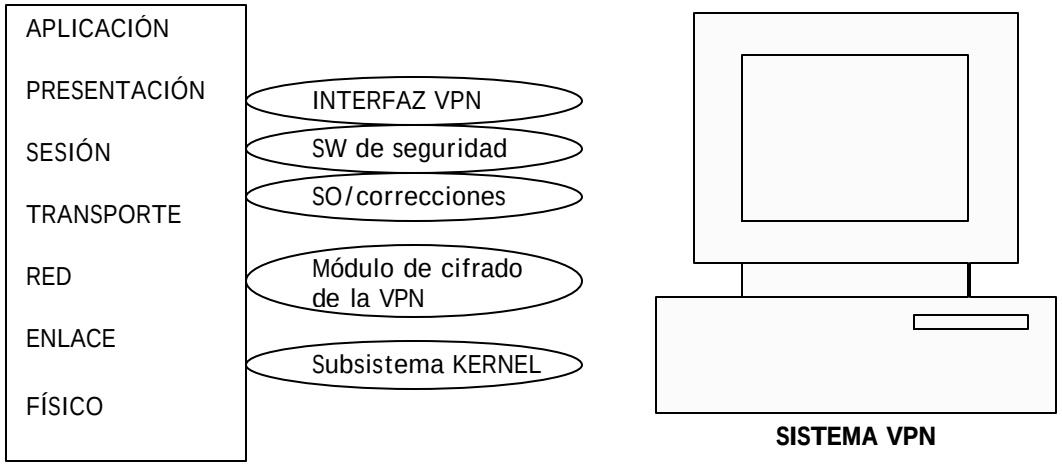


Figura 6.1
Preocupaciones del software de VPN en capas

La figura 6.1 ilustra claramente los problemas de interoperabilidad que podría enfrentar con una VPN de software al darle mantenimiento. Comenzando desde el nivel de aplicación hacia abajo, hasta el nivel de enlace de datos surgen muchos aspectos de interoperabilidad. Una razón por la cual las VPN de hardware tienen una ventaja es la carencia de niveles de software requeridos en estos dispositivos. Sin embargo, adolecen de flexibilidad y tienen sus propios puntos vulnerables.

Nota: aunque pueda parecer que los sistemas operativos tienen más puntos vulnerables que sus contrapartes de caja (o hardware), con los dispositivos VPN de sistema operativo los puntos vulnerables se encuentran rápidamente y la información se distribuye de la misma forma. Debido a que los sistemas operativos de proveedores de hardware son propietarios, es posible que no estén ansiosos de divulgar sus puntos vulnerables.

6.3. Actualizaciones de VPN basadas en Hardware

Al utilizar las VPN de caja negra se enfrentará a un arma de doble filo. Primero, el sistema operativo subyacente es propietario, lo cual significa que probablemente no será capaz de añadir ninguna característica a menos que el proveedor la soporte. Esto no implica que los proveedores no tratan de soportar las características principales que se requieren, si no que es posible que no estén soportados todos los requisitos que la empresa necesite, así que primero se deben establecer esos requisitos. También puede tener un conocimiento limitado acerca de la

seguridad del sistema, los puntos vulnerables, los agujeros, etc. Además, debe basarse en los fabricantes para obtener la información necesaria sobre seguridad de próxima aparición, y después realizar las actualizaciones y correcciones disponibles para ese sistema.

La otra cara de la moneda es que puesto que el sistema operativo es propietario del fabricante, puede ser muy seguro debido a la falta de interés por parte de los intrusos potenciales y a la falta de documentación disponibles al público. Existen miles de libros sobre los sistemas operativos Windows, y esto viene acompañado del conocimiento y de las ideas. La mayor parte de los proveedores también tratan de hacer que sus sistemas operativos sean tan reducidos como sea posible. Primero optimizan el sistema para la siguiente tarea específica, por lo general trabajando en la funcionalidad básica, y probablemente después lo hacen muy seguro. Sin embargo, cuando como cliente se comienzan a demandar más características para aquellos tipos de productos, pueden surgir los agujeros. Así que es una buena idea mantenerse al tanto de los problemas de seguridad general.

6.4. Buenas prácticas de seguridad

Las buenas prácticas recogen las experiencias de los profesionales en seguridad aplicadas en instituciones de cualquier tipo: gubernamentales, comerciales, universidades, etc. y se puede definir una buena práctica de seguridad como un método cuya efectividad ha sido probada y validada por la experiencia de la aplicación en una actividad relacionada con la seguridad.

La tabla 6.1 resume lo que es una buena práctica de seguridad, y lo que no es:

Es..	No es..
Una práctica humana, es decir un método usado repetidamente por la gente para ejecutar alguna acción.	No es un mecanismo de seguridad que se implementa por hardware, software o firmware, aún cuando dichas herramientas frecuentemente son componentes esenciales de una buena práctica de seguridad.
Relacionada con la seguridad, es decir, forma parte de la protección de la información, recursos u operaciones de la organización.	No es una práctica propia del negocio; más bien soporta la operación del negocio
Su efectividad para alcanzar un objetivo de seguridad ha sido probada, como resultado de la experiencia operativa	Tal vez no es la mejor práctica posible, per si es la mejor práctica existente; no teórica
Entre las más efectivas prácticas de seguridad para un proceso de seguridad específico.	No es necesariamente la única, ni la mejor práctica de su tipo

Tabla 6.1
Lo que si es y no es una buena práctica de seguridad

Las buenas prácticas no son disposiciones legales y no deben ser interpretadas como tales. Simplemente reflejan los tipos de medidas prudentes y efectivas que las instituciones han implementado, o están en proceso de implementar para proteger efectivamente la información y asegurarse de su disponibilidad, confidencialidad e integridad.
No se espera que todas las instituciones implementen todas estas prácticas, pues deben verse en el contexto de las necesidades de la organización y al respecto son solamente cuatro buenas prácticas las que deben verse como elementales:

- Desarrollo de una política de seguridad de información
- Clasificación de la información
- Cifrado de la información altamente confidencial
- Autenticación fuerte para controlar el acceso a sistemas críticos

Asegurando un ambiente Windows

Debería asegurarse de que han tratado los siguientes temas dentro de su empresa antes de hacer un plan para proteger un ambiente Windows. Recuerde, la seguridad no es en sí una solución técnica, sino más bien una combinación de medidas técnicas y procesos que se ajustan de forma única a su entorno.

Bloquee o desactive todo aquello que no esté explícitamente permitido

Con algunas oscuras excepciones, no se conocen formas de atacar remotamente un sistema sin servicios en ejecución. De esta forma, si se bloquean o desactivan los servicios completamente, no puede ser atacado.

Por supuesto, sirve de poco para aquellos servicios a los que les está permitido. Si necesita permitir el acceso a un servicio, se debe cerciorar de haberlo asegurado de acuerdo a las prácticas recomendadas (por ejemplo en grupos de Internet)

Utilice siempre una contraseña, hágala compleja y cámbiela a menudo

Las contraseñas amargan al mundo de la seguridad: constituyen la principal forma de autenticación para cada producto que existe. Las contraseñas débiles son la principal forma por la que se puede acceder sin autorización al sistema. Ponga siempre contraseñas, (¡jamás deben de dejarse en blanco!) y no debe ser fácil de adivinar.

Mantenerse al día con los parches del fabricante

Cuando se descubre algún bug en un producto, la prisa del fabricante por ganar fama y popularidad conducen normalmente a la publicación de un exploit en menos de 48 hrs. Esto significa que se dispone aproximadamente de dos días para aplicar parches antes de que alguien intente penetrar al sistema.

Autorizar los accesos utilizando el mínimo privilegio

Éste es el concepto que con menos frecuencia llegan a entender, pero del que más provecho se puede sacar de la red y mejores efectos. La autorización se realiza tras la autenticación para proteger los recursos sensibles de accesos de usuarios con bajos privilegios. Que se adivine una contraseña débil ya es suficientemente malo, pero las cosas empeoran cuando se descubre que la cuenta del usuario de menor categoría que se comprometió puede compartir un recurso que contiene información financiera muy delicada de la empresa. Sí, esto requiere de mucho trabajo para catalogar todos los recursos y asignar los controles de acceso apropiados en su entorno, esto es, en torno al administrador de la red, de sistemas o bien, al responsable de la seguridad de la información de la organización, más si no se hace, será tan resistente como el más débil de sus eslabones de autenticación, haciendo referencia nuevamente al usuario con una contraseña fácil.

No habilitar el uso compartido de archivos

Windows no entiende la seguridad que hay detrás de la seguridad de archivos. Cuando se inicia una sesión, generalmente se pide el nombre de usuario/contraseña. Esto es sólo un identificador para otras máquinas; no intenta proteger a su máquina. Lo que hace es decir a todos en la red, "hay alguien nuevo aquí, y esa persona puede leer o copiar cualquier archivo que ustedes tengan en la red". Los datos accesibles pueden incluir cualquier clave pública/privada que se emplee para cifrar. Si necesita que otros tengan acceso a su máquina, al menos asegúrese de que estén protegidos con contraseñas y restringidos sólo a los recursos necesarios.

Límite de confianza

Ningún sistema es una isla. Uno de los ataques más efectivos a un sistema operativo como Windows consiste en aprovecharse de un equipo de un miembro sin importancia de un dominio con una contraseña de administrador local. Entonces se extraen las credenciales para un usuario válido del dominio desde ese equipo, el cual permite establecerse en la estructura total del dominio y posiblemente en los dominios que confíen en este último. Reconozca que cada relación de confianza que se implanta, tanto si es una confianza de dominio formal de Windows o simplemente una contraseña almacenada en un archivo de lotes en un equipo remoto, amplía el perímetro de seguridad e incrementa los riesgos. Añadiendo algo a esta regla, puede decirse que la reutilización de contraseñas debería estar explícitamente prohibida.

Ser particularmente paranoico con las interfases externas y con la conexión de acceso telefónico

El número total de vulnerabilidades potenciales de una red puede parecer asombroso, pero se debe aprender a concentrarse en aquellas que representan un riesgo mayor. La mayor parte de ellos están relacionados con sistemas de red de cara al público, como servidores Web, etcétera. Los sistemas de este tipo deberían estar sujetos a un estándar de contabilidad más exhaustivo que un sistema interno, ya que los riesgos a los que se enfrentan son mayores.

En cuanto a la conexión de acceso telefónico, si nuestra red es completamente segura, pero alguien dentro de la empresa abre una comunicación de este tipo hace que dicha seguridad quede vulnerable.

La tecnología no protege ante ataques sociales

Esta no es una tesis acerca del arte de la detección de intrusos o del análisis forense, por lo que no se hablará a fondo sobre vigilancia, auditoría y el registro de actividad; pero lo que sí damos por hecho es que se ha aclarado a través de este trabajo la importancia de mantener un registro e implantarlo adecuadamente. No hay que olvidar revisar los registros que se han generado y se conservan; si no, no tiene sentido que se mantengan.

Hemos hablado sobre cómo evitar ser atacado. Pero ¿qué pasa si lo impensable sucede y la organización es atacada? Existen diversos procedimientos de emergencia que deberían seguirse inmediatamente después de un incidente de seguridad para minimizar el daño y esos procedimientos se deberían establecer por adelantado. No obstante, este trabajo tampoco es acerca de respuesta a incidentes y no se va a ahondar aquí en estos asuntos.

Este trabajo está orientado principalmente a ataques tecnológicos que pueden suscitarse en una VPN. Algunos de los ataques más dañinos que hemos visto y oído hacer no implican la tecnología en absoluto. La así llamada ingeniería social utiliza trucos y engaños de persona a persona para conseguir un acceso no autorizado a los datos. Este trabajo sólo puede proteger a nivel de red, bits y datos, no enseña a protegerse de ataques sociales. Es importante conocer las tácticas comunes empleadas por la ingeniería social e instruir y sensibilizar a los miembros de la organización a través de una política de seguridad.

Desarrollar una política de seguridad

Los libros clásicos sobre seguridad describen el desarrollo de una política como el primer paso en un programa integral de seguridad del sistema de información. Pero la mejor recomendación es que mantenga la actitud de tecnología exclusiva de su empresa y que desarrolle al menos una mínima política antes de adentrarse en las soluciones puntuales.

Es importante realizar análisis de riesgos realistas

Nunca se debe permitir que la paranoia haga estragos en los objetivos de negocio, se debe de considerar sólo aquellos riesgos que sean factibles en base al giro del mismo.

Plantillas de seguridad y configuración y análisis de seguridad

Las plantillas de seguridad y la configuración y análisis de seguridad se cuentan probablemente entre las mejores herramientas para ahorrar tiempo y que pueden usarse para desplegar la seguridad a lo largo de una infraestructura de Windows.

Las plantillas de seguridad son listas estructuradas de configuraciones de Windows relevantes para la seguridad que pueden editarse y aplicarse a un sistema con un clic al ratón, evitando la necesidad de identificar, localizar y configurar docenas de ajustes de seguridad individuales. Además, estos archivos de plantilla pueden compararse con la configuración actual de un sistema dado, mostrando las configuraciones que las cumplen o no.

La manera más fácil de acceder a las plantillas de seguridad y a la configuración y análisis de seguridad consisten en crear una consola de administración de Microsoft (MMC) en blanco y añadir los complementos de plantillas de seguridad y configuración y análisis de seguridad. En la tabla 6.2 se mencionan algunas de las plantillas de seguridad para el ambiente Windows.

Plantilla	Definición
setupsecurity	Configuraciones de seguridad predeterminadas de fábrica; aplicarla para deshacer configuraciones de seguridad más restrictivas aplicadas por otras plantillas por el motivo que sea.
compatws	Seguridad relajada desde la instalación limpia predeterminada de Windows 2000 Professional.
basicdc	Configuraciones de seguridad predeterminadas para un controlador de dominio.
basicsv	Configuraciones de seguridad predeterminadas para un servidor.
basicwk	Configuraciones de seguridad predeterminadas para Windows 2000 Professional.
securews	Mejora la seguridad de áreas adicionales sobre basicwk.
securedc	Mejora la seguridad de áreas adicionales sobre basicdc.
ocfilesw	Aplica configuración más segura a componentes instalados opcionalmente de Windows 2000 Professional (aplicar además desecurews o hisecws).
Ocsfiless	Aplica configuración más segura a componentes instalados opcionalmente de Windows 2000 Server (apliquese además de securedc o hisecdc)
Hisecdc	Windows 2000 más seguro: mejoras sólo más allá de securedc.
hisecws	Windows 2000 más seguro: mejoras sólo más allá de securedc.

Tabla 6.2
Plantillas de seguridad para Windows2000

Computadoras personales

Protegerse contra la pérdida o modificación de procesos e información residente en computadoras personales. Debido a la susceptibilidad de las mismas ante el robo o acceso de personal no autorizado, destrucción o falla, se hace necesario transferir el almacenamiento de datos críticos o confidenciales de la computadora personal a servidores ubicados en áreas aseguradas. En el caso de que sea indispensable que dicha información resida en la computadora personal, se deberán utilizar controles de acceso, cifrado y procedimientos de respaldos periódicos.

Virus

La mejor defensa en contra de los virus es una combinación de prácticas de administración y el uso del software de antivirus en todos los servidores, estaciones de trabajo y computadoras portátiles.

- Entrenar a todos los usuarios para que revisen todos los medios de almacenamiento removibles, incluyendo los discos nuevos y archivos bajados de la red, antes de usarlos por primera vez. Prohibir a los usuarios la instalación de su propio software en sistemas que soporten recursos críticos de información. Aun el software comercial "recién desempacado" puede contener virus.

- Se deben revisar los sitios en Internet especializados en virus, así como los sitios del vendedor del software antivirus, ello con el propósito de mantenerse informado de nuevos virus u otro tipo de programas maliciosos que puedan surgir. Se debe enviar una alerta a todos los usuarios si se descubre un virus particularmente contagioso y maligno, y tomar las medidas preventivas en los puntos de entrada críticos, tales como servidores de correo electrónico, proxys, o firewalls.

- Desarrollar y utilizar rutinas consistentes para respaldar la información de sistemas críticos, usando tecnología confiable para respaldos y medios de almacenamiento limpios. Los respaldos se deben probar con frecuencia para asegurarse que la información está siendo almacenada adecuadamente y que los archivos pueden recuperarse en caso de ser necesario. Se debe mantener una copia de los respaldos almacenada en un lugar fuera de la empresa o sitio principal, que sea físicamente seguro.

- Mantener actualizado el software de antivirus, usando los parches y actualizaciones proporcionados por el proveedor.

- Preparar un plan de acción para actuar en caso de presentarse una infección.

CONCLUSIONES

La idea de este trabajo de tesis en sus inicios fue una idea novedosa pero debido al rápido avance de la tecnología de información actualmente podemos encontrar cada día más soluciones económicas para las Redes Virtuales. El valor agregado de este trabajo es que ninguna solución será segura si no se toma en cuenta todo el análisis de requerimientos, el mantenimiento y consejos de seguridad que en él se incluyen.

Se implantó este trabajo en unas sucursales Construrama para probar todo aquello que nos enseña la teoría y durante la instalación nos encontramos con varios detalles que tal vez no tomamos en cuenta anteriormente y son un poco más técnicos.

El principal de los problemas con el que nos topamos fue el enlace a Internet pues tratándose de sucursales que se encuentran fuera de la zona metropolitana la calidad era muy mala a pesar de tratarse de un enlace infinitum y no un simple dial up. Esto nos causó problemas para levantar el túnel debido a la intermitencia de la red ya que no lográbamos sincronizar las solicitudes de enlace. También nos encontramos con el problema de que manejaban un software que no corre bajo TCP/IP por lo que no podíamos transmitir la base de datos por el túnel. La solución a este segundo inconveniente fue apoyarnos de un software para poder acceder remotamente a los distintos servidores de las sucursales. Esto obviamente conlleva a un costo mayor al que se había planteado pues al tratarse de software comercial hay que pagar por la licencia.

En general también observamos que a pesar de que actualmente las redes virtuales son algo que se ocupa diariamente si se va a levantar toda la red, es decir no se conecta a un servidor VPN existente, crear todo de cero es una tarea que sí requiere cierto conocimiento de sistemas de cómputo. Durante el desarrollo de este trabajo de tesis pudimos percatarnos que no es algo inmediato ni algo tan sencillo de comprender como se pensaba en un principio. Por esta razón intentamos hacer digerible este trabajo de tesis, estamos seguras que se requerirá de dicho conocimiento del área, y permitirá a quien lo lea comprenda un poco más de la tecnología que tratamos; que dejará ver que alcances tiene actualmente y en un futuro cercano, así como sus ventajas, desventajas y la forma de lograr un adecuado uso de la misma.

A final de cuentas y regresando a los resultados esperados de este trabajo, se logró conseguir el ahorro económico ya que contaban con una sola computadora conectada a Internet, la cual se conectó a la red y por medio del ruteador se compartió el Internet para todas, dejando sólo los accesos necesarios a cada una de las máquinas optimizando también los recursos que era otro de los puntos que se pretendían alcanzar. Lo que no logramos cumplir al cliente fue con la transparencia debido a que por los problemas del enlace de Internet si se refleja en la transferencia de información los cambios de velocidad o intermitencias.

Tuvimos también la oportunidad de efectuar la instalación en las sucursales y con ello manejar un proyecto real de una pequeña empresa y darnos cuenta de la importancia y la gran oportunidad que se tiene al trabajar con ellas y apoyarlas en su desarrollo mientras que también obtenemos un beneficio.

Creemos que es importante seguir trabajando con este sector económico pues también están siendo apoyados por distintas entidades gubernamentales y particulares para su crecimiento; y es mediante la explotación de los recursos tecnológicos que pueden lograr el mayor crecimiento aprovechando al máximo sus recursos.

GLOSARIO

A

ATM (Asynchronus Transfer Mode): ATM es una tecnología de conmutación y multiplexado de alta velocidad, usada para trasmitir diferentes tipos de tráfico simultáneamente, incluyendo voz, video y datos.

Acceso directo: icono que permite abrir más fácilmente un determinado programa o archivo.

Adjunto: Se llama así a un archivo de datos (por ejemplo una planilla de cálculo o una carta de procesador de textos) enviado junto a un mensaje de correo electrónico.

Agente (agent): Pequeño programa "inteligente" creado para efectuar ciertas tareas, facilitando la operatoria del usuario. Un ejemplo muy conocido de agente son los Asistentes (wizards) que existen en la mayoría de los softwares modernos.

ADSL: Asymmetric Digital Subscriber Line. Tecnología para transmitir información digital a elevados anchos de banda. A diferencia del servicio dial up, ADSL provee una conexión permanente y de gran velocidad. Esta tecnología utiliza la mayor parte del canal para enviar información al usuario, y sólo una pequeña parte para recibir información del usuario.

Algoritmo: conjunto de reglas bien definidas para la resolución de un problema. Un programa de software es la trascripción, en lenguaje de programación, de un algoritmo.

Algoritmo de Encriptación o Cifrado: Sistema de encriptación (con mayor grado de sofisticación cada día) que permite mover información por las redes con seguridad. Existen varios algoritmos, a dual más complejo y eficaz.

Ancho de banda (bandwidth): Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso y mayor tráfico.

ANSI (American National Standards Institute, Instituto Americano de Normas): Organización que desarrolla y aprueba normas de los Estados Unidos. Participó en la creación de gran parte de las normas en uso actualmente en Internet.

Antivirus: programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco duro o disquete.

ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones): Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

ASCII (American Standard Code for Information Interchange, Código americano Normado para el Intercambio de Información): Conjunto de caracteres, letras y símbolos utilizados en todos los sistemas de computadoras de cualquier país e idioma. Permite una base común de comunicación. Incluye a las letras normales de alfabeto español, con excepción de la ñ y toda letra acentuada.

Autoridad Certificante (Certificanting Authority): Empresa en Internet que cumple el rol de "escribano virtual". Se encarga de garantizar la identidad de las personas físicas y las empresas que participan en la Red, a través de la emisión de los llamados Certificados.

B

Backup: copia de seguridad. Se hace para prevenir una posible pérdida de información.

Base de datos: conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Backbone (columna vertebral): Conexión de alta velocidad que conecta a computadoras encargadas de circular grandes volúmenes de información. Los backbones conectan ciudades, o países, y constituyen la estructura fundamental de las redes de comunicación. Usado para interconectar redes entre sí utilizando diferentes tipos de tecnologías.

Backdoor (puerta trasera): Sección oculta de un programa de computadora, que sólo se pone en funcionamiento si se dan condiciones o circunstancias muy particulares en el programa.

Banda ancha: Característica de cualquier red que permite la conexión de varias redes en un único cable. Para evitar las interferencias en la información manejada en cada red, se utilizan

diferentes frecuencias para cada una de ellas. La banda ancha hace referencia también a una gran velocidad de transmisión.

Bit: abreviatura de binary digit (dígito binario). El bit es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora.

Bps: bits por segundo.

Bridge: Dispositivo usado para conectar dos redes y hacer que las mismas funcionen como si fueran una. Típicamente se utilizan para dividir una red en redes más pequeñas, para incrementar el rendimiento.

Browser/Web browser (navegador o visualizador): Programa que permite leer documentos en la Web y seguir enlaces (links) de documento en documento de Hipertexto. Los navegadores "piden" archivos (páginas y otros) a los servers de Web según la elección del usuario y luego muestran en el monitor el resultado.

Bus: enlace común; conductor común; vía de interconexión. Método de interconexión de dispositivos mediante una sola línea compartida. En una topología de Bus cada nodo se conecta a un cable común. No se requiere un hub en una red con topología de bus.

Byte: unidad de información utilizada por las computadoras. Cada byte está compuesto por ocho bits.

C

Caché: en un navegador, el caché guarda copias de documentos de acceso frecuente, para que en el futuro aparezcan más rápidamente.

Caracter: número, letra o símbolo en la computadora, conformado por un byte.

Certificado: consiste en una pareja clave privada-clave pública. Físicamente son dos archivos que nidos permiten definir un conjunto de claves de encriptación y una identidad certificada. La clave privada nunca abandona el servidor, por lo que nadie obtiene esta información, por lo que nadie podrá suplantar la identidad del servidor certificado.

Chip: abreviatura de "microchip". Circuito muy pequeño, compuesto por miles a millones de transistores impresos sobre una oblea de silicio.

Clave privada: Es la clave que tan sólo nosotros conocemos y que utilizamos para desencriptar el mensaje que nos envían encriptado con nuestra clave pública. Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

Cluster: grupo; racimo; agrupamiento. En la tecnología de las computadoras, un cluster es la unidad de almacenamiento en el disco duro. Un archivo está compuesto por varios clusters, que pueden estar almacenados en diversos lugares del disco.

Comando (command): instrucción que un usuario da al sistema operativo de la computadora para realizar determinada tarea.

Cookie: pequeño archivo de texto que un sitio web coloca en el disco duro de una computadora que lo visita. Al mismo tiempo, recoge información sobre el usuario. Agiliza la navegación en el sitio. Su uso es controvertido, porque pone en riesgo la privacidad de los usuarios.

CPU: Central Processing Unit. Unidad central de procesamiento. Es el procesador que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

D

Data: datos, información.

Directorio (directory): grupo de archivos relacionados entre sí que se guardan bajo un nombre.

Disco duro: soporte giratorio de almacenamiento en forma de placa circular revestida por una película magnética. Los datos se graban en pistas concéntricas en la película.

DSL (Línea Digital de Suscripción): Tecnología que permite enviar mucha información a gran velocidad a través de líneas telefónicas.

E

Ethernet: Ethernet fue desarrollado en PARC con la participación de Robert Metcalfe fundador de 3Com, es un set de estándares para infraestructura de red. Además de definir los medios físicos y las conexiones Ethernet define como se trasmiten los datos.

Encriptar: proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

Extranet: parte de una intranet de acceso disponible a clientes y otros usuarios ajenos a la compañía.

F

Fast Ethernet: Un nuevo estándar de Ethernet que provee velocidad de 100 Megabits por segundo (a diferencia de los 10 megabits por segundo de las redes Ethernet).

FDDI (Fiber Distributed Data Interface): Interfaz de datos distribuidos por fibra óptica. Se trata de una red de 100 Megabits por segundo en topología en estrella o anillo muy utilizada en backbones, hoy desplazada por nuevas tecnologías como ATM.

Firewall: Una computadora que corre un software especial utilizado para prevenir el acceso de usuarios no autorizados a la red. Todo el tráfico de la red debe pasar primero a través de la computadora del firewall.

Fibra óptica: tecnología para transmitir información como pulsos luminosos a través de un conducto de fibra de vidrio. La fibra óptica transporta mucha más información que el Cable de cobre convencional. La mayoría de las líneas de larga distancia de las compañías telefónicas utilizan la fibra óptica.

FTP (File Transfer Protocol): protocolo de Transferencia de Archivos. Sirve para enviar y recibir archivos de Internet.

G

Gateway: Dispositivo utilizado para conectar diferentes tipos de ambientes operativos. Tipicamente se usan para conectar redes LAN a minicomputadores o mainframes.

Giga: prefijo que indica un múltiplo de 1.000 millones, o sea 109. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 230, o sea 1.073.741.824.

Gusano: programa que se copia a sí mismo hasta ocupar toda la memoria. Es un virus que suele llegar a través del correo electrónico, en forma de archivo adjunto.

H

Hub: Concentrador. Dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la red.

Hardware: todos los componentes físicos de la computadora y sus periféricos.

Hosting: alojamiento. Servicio ofrecido por algunos proveedores, que brindan a sus clientes (individuos o empresas) un espacio en su servidor para alojar un sitio web.

HTML: Hyper Text Mark-up Language. Lenguaje de programación para armar páginas web.

HTTP: Hypertext Transfer Protocol. Protocolo de transferencia de hipertextos. Es un protocolo que permite transferir información en archivos de texto, gráficos, de video, de audio y otros recursos multimedia.

I

Internet: Internet se define generalmente como la red de redes mundial. Las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado, TCP/IP (Transmission Control Protocol/ Internet Protocol). Fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA. Se la llamó primero Arpanet y fue pensada para cumplir funciones de investigación. Su uso se popularizó a partir de la creación de la WWW. Actualmente es un espacio público utilizado por millones de personas en todo el mundo como herramienta de comunicación e información.

Intranet: Las Intranets son redes corporativas que utilizan los protocolos y herramientas de Internet. Su aspecto es similar al de las páginas de Internet. Si esta red se encuentra a su vez conectada a Internet, generalmente se la protege mediante firewalls.

IEEE: Institute of Electrical and Electronics Engineers: importante asociación de técnicos y profesionales, con sede en los Estados Unidos. Fue fundada en 1884 y en 1998 tenía aproximadamente 320.000 miembros en 147 países. Favorece la investigación en campos diversos, como la tecnología aeroespacial, la computación, las comunicaciones y la tecnología biomédica. Promueve la estandarización de normas.

Inteligencia artificial: simulación de los procesos de la inteligencia humana, por medio de sistemas de computación.

Interfase: Elemento de transición o conexión que facilita el intercambio de datos. El teclado, por ejemplo, es una interfase entre el usuario y la computadora.

IP: Protocolo de Internet.

ISDN: Integrated Services Digital Network: Integrated Services Digital Network: sistema para transmisión telefónica digital. Con una línea ISDN y un adaptador ISDN es posible navegar por la Web a una velocidad de 128 kbps, siempre que el ISP también tenga ISDN.

ISO: International Organization for Standardization. Fundada en 1946, es una federación internacional que unifica normas en unos cien países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de comunicación.
ISP: Proveedor de servicios de Internet.

K

keyword: palabra clave para cualquier búsqueda.

kilobit: 1.024 bits.

kilobyte (KB): unidad de medida de una memoria. l kilobyte = 1024 bytes.

L

LAN: Local Area Network o red de área local: Se trata de una red de comunicación de datos geográficamente limitada, por ejemplo, una empresa.

LAN Manager: sistema operativo de red.

Laptop: computadora portátil del tamaño aproximado de un portafolio.

Latencia: lapso necesario para que un paquete de información viaje desde la fuente hasta su destino. La latencia y el ancho de banda, juntos, definen la capacidad y la velocidad de una red.

Link: enlace. Imagen o texto destacado, mediante subrayado o color, que lleva a otro sector del documento o a otra página web.

M

Megabit: Aproximadamente 1 millón de bits. (1.048.576 bits).

Megabyte (MB): unidad de medida de memoria. 1 megabyte = 1024 kilobytes = 1.048.576 bytes.

Microprocesador (microprocessor): es el chip más importante de una computadora. Su velocidad se mide en MHz.

Módem: modulador-demodulador. Dispositivo periférico que conecta la computadora a la línea telefónica.

Motherboard: Placa que contiene los circuitos impresos básicos de la computadora, el CPU, la memoria RAM y slots en los que se puede insertar otras placas (de red, de audio, etc.).

N

Network: (red) Una red de computadoras es un sistema de comunicación de datos que conecta entre si sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Nodo: Un dispositivo de la red, generalmente una computadora o una impresora.

Navegador: programa para recorrer la World Wide Web. Algunos de los más conocidos son Netscape Navigator, Microsoft Explorer.

Norma CDMA: Code didivison Multiple Access: Acceso Múltiple de División de Código. Norma de transmisión de datos a través de teléfonos inalámbricos.

Norma TDMA: Time division Multiple Access: Acceso Múltiple de División de Tiempo. Norma de transmisión de datos a través de teléfonos inalámbricos.

O

OSI (Interconexión de Sistemas Abiertos): Norma universal para protocolos de comunicación.

P

Par trenzado: Cable similar a los pares telefónicos estándar, que consiste en dos cables aislados "trenzados" entre sí y encapsulados en plástico. Los pares aislados vienen en dos formas: cubiertos y descubiertos.

Protocolo: Un conjunto de reglas formales que describen como se trasmiten los datos, especialmente a través de la red.

Página web: una de las páginas que componen un sitio de la WWW. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".

Paquete (packet): la parte de un mensaje que se transmite por una red. Antes de ser enviada a través de Internet, la información se divide en paquetes.

Password: contraseña.

Periférico: todo dispositivo que se conecta a la computadora. Por ejemplo: teclado, monitor, mouse, impresora, escaner, etcétera.

Portal: sitio web que sirve de punto de partida para navegar por Internet. Los portales ofrecen una gran diversidad de servicios: listado de sitios web, noticias, e-mail, información meteorológica, chat, newgroups (grupos de discusión) y comercio electrónico. En muchos casos el usuario puede personalizar la presentación del portal. Algunos de los más conocidos son Altavista, Yahoo!, Netscape y Microsoft.

Procesador (processor): conjunto de circuitos lógicos que procesa las instrucciones básicas de una computadora.

Protocolo: lenguaje que utilizan dos computadoras para comunicarse entre sí.

Proveedor de servicios de Internet: compañía que ofrece una conexión a Internet, e-mails y otros servicios relacionados, tales como la construcción y el hosting de páginas web.

Puerto paralelo: conexión por medio de la cual se envían datos a través de varios conductos. Una computadora suele tener un puerto paralelo llamado LPT1.

Puerto serial: conexión por medio de la cual se envían datos a través de un solo conducto. Por ejemplo, el mouse se conecta a un puerto serial. Las computadoras tienen dos puertos seriales: COM1 y COM2.

Puerto: en una computadora, es el lugar específico de conexión con otro dispositivo, generalmente mediante un enchufe. Puede tratarse de un puerto serial o de un puerto paralelo.

R

Repetidor: Un dispositivo que intensifica las señales de la red. Los repetidores se usan cuando el largo total de los cables de la red es mas largo que el máximo permitido por el tipo de cable. No en todos los casos se pueden utilizar.

Router – Ruteador: Dispositivo que dirige el tráfico entre redes y que es capaz de determinar los caminos mas eficientes, asegurando un alto rendimiento.

RAM: Random Acces Memory: Memoria de acceso aleatorio. Memoria donde la computadora almacena datos que le permiten al procesador acceder rápidamente al sistema operativo, las aplicaciones y los datos en uso. Tiene estrecha relación con la velocidad de la computadora. Se mide en megabytes.

Red: en tecnología de la información, una red es un conjunto de dos o más computadoras interconectadas.

ROM: Read Only Memory: Memoria de sólo lectura. Memoria incorporada que contiene datos que no pueden ser modificados. Permite a la computadora arrancar. A diferencia de la RAM, los datos de la memoria ROM no se pierden al *-apagar el equipo.

Router: ruteador. Sistema constituido por hardware y software para la transmisión de datos en Internet. El emisor y el receptor deben utilizar el mismo protocolo.

S

Server: Ver Servidor.

Switch: Un dispositivo de red capaz de realizar una serie de tareas de administración, incluyendo el redireccionamiento de los datos.

Serial: método para transmitir datos secuencialmente, es decir, bit por bit.

Servidor: computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas. Sistema que proporciona recursos (por ejemplo, servidores de archivos, servidores de nombres). En Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

Sistema operativo: programa que administra los demás programas en una computadora.

SMTP: Simple Mail Transfer Protocol. Es un protocolo estándar para enviar e-mail.

Software: término general que designa los diversos tipos de programas usados en computación.

Spam: correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a Internet.

Socket: (soporte) conector eléctrico, toma de corriente, enchufe. Un socket es el punto final de una conexión. Método de comunicación entre un programa cliente y un programa servidor en una red.

SSL: Secure Sockets Layer. Protocolo diseñado por la empresa Netscape para proveer comunicaciones encriptadas en Internet.

T

Token ring (red en anillo): Una red en anillo es un tipo de LAN con nodos cableados en anillo. Cada nodo pasa constantemente un mensaje de control ("token") al siguiente, de tal forma que cualquier nodo que tiene un "token" puede enviar un mensaje.

Topología: La "forma" de la red. Predominan tres tipos de tecnologías: Bus, Estrella y Anillo.

TCP/IP: Transfer Control Protocol / Internet Protocol. Es el protocolo que se utiliza en Internet.

Troyano (caballo de Troya): programa que contiene un código dañino dentro de datos aparentemente inofensivos. Puede arruinar parte del rígido.

Tarjeta Ethernet: placa que se inserta en una computadora para conectarla en red con otras a través de un cable.

Topología Estrella: En las topologías Star Ring o estrella, los nodos radian desde un hub. El hub o concentrador es diferente dependiendo de la tecnología utilizada Ethernet, FDDI, etc. La mayor ventaja de esta topología es que si un nodo falla, la red continúa funcionando.

U

Unix: sistema operativo multiusuario, fue muy importante en el desarrollo de Internet.

USB (Universal Serial Bus): es una interfase de tipo plug & play entre una computadora y ciertos dispositivos, por ejemplo, teclados, teléfonos, escáner e impresoras.

V

Virus: pequeño programa que "infecta" una computadora; puede causar efectos indeseables y hasta daños irreparables.

W

WAN- Wide Area Network: Red de área amplia: Una red generalmente construida con líneas en serie que se extiende a distancias mayores a un kilómetro.

Windows 2000: Versión del sistema operativo Windows, cuyo lanzamiento ha sido anunciado por Microsoft para el año 1999.

Windows NT Server: Windwos NT diseñado para máquinas que proveen servicios a computadoras conectadas a una LAN.

Workstation: estación de trabajo. Computadora personal conectada a una LAN. Puede ser usada independientemente de la mainframe, dado que tiene sus propias aplicaciones y su propio disco rígido.

World Wide Web: Es la parte multimedia de Internet, que implica la inserción de hipertexto y gráficos. Es decir, los recursos creados en HTML y sus derivados. Es el sistema de información global desarrollado en 1990 por Robert Cailliau y Tim Berners-Lee en el CERN (Consejo Europeo para la Investigación Nuclear) que fue la base para la explosiva popularización de Internet a partir de 1993.

Z

Zip: formato de compresión de archivos.

BIBLIOGRAFIA

Autor Randall Jorde Covill
Titulo Implementing extranets: the Internet as a virtual private network
Impr. Boston : Digital Press, c1998

Autor Peter Tomsu and Gerhard Wieser
Titulo MPLS-based VPNs: designing advanced virtual networks
Impr. Upper Saddle River, New Jersey : Prentice Hall, c2002

Autor Brown, Steven
Titulo Implementing virtual private networks
Impr. New York : McGraw-Hill, 1999

Autor Fowler, Dennis
Titulo Virtual private networks : making the right connection
Impr. San Francisco, Calif. : M. Kaufmann, c1999

Autor Norris, Mark, Steve Pretty
Titulo Designing the total area network : Intranets, VPN's andenterprise networks explained
Impr. Chichester, England : J. Wiley, c2000

Autor Peter J. Denning
Titulo Computers Ander Attack, Intruders, Works ans Viruses
Impr. Adison Wesley, c1991

Autor Amparo Fúster Sabater, Dolores de la Guía Mtz, Et Al
Titulo Técnicas Criptográficas de Protección de datos
Impr. Alfaomega, México, c2000

Autor R&D Book
Titulo Unix Security
Impr. Millar Freeman, 1997

Autor Richard Grigonis
Titulo Disaster Survival Guide for Bussiness Comunications Networks.
Impr. CMP Bookds, USA c2002

Autor William Stallingas
Titulo Network Security Essentials
Impr. Prentice Hall, USA, c2000

Autor P. Gómez, P. Bichon
Titulo Las redes de Empresa
Impr. Ediciones 2000, Barcelona, c1994

Autor Thomas A. Wadlow
Titulo The process of Network Security
Impr. Addison Wesley, USA, 2000

Autor Patrick H. Corrigam
Titulo LAN Disaster Prevention and Recovery
Impr. Prentice Hall, USA, 1994

Autor Eugene Schutz, Russell Shumway
Titulo Incident Response
Impr. New Riders, USA

Autor Eric A. Fish, Gregory B. White
Titulo Secure Computers and Networks, Análisis, design and Implementation
Impr. CRC Press, USA, 2000

Autor Stuart Mc. Clure, Joel Scambray
Titulo Hackers en Windows 2000
Impr. Mc. Graw Hill 2002

Autor Frederic J. Cooper, Chris Goggans, et al
Titulo Implementing Internet Security
Impr. New Riders publishiung, USA, 1995

Autor Paul Ashley, Mark Vandenwauver
Titulo Practical Intranet Security Overview of the state of art an Avaible Technologies
Impr. Klumber Academic Publishers

http://www.unam-cert.unam.mx