CAPÍTULO 3
Mecanismos de seguridad en red

La seguridad es un aspecto primordial que no sólo se considera en el ámbito del cómputo, actualmente las organizaciones y sus sistemas de información se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes, medios tecnológicos, humanos y físicos.

3.1. Planeación de la seguridad en red

La implementación de seguridad en cómputo no sólo requiere recursos tecnológicos, se deben considerar procesos de entrenamiento y recursos humanos especializados, esta meta es difícil de alcanzar debido a los constantes cambios. Con el paso de los años se han desarrollado nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP, en la configuración, operación de los equipos y sistemas que conforman las redes conectadas a internet. Estos nuevos métodos de ataque se han automatizado, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

Las organizaciones deben contemplar la planeación de la seguridad, revisar sus prácticas, aprender del entorno y desarrollar planes para mejorarlas, todo esto tiene una base en común, la administración de sus sistemas, dentro de la cual se debe contar con un responsable de la administración y sistemas de seguridad, así también con un inventario de todos los equipos físicos como computadoras, impresoras de red, servidores, máquinas portables, guías de configuración y conexión a Internet, en lugares estratégicos, el seguimiento de estos puntos debe ser considerado para planear la seguridad.

Es importante tener en cuenta que para implementar un esquema de seguridad antes se debe contar con una administración bien definida, el siguiente paso de la administración es la planeación de un esquema de seguridad el cual es determinado con base en un análisis del sistema actual, los recursos económicos, las necesidades de la organización y la aprobación de la gerencia. Realizando un análisis de riesgos posterior contemplando la arquitectura de la red, políticas de seguridad actuales, mecanismos de detección de intrusos, robos, desastres naturales, concientización de usuarios, seguridad interna, confidencialidad, seguridad en redes inalámbricas y mantenimiento principalmente, dentro de este punto se debe contemplar tanto la seguridad física como la lógica para asegurar la red y cada host, generando lo que actualmente se conoce como seguridad convergente.

Algunos puntos básicos que se hacen al momento de realizar una planeación de la seguridad son:

- ¿Qué bien se protegerá?.
- ¡Qué valor cualitativo o cuantitativo representa el bien para la organización?.
- ¿Cuál es el impacto en la organización si se compromete este bien?.
- ¿De qué se busca proteger el bien?.
- ¿Qué mecanismos se pueden implementar para asegurar el bien?.
- ¿Cuánto es el monto destinado para la protección de este bien?.
- ¿Apegarse a la decisión ejecutiva de la organización?.

La planificación de la seguridad puede apoyarse en estándares y buenas prácticas, los cuales no sólo son recomendaciones personales, sino modelos a seguir por agencias gubernamentales, como el NIST (National Institute of Standards and Technology – Instituto Nacional de Estándares y

Tecnología), organizaciones mundiales como ISO (International Organization for Standardization – Organización Internacional de Estándares) e IETF (Internet Engineering Task Force – Destacamento de Ingeniería en Internet), entre otras, aunque en algunos casos bastará con definir una metodología a seguir con la finalidad de cumplir con las metas que se planteen en la organización, todo depende del alcance que se desee conseguir.

3.2 Estrategias de seguridad

Implementar una solución de seguridad por más simple que sea, requiere de una planeación, las tecnologías por sí solas no aseguran la red, invertir en equipo no necesariamente garantiza la seguridad de la red , el problema es entender que todas las tecnologías son una inconsistencia si no se consideran las aplicaciones, el método de almacenamiento, los hosts, tránsito de la información, el perímetro, configuraciones y lo más importante, las personas, ya que no se puede confiar sólo en la tecnología para proteger la red, debido a que las personas que generan las tecnologías cometen errores también, no se puede esperar que la tecnología por si sola proteja contra el crimen cibernético.

Una solución global es definir esquemas de seguridad, un esquema de seguridad contempla la seguridad física, lógica y de procedimientos, es importante mencionar que el esquema que se defina para la protección depende de la empresa, es evidente que las instituciones cuentan con un esquema de seguridad que quizás no sea el más adecuado, pero que trata de ajustarse a las necesidades de la seguridad de la misma. Las aplicaciones, el almacenamiento de la información, las computadoras, los dispositivos de red, y los dispositivos de seguridad perimetral forman parte de un modelo de seguridad. La figura 3.1 muestra un modelo de 6 capas.[23]

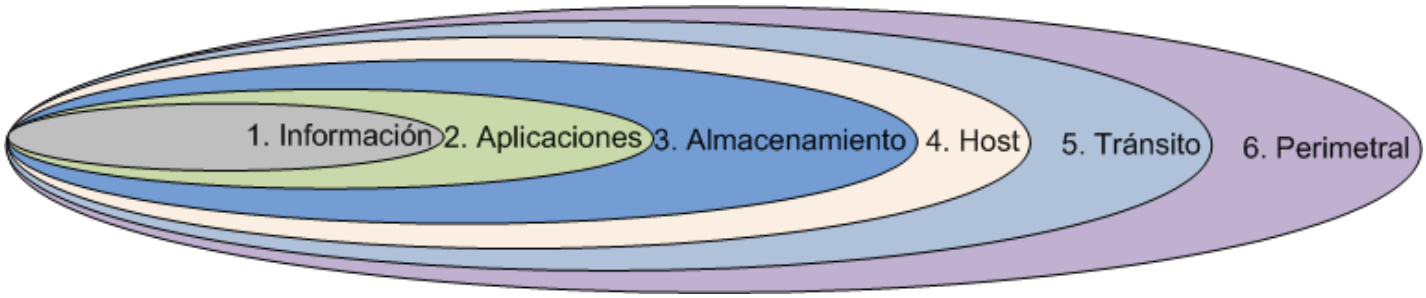

Figura 3. 1 Modelo de seguridad.

Este tipo de modelos puede contemplar estas capas, que se deben ligar con las diferentes posturas de seguridad para implementar cada mecanismo, el número de capas puede aumentar o disminuir con base en las necesidades de la organización.

Ajustarse a una estrategia de seguridad es muy importante al momento de construir o elegir una solución de seguridad, existen diferentes estrategias que responden a diferentes principios asumidos

[23] Aaron Clemente Lacayo Arzú, Análisis e Implementación de un esquema de Seguridad en Redes para las Instituciones de Educación superior, Universidad de Colima http://www.cujae.edu.cu/eventos/convencion/cittel/Trabajos/CIT052.pdf

para llevar a cabo la implementación de una solución de seguridad, inclusive se pueden emplear diferentes estrategias de manera simultánea en diferentes puntos dentro de la organización, dentro de éstos se encuentran:

- Defensa perimetral.
- Seguridad en profundidad.
- Eslabón más débil.
- Seguridad basada en red.
- Seguridad basada en host.
- Principio de menor privilegio.
- Seguridad por oscuridad.
- Simplicidad.
- Punto de ahogo.
- Diversidad de la defensa.

1. Defensa perimetral

El modelo de defensa perimetral es una analogía a un castillo rodeado por una fosa, cuando se utiliza este modelo en la seguridad de una red, las organizaciones aseguran o fortalecen los perímetros de sus sistemas y los límites de sus redes, en sí la defensa perimetral es un conjunto de medidas, estrategias, técnicas que permiten defender y establecer un monitoreo de la parte más exterior de la red, los mecanismos más utilizados para establecer perímetros son los firewalls, IDS, VPN, DMZ y NAT. Permite una administración centralizada de la red, ya que se concentran los esfuerzos en algunos pocos puntos de acceso que definen al perímetro. Es importante mencionar que este modelo no hace nada para proteger los sistemas de ataques internos, puede presentar fallas eventuales como cualquier otro sistema.

En la elección de las herramientas a utilizar se deben tomar en cuenta los siguientes aspectos:

- Recursos físicos.
- Infraestructura de red.
- Flujo de Información.
- Políticas establecidas.
- Cantidad de información (Capacidad de manejo de información).

Antes de su implementación se debe saber de qué se busca protegerse en el exterior, para determinar qué control es el más adecuado para cubrir este bien, así como las políticas actuales de la organización.

2. Seguridad en profundidad

El principio universal del concepto de defensa en profundidad y que se encuentra en los tres ámbitos, militar, industria y seguridad de sistemas de información, define varias barreras independientes, esta estrategia es el modelo más robusto de defensa ya que se esfuerza por robustecer y monitorear cada sistema.

Se basa en la implementación de diferentes zonas de seguridad resguardadas por diferentes mecanismos, donde cada uno de ellos refuerza a los demás, de esta manera se evita que si uno de los mecanismos falla se deje vulnerable la red completa ya que existen otros mecanismos que vencer.

El principio trata de hacer más difícil y costoso a un atacante la tarea de violar la seguridad de una red, esto se logra con la multiplicidad y redundancia de la protección, organizada entorno a múltiples niveles de seguridad, cada mecanismo respalda a otro que se encuentre en una capa inferior, cubriendo en ocasiones aspectos traslapados.

Un punto importante de esta estrategia determina evitar fallas de modo común, es decir, que los mecanismos empleados deben ser cuidadosamente configurados para evitar que las fallas de uno no se propaguen al resto, la defensa en profundidad recomienda que los mecanismos sean de diferentes marcas, debido a que si se logra vulnerar por algún medio uno de ellos, el siguiente no pueda ser vulnerado de la misma forma.

3. Eslabón más débil

Esta postura de seguridad determina la robustez de la misma con base en su punto de falla mas critico, aplicado a redes, establece que un equipo es tan seguro como lo es su punto más débil, este punto suele ser el objetivo de los ataques de una red. El objetivo de esta estrategia identifica aquellos enlaces débiles en la red y tratar de eliminarlos, algunos ejemplos de eslabones débiles dependientes de otros factores pueden ser configuraciones, vulnerabilidades, personal y contraseñas principalmente.

4. Seguridad basada en red

Se centra en controlar el acceso a la red, y no en asegurar los hosts en sí mismos, este modelo se encuentra diseñado para tratar los problemas en el ambiente de seguridad perimetral, aplicando los mecanismos de protección en un lugar común por el cual circula todo el tráfico desde y hacia los hosts. Un enfoque de seguridad en red involucra la construcción de firewalls, mecanismos de autenticación, cifrado para proteger la confidencialidad e integridad de datos y detectores de intrusos principalmente.
La ventaja sobre el modelo de seguridad de host es una considerable reducción en la administración, ya que sólo se requiere proteger unos pocos puntos de acceso, lo que permite concentrar todos los esfuerzos en una solución perimetral. Este modelo es escalable en medida de que la solución perimetral pueda soportar los cambios sin afectar su desempeño. Una desventaja de este modelo es que depende de algunos puntos de acceso, por lo que puede producir en el desempeño reducciones del tráfico de entrada y salida.

5. Seguridad basada en host

Los esfuerzos de seguridad están enfocados en los sistemas finales de una red privada, es decir, que los mecanismos de seguridad son implementados en los sistemas y son ellos mismos los encargados de su protección.

Probablemente sea el modelo de seguridad para computadoras comúnmente utilizado, pero no recomendado para organizaciones grandes, los problemas más comunes para este tipo de estrategia son:

- La administración de seguridad de todos los equipos no es centralizada, por lo que se recomienda emplearlo en esquemas pequeños o donde no existe una red configurada que pueda ofrecer dicha protección.
- Son heterogéneos los mecanismos de seguridad que se tiene en los hosts, es decir, los mecanismos de protección son diferentes en cada equipo.
- Mantener e implementar efectivamente la protección a este nivel requiere una importante cantidad de tiempo y esfuerzo.
- No es recomendable implementar seguridad basada en host para sitios grandes, ya que se requiere demasiado personal de seguridad para esta tarea.

Es importante considerar esta protección para entornos grandes pero debe ser complementada con seguridad perimetral y en profundidad para brindar mayor protección.

6. Principio de menor privilegio

Va dirigido al control de acceso y a la autenticación, consiste en conceder a cada objeto (usuario, programa, sistema, etcétera) sólo aquellos permisos o privilegios para que se realicen las tareas que se programaron para ellos.

Esta estrategia permite limitar la exposición a ataques y disminuir el daño que se puede causar por accesos no autorizados a recursos, está basada en el razonamiento de que todos los servicios ofrecidos están pensados para ser utilizados por algún tipo de objeto y que no cualquiera pueda acceder al recurso que desee, muchas soluciones utilizan técnicas para implementar una estrategia de mínimo privilegio, que permite el paso únicamente para los servicios o recursos deseados.

Cuando se implementa alguna política de seguridad, un comienzo para una buena implementación es brindar derechos a los usuarios en función de su trabajo, una filosofía conocida como menor privilegio.

7. Seguridad por oscuridad

Seguridad por oscuridad confía en el secreto como seguridad, el concepto detrás de este modelo es que si uno no conoce que red o sistema existe, éste no será susceptible de ataques. La idea de esta estrategia está basada en mantener oculta la verdadera naturaleza del mecanismo empleado para brindar seguridad, en el caso de una red, la red privada y sus componentes, esta suposición es algo ingenua ya que varios estudios han demostrado que el interés de un atacante por un determinado sitio, involucran varios sistemas y varias cuentas de usuario para obtener acceso a otros sistemas antes de alcanzar su objetivo real.

Esta estrategia aunque puede ser útil en un comienzo de la vida de un sistema y una buena precaución, es una base pobre para una solución de seguridad a largo término, ya que la información tiende a filtrarse.

8. Simplicidad

Se tiene el entendido de que mientras más grande sea un sistema, los mecanismos de seguridad que deberán de implementarse serán de la magnitud del sistema, pero los protocolos de administración a emplear deberán ser elegidos solo aquellos que se planeen utilizar, ya que de lo contrario se generarán más errores, debido a más configuraciones, puntos vulnerables y falta de mantenimiento principalmente, lo que como consecuencia trae que posiblemente existan agujeros de seguridad no conocidos que un atacante pueda explotar, por más complejos que sean.

La simplicidad de los sistemas de seguridad es un factor importante de una sólida defensa de red, particularmente de los sistemas de seguridad de red a nivel de aplicación, no deberá tener funcionalidades desconocidas y deberá mantenerse lo más simple posible.

9. Punto de ahogo

Enfocado a la red, consiste en depender de un único punto de acceso a la red privada para todas las comunicaciones entre ésta y la red pública, ya que no existe otro camino para el tráfico de entrada y salida, los esfuerzos de control y mecanismos se centran en monitorear un solo sitio de red.

Esta estrategia se considera como una solución centralizada, pero como consecuencia si se logra comprometer la seguridad en esta estrategia, se tendrá acceso a todos los recursos de la red, o en caso contrario, bloquear todos los servicios, esta situación puede ser tratada utilizando mecanismos de protección redundantes y reforzar la seguridad de los puntos de ahogo.

Los inconvenientes que puede provocar esta estrategia son:

- Puede producir bajas en el desempeño de la comunicación con la red exterior.
- Se emplean firewalls perimetrales en esta solución, por lo que el firewall debe tener la capacidad de poder procesar todo el tráfico que pase.
- Si se cuenta con algún otro tipo de acceso alternativo a la red interna esta solución no tiene sentido, ya que se deberá asegurar también el otro acceso a la red.

10. Diversidad de la defensa

Esta estrategia plantea el uso de diferentes tipos de sistemas de seguridad, es decir, de diferentes proveedores y mecanismos, pueden contemplarse como defensa en profundidad. El objetivo de la variedad es reducir la posibilidad de fallas comunes en todos los sistemas utilizados para proteger la red debido a errores propios de los sistemas o configuraciones.

Esta estrategia tiene las siguientes desventajas:

- Posible costo adicional, tanto económico, como de tiempo y complejidad, ya que se debe conocer el funcionamiento y manejo de más de un producto.
- La posible incompatibilidad de los sistemas, aunque actualmente existen estándares que permiten a diferentes sistemas que coexistan como una sola red para lograr una solución integral.

Estas consideraciones deben de ser evaluadas por la organización, para determinar la conveniencia de esta estrategia.

3.3 Servicios seguros

Los servicios seguros brindan mayor confiabilidad en sus procesos, dentro de éstos se encuentran integridad, confidencialidad, no repudio, autenticación, control de acceso y disponibilidad.

Muchos de los mecanismos de seguridad que se emplean actualmente pueden ser utilizados para provocar un ataque cuando no son configurados de manera adecuada, errores propios de sistema y vulnerabilidades aún no descubiertas, por esta razón es importante contemplar las debilidades conocidas que poseen los protocolos y mecanismos de seguridad que se empleen, el escenario donde se implementará y una buena configuración, esto con la finalidad de conocer puntos débiles en ellos y encontrar la manera de protegerlos.

Aun así el uso de mecanismos de seguridad con un buen funcionamiento tienen su parte negativa, por ejemplo, el hecho de utilizar un canal cifrado, permite a los puntos involucrados mantener una comunicación por un canal seguro, pero qué pasa si es comprometido uno de los puntos, en este caso el cifrado no protege el resguardo de la contraseña, lo que permite al atacante utilizar este canal para la finalidad que él desee, además por ser un canal seguro, las operaciones y comandos que realice el atacante no podrán ser analizados de manera directa, generando un problema en las bitácoras. En el ejemplo anterior se plantea una debilidad de emplear canales seguros, la solución propuesta sería generar bitácoras de los sistemas y las operaciones que realicen todos los usuarios.

Otro problema que genera un canal seguro es la creación de más paquetes para la comunicación, la carga de procesador generada es mayor, así como el consumo de memoria adicional al momento de transmitir la información o almacenarla, por tal razón debe ser considerado si no afecta la disponibilidad del sistema en este caso, algunas soluciones permiten comprimir la información, antes de cifrarla, lo que disminuye un poco la carga de procesador y memoria.

1. Cifrado[24]

La herramienta automatizada más importante, para la seguridad de redes y comunicación es el cifrado, uno de los mecanismos más utilizados que busca garantizar la confidencialidad entre dos entidades, generalmente los sistemas criptográficos se clasifican atendiendo a tres factores independientes:

- ***El tipo de operación utilizada para transformar el texto claro en texto cifrado*:** todos los algoritmos de cifrado se basan en dos principios generales: sustitución donde cada elemento de texto claro (bit, letra, grupo de bits o letras) se sustituye por otro diferente y transposición, donde todos los elementos del texto claro se reordenan con base a operaciones específicas. Lo fundamental del proceso es que no se pierda la información, es decir, que todas las operaciones sean reversibles. La mayoría de los algoritmos criptográficos emplean múltiples etapas de sustitución y transposición.
- ***El número de claves usadas*:** si tanto el emisor como el receptor utilizan la misma clave, el sistema se denomina cifrado simétrico, de clave única o cifrado convencional. En cambio, si el emisor y el receptor utilizan cada uno claves diferentes, el sistema se denomina cifrado asimétrico, de dos claves o cifrado de clave pública.
- ***La forma de procesar el texto claro*:** un cifrado de bloque procesa un bloque de elementos cada vez, produciendo un bloque de salida por cada bloque de entrada. Un cifrado de flujo procesa los elementos de entrada continuamente, produciendo la salida de un elemento cada vez.

Considerando la segunda clasificación (número de claves usadas), existen dos tipos de cifrados, los simétricos (utilizan la misma clave en ambos extremos, es decir, una clave privada) y los asimétricos (contemplan un par de claves diferentes para cada usuario.

El esquema para el cifrado simétrico se muestra en la figura 3.2, este tipo es empleado para brindar confidencialidad, algunos de los algoritmos más utilizados son: DES, 3DES, IDEA, RC5, BLOWFISH y AES.

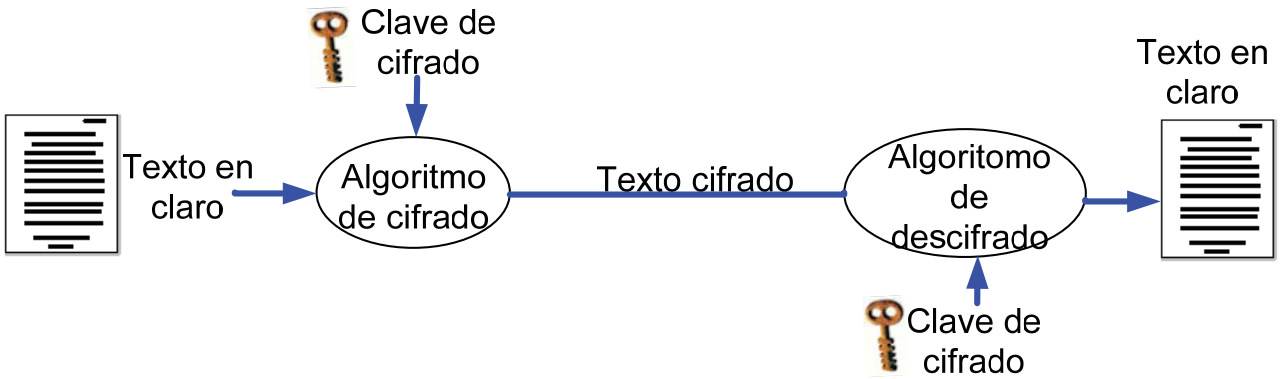

Figura 3. 2 Modelo simplificado de cifrado simétrico.

[24] Ver apéndice C para mayor detalle.

La criptografía asimétrica surge como un complemento a la criptografía simétrica, ya que ésta cubre otros servicios de seguridad como:

- **Cifrado:** Contemplado en la criptografía simétrica.
- **No repudio:** Por medio de firmas digitales.
- **Intercambio de claves:** Algoritmos para resolver la problemática de intercambio de claves.
- **Autenticación:** Autenticación de origen y destino de los datos gracias a su diseño de arquitectura al emplear dos claves.

Un esquema de cifrado de clave pública tiene seis componentes básicos: texto claro, algoritmo de cifrado, clave pública y privada, texto cifrado, algoritmo de descifrado y en algunos casos entidad certificadora (figura 3.3). Los algoritmos de cifrado asimétrico más empleados son: RSA, ElGamal, Diffie –Hellman, DSS, ECC.

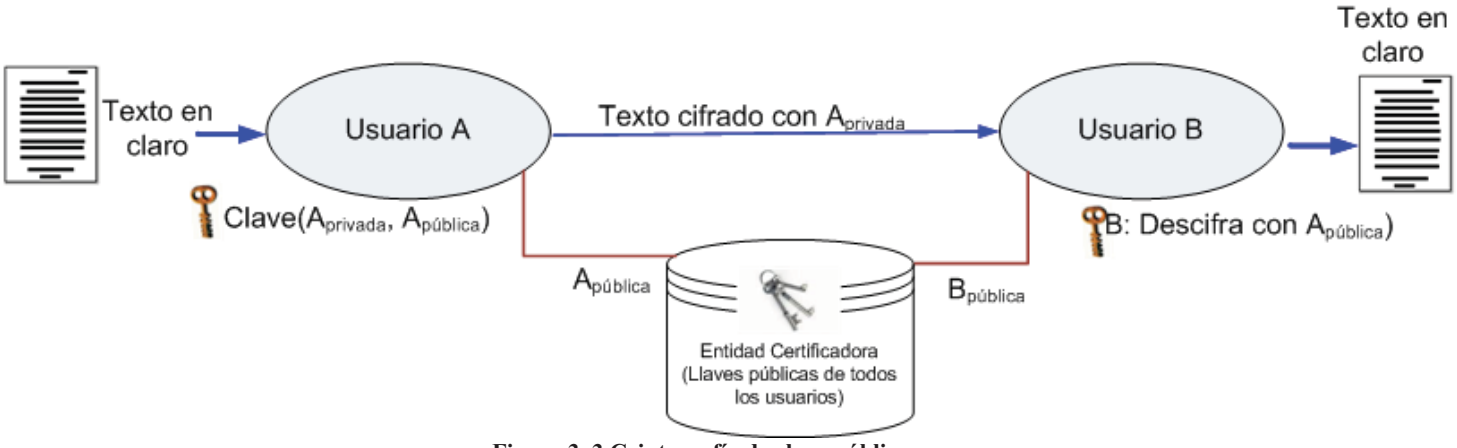

Figura 3. 3 Criptografía de clave pública.

Adicional a estos tipos de cifrado existen algoritmos de resumen llamados funciones Hash que buscan garantizar la integridad de los archivos u ocultar información en claro, dentro de las funciones Hash más comunes se tiene MD5, SHA1, RIPEMD.[25]

2. Seguridad en servidores web

La World Wide Web es una aplicación cliente - servidor que se ejecuta en internet y en las intranets, la web presenta nuevos retos que generalmente no se aprecian en el contexto de la seguridad de los equipos de cómputo ni de las redes:

- Internet es bidireccional, al contrario de los entornos de publicación tradicional, la web es vulnerable a los ataques a los servidores web, desde internet.
- La web se emplea cada vez más para dar información acerca de la organización, productos y como plataforma para transacciones de negocio. Si se comprometen se puede perjudicar la imagen y ocasionar pérdidas económicas.

[25] Ver Apéndice C para mayor detalle.

- Aunque los navegadores web son muy fáciles de usar, los servidores relativamente sencillamente de configurar y gestionar y los contenidos web cada vez más fáciles de desarrollar, el software subyacente es extraordinariamente complejo, éste puede ocultar muchos posibles fallos de seguridad.
- Un servidor web puede utilizarse como una plataforma de acceso a todo el complejo de computadoras de una agencia o corporación, una vez comprometida la seguridad del servidor web, un atacante podrá obtener acceso a datos y sistemas fuera del propio servidor pero que están conectados a éste en el sitio local.
- Habitualmente los clientes de servicios basados en web son usuarios ocasionales y poco preparados (en lo que a seguridad se refiere), los cuales no tienen por qué ser conscientes de los riesgos que existen y no tienen las herramientas ni los conocimientos necesarios para tomar medidas efectivas.[26]

Tabla 3. 1 Amenazas en la web.

	Amenazas	Consecuencias	Contramedidas
Integridad.	- Modificación de datos de usuario. - Modificación de memoria. - Modificación del tráfico del mensaje en tránsito.	- Pérdida de información. - Vulnerabilidad al resto de las amenazas.	- Suma de comprobación (checksum) criptográfica.
Confidencialidad.	- Escuchas ocultas en la red. - Robo de información del servidor - Robo de datos del cliente. - Información sobre la configuración de la red. - Información sobre qué cliente se comunica con el servidor.	- Pérdida de información. - Pérdida de privacidad.	-Cifrado.
Denegación de servicio.	- Interrupción de procesos del usuario. - Llenar el espacio del disco, memoria o procesador. - Aislar la máquina mediante ataques DNS.	- Destructivo. - Molesto. - Impide que los usuarios finalicen su trabajo.	- Difícil de prevenir.
Autenticación.	- Suplantación de usuarios legítimos. - Falsificación de datos.	-Suplantación de identidad. - Creer que la información falsa es válida.	- Técnicas criptográficas, mecanismos de control de acceso, políticas de contraseñas.

[26] William Stallings, Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Prentice Hall, 2da edición, 2005 pág. 225

La tabla 3.1 muestra un resumen de los tipos de amenazas a la seguridad que se afrontan al usar la web, otra manera de clasificar las amenazas a la seguridad de la web es en función de la ubicación de la amenaza: servidor web, navegador web y tráfico de red entre navegador y servidor.

Hay varios enfoques para brindar seguridad en la web, dichos enfoques son similares en los servicios que proporcionan y hasta cierto punto, en los mecanismos que usan, pero diferentes en lo que respecta a su ámbito de aplicabilidad y en cuanto a su ubicación relativa dentro de la pila de protocolos TCP/IP.

La figura 3.4a ilustra las diferentes formas de proporcionar seguridad en la web, una forma de proporcionar seguridad en la web es usar seguridad IP (IPSec- IP Security), las ventajas de usar IPSec es que es transparente para el usuario final y para las aplicaciones, proporcionando una solución de propósito general, además IPSec ofrece capacidad de filtrado de manera que solamente el tráfico seleccionado afecta la carga de procesamiento del mismo.

Otra solución de propósito relativamente general es implementar la seguridad justo encima de TCP (figura 3.4b). El principal ejemplo de este enfoque es Secure Socket Layer –Capa de socket seguro (SSL) y su sucesor Transport Layer Security – Seguridad en la capa de transporte (TLS), se podrían proporcionar como parte de la suite de protocolos y de esta manera, ser transparente a las aplicaciones, como es el caso de los navegadores Netscape y Microsoft Explorer y la mayoría de los servidores web vienen equipados con SSL.

El último enfoque consiste en la inclusión de servicios de seguridad específicos de las aplicaciones, la ventaja de este enfoque es que el servicio se puede adecuar a las necesidades de una aplicación. En el contexto de la seguridad en web, un ejemplo importante de este enfoque es SET (Secure Electronic Transaction – Transacciones electrónicas seguras).

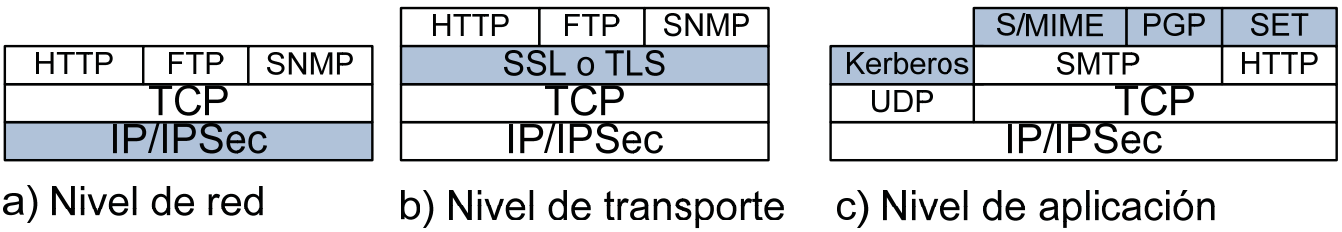

Figura 3. 4 Ubicación relativa de las herramientas de seguridad en la pila de protocolos TCP/IP.

3. SSL

Secure Socket Layer – Capa de socket seguro, es el acrónimo de SSL, este protocolo fue desarrollado por Netscape para brindar seguridad cuando se transmite información a través de Internet, Netscape reconoció la necesidad de transmitir información en internet garantizando confidencialidad, esa fue la razón de implementar este protocolo.

SSL está diseñado de forma que utilice TCP para proporcionar un servicio fiable y seguro extremo a extremo, SSL no es un protocolo simple, ya que está formado por dos niveles de protocolos (SSL

Record Protocol – Protocolo de registro SSL y SSL Handshake Protocol - Protocolo de saludo SSL), como se observa en la figura 3.5.

Figura 3. 5 Pila de protocolos SSL.

SSL emplea llaves tanto simétricas como asimétricas para configurar la transferencia de datos de una manera segura sobre una red insegura, cuando un cliente establece una conexión SSL entre su navegador y el servidor, genera un canal seguro para HTTP conocido usualmente como HTTPS, de tal forma que impide a un intruso interpretar los datos que son trasmitidos por este canal, la figura 3.6 muestra la forma en la que opera este protocolo.

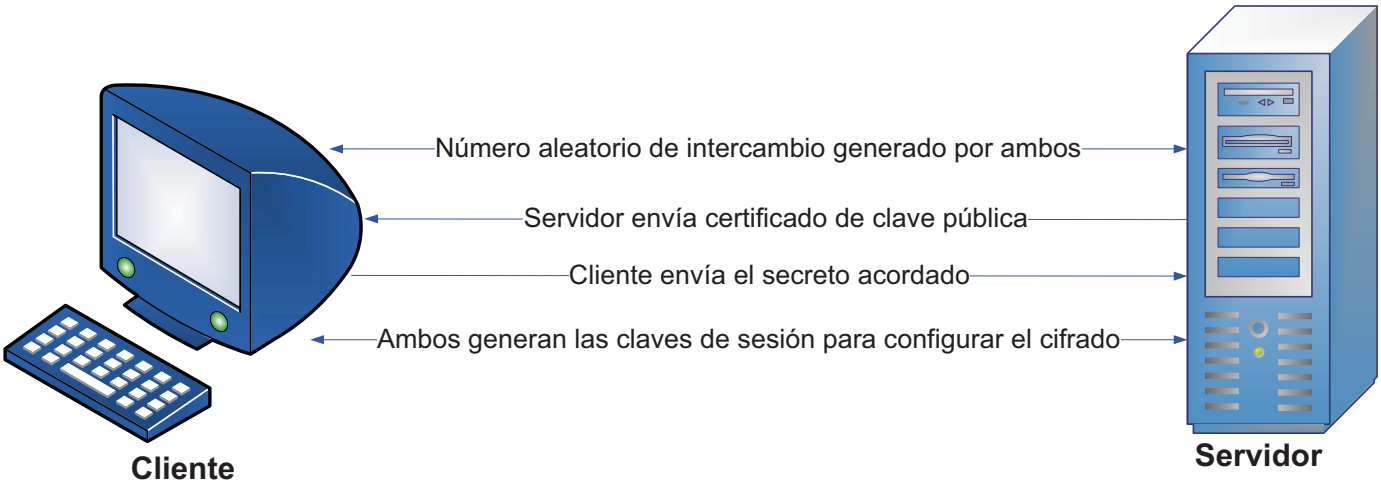

Figura 3. 6 Handshake de SSL.

El funcionamiento del protocolo SSL consiste de lo siguiente:

- El cliente hace una petición a páginas Web de tipo HTTPS.
- El servidor envía su certificado digital al cliente.
- El cliente comprueba que el certificado ha sido emitido por una entidad certificadora de confianza.
- El cliente y el servidor acuerdan un algoritmo de cifrado soportado por ambas partes.
- Se realiza un intercambio de claves por medio de criptografía.
- Se comunican de forma cifrada utilizando la clave compartida.

4. TLS

TLS (Transport Layer Security – Seguridad en la capa de transporte), es una iniciativa de estandarización de la IETF cuyo objetivo es producir una versión sucesora al estándar SSL, está basada en la versión SSL v3 y ofrece las mismas ventajas que SSL. Al generar un canal seguro para el protocolo HTTP en conexiones TCP, creó un nuevo protocolo denominado HTTPS, el cual genera canales seguros para sus comunicaciones.

Un par de participantes TLS negocia qué algoritmos de cifrado utilizar, y una elección de:

- Hash de integridad de datos, MD5 o SHA1.
- Cifrado de clave simétrica para confidencialidad, algunas posibilidades son DES, 3DES y AES.
- Establecer clave de sesión, algunas opciones son Diffie Hellman, corrección de Diffie Hellman y algunos protocolos de autenticación de clave pública como RSA o DSS.
- Permite configurarse como autenticación mutua o sólo unilateral.

Adicional a esto los participantes pueden negociar el uso de algún algoritmo de compresión de datos. Aunque el método utilizado con más frecuencia para establecer conexiones seguras a través de internet sigue siendo SSL.

5. SSH

SSH es el acrónimo de Secure Shell – Shell seguro, fue originalmente diseñado para asegurar los flujos de datos en Telnet, este protocolo fue un protocolo de facto en los sistemas operativos Unix es el protocolo sucesor a Telnet, el cual permitía conectarse a un host y establecer una consola remota de texto para que el host pudiera ser operado por un canal seguro, Telnet fue muy utilizado hace algunos años cuando los atacantes no tenían acceso a internet, éste no implementaba cifrado y los datos de usuario y contraseña viajaba como texto en claro.

SSH brinda una autenticación confiable ya que permite verificar la identidad de un usuario por contraseña, mediante clave pública y privada, además de cifrar los datos que se transmiten entre dos terminales, utiliza cifrado de clave pública, es una herramienta útil para la administración de sistemas(figura 3.7).

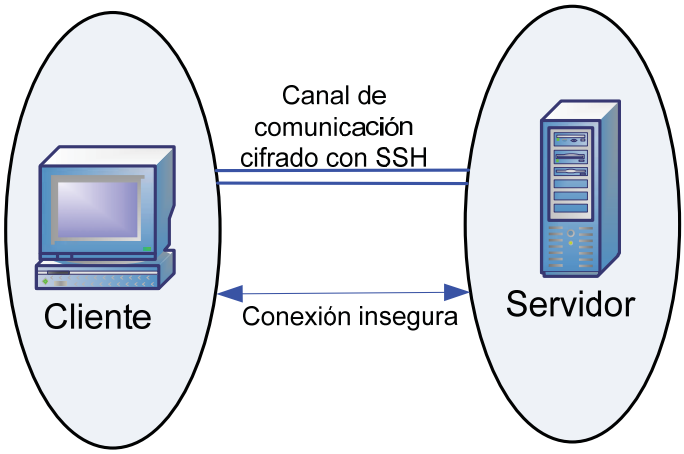

Figura 3. 7 SSH.

SSH provee fuerte autenticación y comunicación segura sobre un canal inseguro y nace como remplazo a los comandos telnet, ftp, rlogin, rsh y rcp, los cuales proporcionan gran flexibilidad en la administración de una red, pero representan riesgos de seguridad.
Secure Shell admite varios algoritmos de cifrado entre los cuales se incluye:

- Blowfish.
- 3DES.
- IDEA.
- RSA.

6. VPN

Acrónimo de Virtual Private Network –Red privada virtual, es un mecanismo empleado por dispositivos activos o por software que permite generar un canal seguro de comunicación, utiliza una infraestructura pública compartida como Internet en la cual ofrece las facilidades y ventajas de una red privada. Dentro de las redes privadas se consideran las VPN y LAN virtuales, pero dentro de las VPN sus clasificaciones con base en su modo de trabajo son host-to-host (figura 3.8), host-to-network (figura 3.9) y network-to-network (figura 3.10).

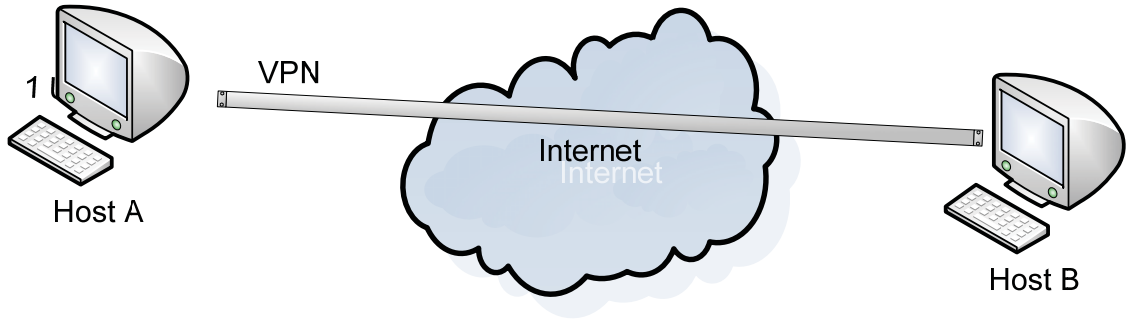

Figura 3. 8 VPN Host to Host

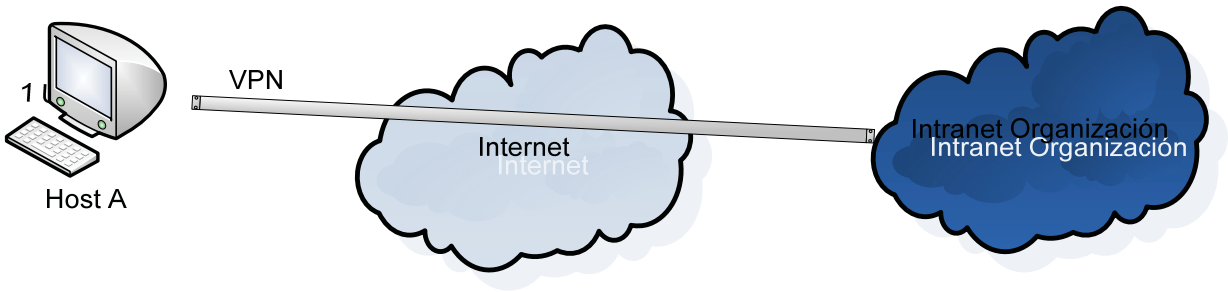

Figura 3. 9 VPN Host to Network

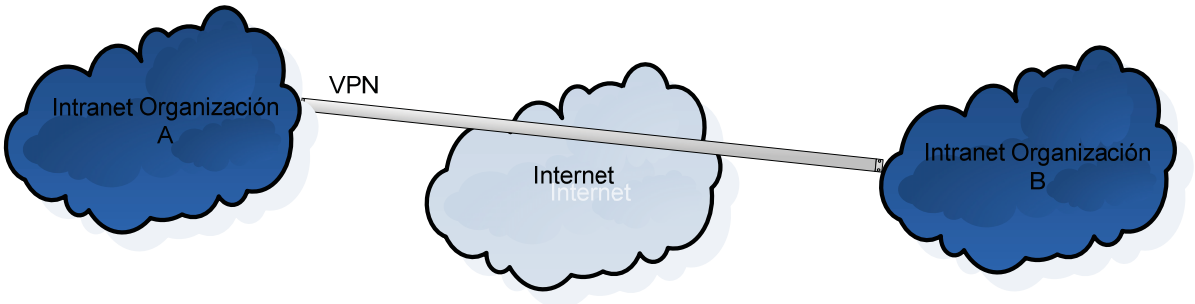

Figura 3. 10 VPN Network to Network.

Las VPN's pueden ser configuradas con diferentes protocolos PPTP, L2TP, IPSEC, SSL, éstos definen en qué capa del modelo OSI trabajarán(figura 3.11). El protocolo PPTP fue desarrollado por Microsoft y actualmente es un estándar de facto, suficientemente seguro para casi todas las aplicaciones, el protocolo L2TP es un estándar de la IETF, el problema de este protocolo es su interoperabilidad.

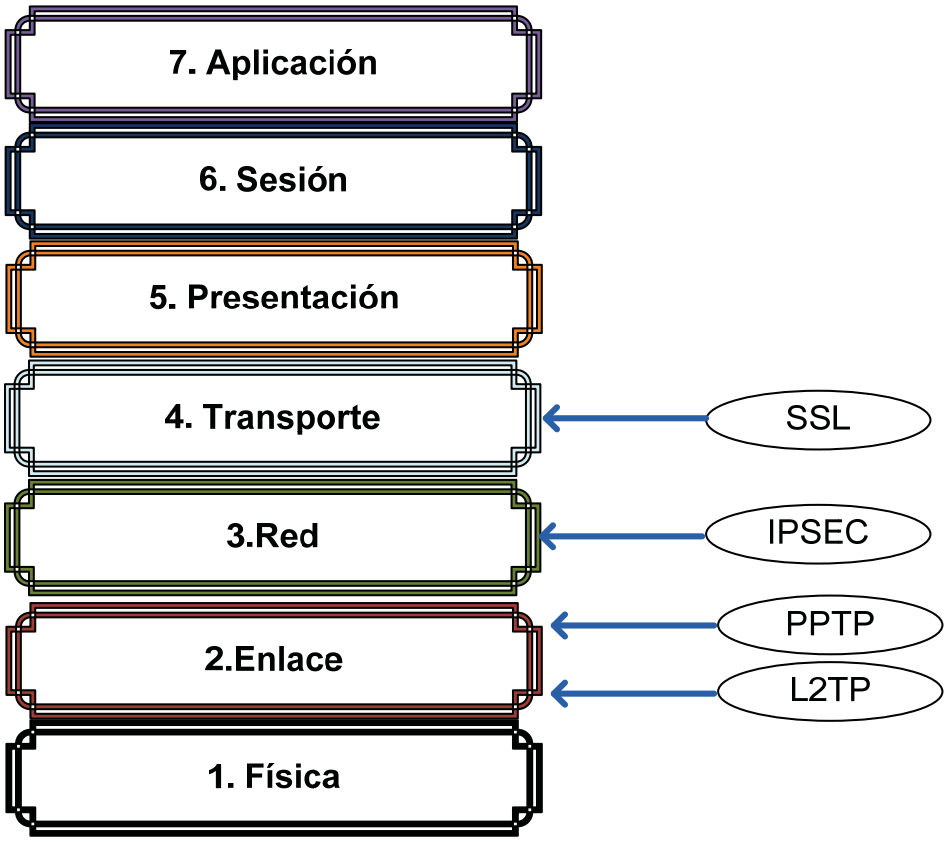

Figura 3. 11 Protocolos VPN en el modelo OSI.

La configuración de éstos depende de las necesidades de la empresa, es conveniente su implementación pero también puede crear grandes agujeros en la red, algunas prácticas que se recomiendan son:

a) Asegurar el sistema operativo de los equipos de comunicación: Una solución de VPN no brinda solución efectiva si el sistema operativo de los equipos no es seguro, presumiblemente el firewall deberá proteger de los ataques al sistema operativo, por tal razón en un esquema VPN se debe de contemplar un firewall para rechazar los hosts que no son reconocidos para implementar una comunicación.

b) Implementar alguna VPN de un punto final hacia un servidor interno de la organización: Con una implementación fuerte de filtrado hacia la VPN puede ser fácilmente comprometida para obtener acceso a la red desde cualquier lugar.

c) Asegurar los host remotos: Qué los usuarios que se conectan de manera remota a la VPN utilicen software VPN seguro.

d) Utilizar un solo ISP: Utilizar un solo ISP (Internet Services Provider – Proveedor de servicios de Internet) para conectar todos los puntos finales, esto garantiza el acceso hacia ellos.

7. NAT

Un NAT (Network Address Translation –Traducción de direcciones de red), es un esquema implementado por las organizaciones para desafiar la deficiencia de direcciones de las redes IPv4, básicamente traduce direcciones privadas que son normalmente internas a una organización en particular, en direcciones ruteables sobre las redes públicas como Internet.

En particular, NAT es un método para conectar múltiples computadoras a Internet o cualquier otra red IP utilizando una misma dirección IP homologada, aunque la meta principal de un NAT es incrementar el alcance de direcciones IP (contemplando mucho más direcciones IP en la arquitectura IPv6), la seguridad es un atributo esencial que puede potencialmente ser alcanzado por una NAT.

Un NAT puede ser complementada con el uso de firewall brindando una medida extra de seguridad para la red interna de una organización, usualmente los hosts internos de una organización son protegidos con direcciones IP privadas, las cuales pueden comunicarse con las redes exteriores pero no de manera inversa (figura 3.12), permiten a una organización que opere utilizando pocas direcciones IP homologadas, lo que permite confundir a un atacante para ubicar cuál host en particular es su objetivo.

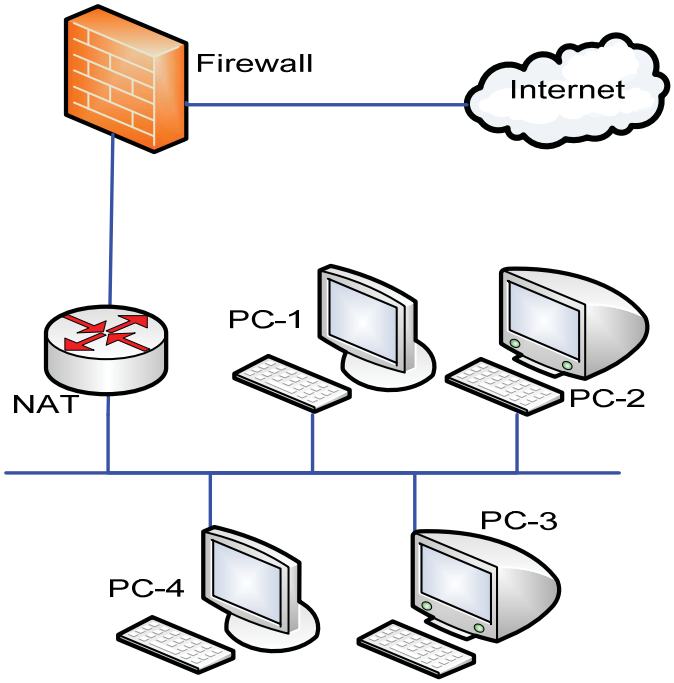

Figura 3. 12 Diagrama de funcionamiento de un NAT.

La principal característica en una NAT es la tabla de traducción, una NAT puede ser implementada con una PC y las apropiadas interfaces de red, así como por medio de un router ya pre configurado en el BIOS del dispositivo, las tablas de traducción mapean una única dirección IP homologada a las direcciones IP privadas, normalmente este mapeo no es uno a uno, para conservar el espacio de direcciones, una dirección IP pública puede mapear a más de una dirección IP privada, típicamente se realiza una asociación de puertos en las NAT creadas para lograr múltiples mapeos de direcciones públicas y privadas. Cualquier paquete del exterior intenta encontrar un host particular en la red

privada obteniendo la ruta que la dirección global de la NAT le asigne, es responsabilidad de ésta buscar en la tabla de traducción la dirección privada que busca el paquete específico.

8. Kerberos

Kerberos es un sofisticado método de autenticación de red y protocolo de seguridad desarrollado por el MIT (Massachusetts Institute of Technology – Instituto de tecnología de Massachusetts), el nombre se deriva del guardián de las puertas del infierno en la mitología Griega. Kerberos es un esquema de autenticación basado en certificados que confía en la autenticidad de éstos, por medio de una autoridad certificadora.

Fue diseñado para abordar el problema que plantea un entorno abierto distribuido, los usuarios de estaciones de trabajo quieren acceder a servicios de servidores distribuidos por toda la red, es conveniente que los servidores pudiesen restringir el acceso a los usuarios autorizados y autenticar las solicitudes de servicio. En este entorno no se puede confiar en que una computadora identifique a sus usuarios correctamente ante los servicios de red, ya que se pueden presentar las tres amenazas que se exponen a continuación:

- Un usuario podría obtener acceso a una computadora concreta y fingir ser otro usuario que opera desde ese equipo.
- Un usuario podría alterar la dirección de red de una computadora para que las solicitudes enviadas parezcan proceder del equipo que ha sido suplantado.
- Un usuario podría correr un sniffer y ver los intercambios de paquetes, buscando hacer un ataque de repetición para entrar a un servidor.

En cualquiera de estos casos, un usuario no autorizado podría obtener acceso a servicios y datos para los que no tenga autorización. En vez de crear protocolos elaborados de autenticación en cada servidor, Kerberos proporciona un servidor centralizado de autenticación, cuya función es autenticar a los usuarios al servidor, y los servidores a los usuarios.

9. Active Directory

Es un servicio que brindan los sistemas operativos para servidores de Microsoft, su función es gestionar las identidades y relaciones que conforman los entornos de red, permite administrar eficazmente los recursos de red, permite un punto único de administración para todos los recursos públicos como archivos, dispositivos, bases de datos, usuarios, etcétera. Para este tipo de implementación se debe contemplar el entorno que conforma la red, ya que sólo aquellos equipos que tengan sistema operativo Microsoft u algún software adicional en el caso de UNIX, podrán ser contemplados en este funcionamiento, así como también tomar en cuenta el gasto monetario que involucran las licencias tanto de los miembros como del servidor.

La arquitectura básica de Active Directory – Directorio activo, parte de la creación de un dominio, el cual será la unidad lógica que agrupa objetos (usuarios o equipos) a los que se les dará acceso a los recursos (archivos, dispositivos, base de datos), en dicha arquitectura se tiene dos figuras principales:

a) **Controlador de dominio**: Equipo con alguna versión de Windows Server que mantiene la base de datos de Active Directory.
b) **Servidor miembro**: Equipo que forma parte del dominio haciendo uso de los servicios del mismo.
Las características que ofrece contemplan escalabilidad en la cantidad de objetos que puede administrar, integración de servidor DNS, permite manejar servidores secundarios de Active Directory garantizado disponibilidad, manejo de unidades organizacionales, grupos, permite que trabajen varios dominios de manera conjunta, entre muchas otras más prestaciones, este tema es bastante extenso, debido a ello si se requiere más información de algún punto particular de Active Directory se refiere la siguiente bibliografía.[27]

3.4. Control de acceso

Quizá uno de los más importantes elementos de seguridad de la información, es definir qué sujetos tienen acceso sobre los objetos, la finalidad del control de acceso es típicamente descrito por la abreviatura AAA (Authentication, Authorization, Auditing -Autenticación, autorización y Auditoría).

Autenticación es la primera meta del control de acceso, ésta asegura que el usuario sea quien dice ser, autorización define los permisos que posee el usuario dentro del sistema y auditoría determina un seguimiento de las actividades que hace el usuario.

Se utilizan definiciones como:

- ***Objeto***; cualquier ente pasivo que contiene información (cualquier archivo).
- ***Sujeto***; cualquier ente activo que funciona en nombre de los usuarios (proceso, servicio, tarea, sistema, etcétera).

El control de acceso en la parte de autorización es dividido en tres modelos, Control de acceso discrecional (Discretionary Access Control -DAC), control de acceso mandatorio (Mandatory Access control - MAC) y control de acceso basado en roles (Role Base Access Control - RBAC).

a) ***El control de acceso discrecional***, donde una autoridad define limitaciones de privilegios de acceso a recursos, también conocidos como ACL Access Control List – Lista de control de acceso, permite a los propietarios de los recursos crear reglas de acceso a sus propios recursos, es ideal para un ambiente descentralizado, pero puede ser difícil de administrar.
b) El control de mandatorio*,* el control de acceso es definido por medio de etiquetas las cuales indican los privilegios a los que se tienen derecho dependiendo de la etiqueta que posea el objeto,

[27] Melissa M, Syngress, Designing a Windows server 2003 active Directory Infrastructure.

cuando un usuario intenta acceder a un objeto, las etiquetas de seguridad para el usuario y el objeto son comparadas, si el nivel de seguridad del usuario es más alto que del objeto, el acceso es permitido.
El control de acceso mandatorio es regido por:

- El usuario no controla la autorización de acceso a la información.
- Los usuarios reciben un nivel de autorización de acceso denominada etiqueta.
- La información se clasifica según su sensibilidad con una etiqueta (pública, privada, confidencial interna, propietaria, corporativa, top secret, etcétera).
- Los dos puntos anteriores se combinan para crear clases de acceso, comparando la etiqueta del objeto con la etiqueta del sujeto.

El control de acceso mandatorio es adecuado para organizaciones grandes con administración centralizada, el creador de los documentos puede determinar a un usuario qué nivel de acceso le dará a sus documentos, pero el sistema operativo por sí mismo determinará qué usuarios tendrán acceso al archivo y quiénes pueden modificar los permisos otorgados por el propietario.

La implementación de control de acceso mandatorio más común se encuentra en el campo militar, aquí los niveles de seguridad del más bajo al más alto son; sin clasificación, sensitiva pero sin clasificación, confidencial, secreta y top secret. Dentro de un entorno empresarial, cuando es implementado estrictamente, las etiquetas de seguridad de la más alta a la más baja son públicas, sensitivas, privadas y confidenciales.[28]

c) Control de acceso no discrecional (este tipo de control de acceso está definido con base en el papel del individuo dentro de la organización, o las responsabilidades que tenga, el control de acceso basado en rol es utilizado frecuentemente en organizaciones donde el personal cambia frecuentemente, lo cual elimina la necesidad de cambiar privilegios.

Los controles de acceso son utilizados para prevenir ataques, para determinar si un ataque ha ocurrido o se está intentando y monitorear el estado de la red con la finalidad de verificar si un ataque se ha presentado para tratar de corregir la vulnerabilidad explotada, estos tres tipos de controles son llamados preventivo, detectivo y correctivo.

- Preventivo: Previene la ocurrencia de un incidente con base en experiencias anteriores.
- Detectivo: Detecta comportamientos anómalos, emitiendo alertas con el fin de verificar si el comportamiento es válido o se está presentando un incidente.
- Correctivo: Aplica configuraciones con la finalidad de corregir errores detectados anteriormente.

[28] Cliff Riggs, Network perimeter security: building defense in-depth, Auerbach publications, 2000, capítulo 6

3.4.1 Modelos de control de acceso

a) Matriz de acceso

Un modelo de protección visto abstractamente como una matriz, donde los renglones de la matriz representan dominios y las columnas objetos, cada entrada en la matriz determina un conjunto de derechos de acceso (figura 3.13).

Elementos de la matriz de acceso:

- Filas → Conjuntos de Dominios.
- Columnas → Conjunto de Objetos.
- Celdas → Derechos de acceso.

	Objeto 1	Objeto 2	Objeto……..	Objeto N
Dominio 1	Leer	Leer, Escribir, Ejecutar		
Dominio 2				Leer, Escribir
Dominio …….			Ejecutar	
Dominio N		Escribir		

Figura 3. 13 Matriz de acceso ejemplo.

La mayor complicación al momento de definir acceso por medio de la matriz se presenta cuando el número de dominios y objetos es de gran tamaño, lo cual complica su administración al brindar permisos masivos sobre uno o varios objetos, así mismo para la revocación de permisos.

b) Bell-Lapadula

El modelo Bell Lapadula, también llamado modelo multinivel, fue propuesto por Bell y Lapadula para reforzar el control de acceso dentro del gobierno y aplicaciones militares estadounidense en 1973, este modelo es aplicado a la confidencialidad para ayudar a proteger secretos militares, consiste de los siguientes componentes:

- Un conjunto de sujetos, objetos y matriz de control acceso.
- Niveles de seguridad ordenados; cada sujeto cuenta con un nivel de autorización y cada objeto una clasificación determinada en los niveles de seguridad, además cada sujeto tiene un nivel de autorización actual que no puede exceder.

El conjunto de derechos de acceso que se asigna a los sujetos son:

- Sólo lectura: Sólo se puede leer el objeto.
- Agregar: El sujeto puede escribir el objeto pero no puede leerlo.
- Ejecutar: El sujeto puede ejecutar el objeto, pero nunca leer o escribirlo.

- Leer y escribir: El sujeto tiene permisos de leer y escribir el objeto.

Este modelo establece restricciones impuestas:

- **Lectura hacia abajo**: Un sujeto tiene derecho de leer objetos que tengan niveles de seguridad igual o debajo del nivel de seguridad del sujeto, esto previene que un sujeto pueda obtener información disponible en niveles superiores que el nivel de autorización que posee.
- **Escritura hacia arriba**: Un sujeto sólo puede escribir a objetos de su mismo nivel de seguridad o inferior, esto previene que un sujeto aceda a información de nivel inferior, también llamado propiedad de confinamiento.
- **Propiedad de seguridad discrecional**: Se utiliza una matriz de acceso para especificar el control de acceso discrecional.

3.4.2 Métodos de autenticación

Los métodos de autenticación son los caminos que se tienen para comprobar la identidad de un sujeto, de manera general se tiene cuatro factores de autenticación, algo que se tiene, algo que se sabe, algo que se es y por la ubicación física.

En días presentes se dice que un sistema de autenticación es robusto si mezcla dos o más factores de autenticación, un ejemplo claro de este mecanismo es el que emplean actualmente algunos bancos para realizar transferencias bancarias al emplear algo que se sabe por medio de una contraseña y algo que se tiene por medio de un token.

La autenticación hoy en día se puede realizar por cualquiera de los siguientes cuatro factores, o en ocasiones con la combinación de éstos.

- Algo que se sabe (Contraseñas).
- Algo que se es (Biometría).
- Algo que se tiene (Por ejemplo un token).
- Por la ubicación física (Por ejemplo coordenadas geográficas).

Los métodos de autenticación que emplean sólo uno de estos factores de autenticación se conocen como *autenticación de un factor*, la mayoría de los sistemas emplean este método de autenticación, los sistemas que emplean dos o más de estos factores combinados se conocen como métodos de autenticación robusta, significativamente mejora la confidencialidad. La autenticación de dos factores es poco común su implementación en infraestructuras de red, ya que éstas no han sido implementadas para soportarlos.

a) Algo que se sabe

Esto normalmente es un intangible que sólo el usuario autorizado debe conocer, se basa en un secreto compartido para el usuario y el sistema, típicamente se trata de una contraseña (sucesión de caracteres alfanuméricos).

Éste es el camino más común de autenticación, la ventaja principal que ofrece es la administración pero como desventaja en ocasiones los usuarios tienden a elegir como contraseñas datos que se relacionan con ellos y fáciles de recordar, lo que en ocasiones limita la seguridad por la posibilidad de ataques de diccionarios o fuerza bruta, por esta razón es importante implementar en la organización una política de contraseñas robustas.

Se entiende que una contraseña es robusta cuando cumple con lo siguiente:

- Formada por al menos 8 caracteres.
- Maneje caracteres alfanuméricos (números, letras mayúsculas y minúsculas, símbolos).
- No se contemplen palabras de diccionario incluyendo otros idiomas.
- No derivarse del nombre de usuario, familiar cercano o datos personales (teléfono, CURP, RFC, fecha de nacimiento).
- Cambio de contraseñas de manera periódica (por ejemplo cada 3 meses en el caso de cuentas de administración y en cuentas de servicio cada año).
- Debe de crearse de forma que pueda recordarse fácilmente.
- Generar las contraseñas de manera automática por medio de una fuente aleatoria (Por ejemplo fuentes de ruido electromagnético).

Cuando se generan las contraseñas de manera automática, puede provocar que resulte complicado recordar la contraseña, en estos casos se debe educar al usuario en la medida de lo posible para que memorice la contraseña evitado escribir la misma en cualquier lugar.

Como se trata de un secreto compartido se debe proteger éste en ambos extremos, así como en la forma que viaja, ya que si se compromete este secreto la seguridad del sistema se vulnera, por esta razón se debe considerar:

- Guardar siempre las funciones hash de las contraseñas, no el texto en claro.
- En el transporte, no transmitir la contraseña en claro, emplear funciones hash, un canal cifrado o el uso de criptografía de clave pública.
- Políticas de resguardo y educar al usuario en temas de seguridad.
- Establecer controles de acceso a los archivos que resguardan las contraseñas.

Por el lado de los sistemas se deberá configurar para que:

- Se permita cierto número de intentos para autenticarse, alertando al administrador cuando se excedan éstos.
- Limitar el horario de acceso al sistema.

- No permitir sesiones concurrentes.
- Definir desde qué lugar puede iniciar sesión un usuario.

b) Algo que se tiene

Este tipo de autenticación hace referencia a objetos utilizados como métodos de autenticación, es el segundo método más utilizado, asume que el usuario autorizado tiene en su posesión un objeto físico que pruebe su identidad. El objeto de uso común en estos días es el token, cinta magnética, RFID y chips. El principal problema de esta solución si se utiliza solo, es que el objeto físico puede ser perdido, robado u clonado.[29]

Un ejemplo que se puede considerar utilizando este método de autenticación es la llave de los automóviles actuales que utilizan un chip para autenticarse con el automóvil, el sistema de autenticación asume que sólo el dueño del automóvil deberá estar en posesión de la llave, esto por supuesto no siempre es verdad.

Si estos dispositivos se emplean para autenticar de manera remota, es decir fuera del lugar donde está ubicado el sistema de información, se corre el riesgo de que la autenticación del usuario no ocurra, ya que se autentica el dispositivo y éste puede estar en otras manos.

Los riesgos más comunes para este tipo de método incluyen:

- Robo.
- Clonación.

c) Algo que se es

Esta categoría de autenticación, confía en algunas características personales únicas, como lo es ADN, huellas de los dedos, geometría de la mano, iris, retina, reconocimiento facial, forma de caminar y voz principalmente, los humanos tienen un número de características únicas que puede utilizarse para determinar una identidad con un alto grado de certeza.

Mientras que los identificadores biométricos son generalmente considerado lo último a nivel mundial con lo que respecta a métodos de autenticación, éstos sufren de problemas en su implementación. Los más notables, seguridad, aceptación de usuarios y costo, son razones que limitan el uso de este método de autenticación, el problema principal en esta categoría de autenticación consiste en la precisión del instrumento de medición empleado y el rango de error que maneja el dispositivo de lectura.

El umbral de errores en las lecturas es un valor que puede ser configurado en los dispositivos de lectura, de tal manera que se abra el grado de aceptación generando falsos positivos o reducir el

[29] Ibid.

grado de aceptación generando falsos negativos, cuando ambos valores son iguales se tiene una tasa de error igualmente probable.

d) Ubicación física

La autenticación por medio de la ubicación física puede emplear coordenadas geográficas por medio del uso de dispositivos GPS mediante una terminal móvil o teléfono celular el cual brinda un mayor grado de seguridad, en ocasiones también se hace autenticación por el origen de la conexión generando una simulación de autenticación por ubicación utilizando la dirección IP desde donde se realiza la consulta.

El método de autenticación por ubicación más común, es definiendo acceso por el origen de la conexión, mediante la dirección IP, aunque este factor es suplantable.

3.4.3 Por la manera de autenticar

Este factor que se tiene al momento de implementar un control de acceso define la manera en la cual se llevará a cabo la autenticación, es decir, si se autentica de manera unilateral, mutua o por medio de un tercero confiable, la elección de este factor depende de los recursos y nivel de seguridad que se desea conseguir.

a) Unilateral

Este tipo de autenticación permite sólo que uno de los dos participantes se autentique con respecto a otro, por ejemplo al momento de verificar una contraseña sólo se está autenticando en un solo sentido ya que en ningún momento se verifica contra quién o qué se está autenticando (figura 3.14).

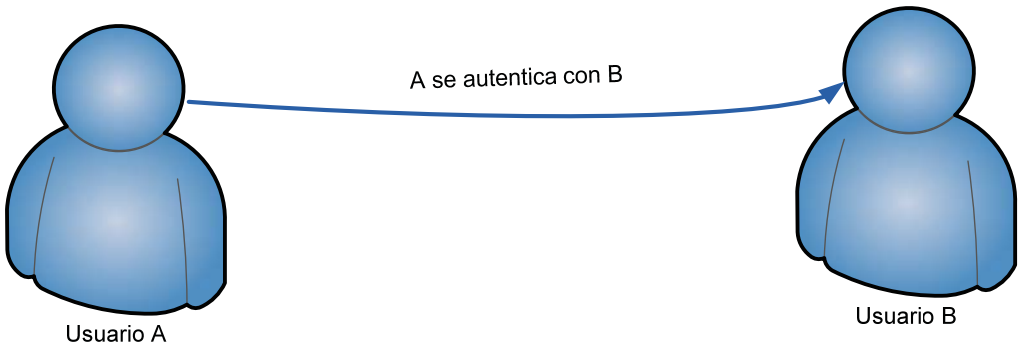

Figura 3. 14 Autenticación Unilateral.

b) Mutua

La autenticación mutua ofrece un nivel de seguridad superior a la autenticación unilateral debido, a que en este esquema los usuarios se autentican entre sí, es decir 'A' se autentica con 'B' y 'B' se autentica con 'A' (figura 3.15).

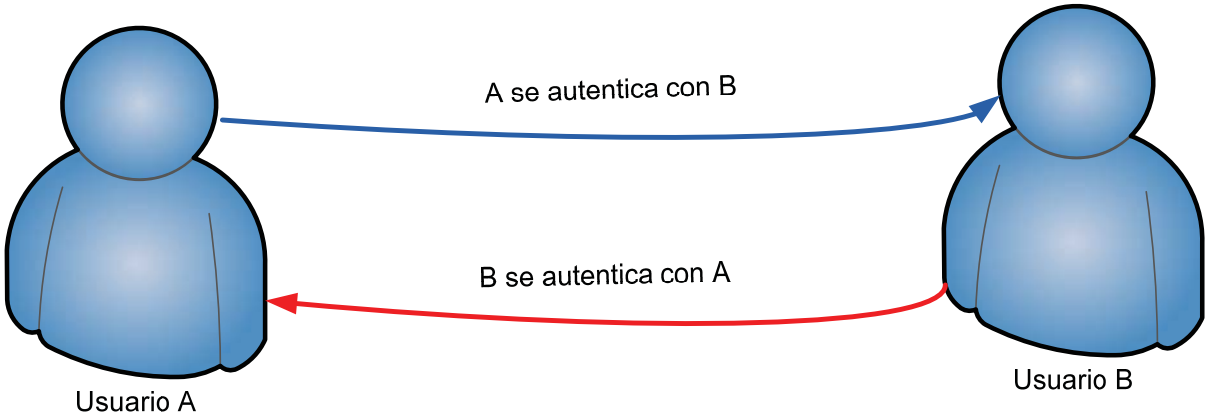

Figura 3. 15 Autenticación mutua.

c) Tercero confiable

En este esquema se autentican los usuarios y verifican la autenticidad de cada usuario con un tercero confiable, se implementa por medio de certificados digitales en su mayoría (figura 3.16).

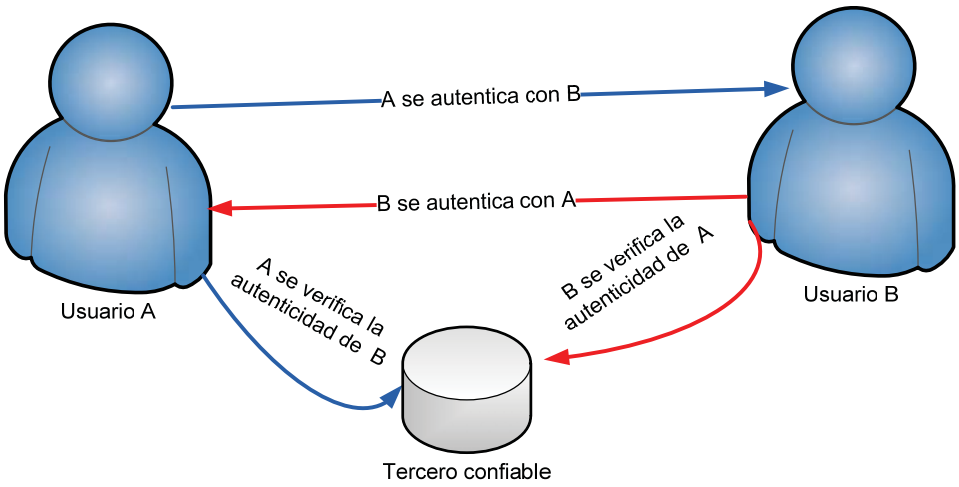

Figura 3. 16 Autenticación por medio de un tercero confiable.

3.4.4 Autorización

Una vez identificado y autenticado, la autorización es el siguiente paso en el control de acceso, los derechos de acceso que un usuario tiene en la red y sistemas deben ser establecidos.

Muchas computadoras, sistemas y redes emplean el concepto de permiso para controlar el acceso. Los permisos especifican qué operaciones diferentes pueden los usuarios realizar sobre algún objeto como archivo, puerto, servicio, proceso y por usuario un sistema, computadora, red, persona u objeto.

A todos los usuarios se les asigna un nivel de acceso a los directorios y archivos, todos los usuarios y archivos son asignados a un grupo, estos grupos pueden ser especificados en una ACL (Access Control List –listas de control de acceso), al momento de dar algún permiso sobre un grupo éste afecta a todos los objetos que lo forman, la mayoría de los sistemas determina por lo menos tres o cuatro niveles de permisos.

- ***Lectura**:* A un usuario final se le asigna este nivel, tanto para archivos o directorios de tal manera que sólo tiene la capacidad de ver el contenido de archivos y directorios, así como sus propiedades.
- ***Escritura**:* A un usuario final se le asigna este permiso sobre archivos o directorios para que tenga la capacidad de escribir o alterar un archivo, así como crear archivos y en algún caso también se otorgan permisos sobre algún directorio en particular.
- ***Ejecución**:* Este privilegio permite al usuario final la capacidad de realizar alguna tarea.
- ***Borrado**:* Este derecho de acceso permite al usuario final borrar archivos y directorios.

En la mayoría de los equipos de cómputo, sistemas operadores de redes, el acceso es dividido en tres niveles que dependen del grupo al que el usuario pertenece; propietario, grupo y acceso público (cada grupo tiene asignado niveles de acceso a los recursos), estos niveles se describen a continuación.

- ***Propietario***: Este grupo hace referencia a los propietarios del archivo o recurso, en virtud de aquel que lo ha creado o comienza a tenerlo tomando propiedad del recurso, usualmente tiene lectura, escritura y ejecución.
- ***Grupo**:* Este grupo se refiere a los usuarios que comparten una plantilla en común de permisos, como el hecho de tener el mismo puesto, trabajar en el mismo departamento, pertenecer a la misma institución, por ejemplo, todos los recursos humanos deberán tener una plantilla de grupo, posteriormente se genera un grupo que contemple todos los recursos humanos para finalmente asignarle permisos al grupo y éste a su vez afecte los permisos de todos los recursos humanos, como lectura, escritura, ejecución y borrado.
- ***Público**:* Este grupo hace referencia al nivel de acceso donde todos pueden acceder al recurso, dentro del sistema operativo de Windows este grupo se denomina Everybody-Todos, por razones de seguridad la mayoría de las veces a este grupo sólo se le dan permisos de lectura. Frecuentemente los recursos en una red como son impresoras o directorios compartidos, deberán ser limitados a los usuarios que pertenezcan al grupo público.

En cualquier sistema se debe de asegurar que el nivel de acceso que se determina a los grupos brinde sólo derecho a aquellas funciones que se requieran, se debe ser cuidadoso de los permisos de borrado que se otorgan al grupo público, por ejemplo, si se dan permisos de borrar al grupo público éste podrá borrar la impresora compartida de manera accidental o maliciosamente.

El control de acceso, los permisos y los grupos son conceptos importantes que se deben de entender, ya que son herramientas para el acceso de un usuario final hacia los recursos de un sistema. Cuando se emplea en conjunto efectivo los grupos y derechos de acceso puede ser una medida de seguridad

efectiva, desafortunadamente los permisos de acceso son frecuentemente ignorados y la asignación de grupos es usualmente la misma para todos los usuarios, como resultado los derechos de acceso a un sistema de archivos críticos permiten vulnerar el sistema o que sea comprometido.[30]

3.5 Seguridad física

Desde que el hombre ha tenido algo importante que proteger, ha encontrado varios métodos de asegurarlo. La seguridad física describe las medidas que previenen o detectan ataques de acceso a un recurso o información almacenado en un medio físico, la seguridad física es un factor muy importante para la seguridad informática.

Las acciones de seguridad que están involucradas con la seguridad física intentan proteger los activos de condiciones físicas como el clima, desastres naturales, medidas para proteger al personal, condiciones de temperatura recomendadas para mantener los equipos activos críticos y sistemas contra amenazas deliberadas o accidentales.

Actualmente existen EPS (Electronic Physical Security - Seguridad física electrónica), que incluyen detectores de fuego, sistemas de supresión de gas automáticos, circuitos cerrados, control de acceso por medio de smart card, biométricos o por RFID, detectores de intrusos, equipo de vigilancia y plan de vigilancia principalmente.

La seguridad física es un mecanismo empleado para proteger los activos, las medidas de seguridad física pueden ser:

- ***Físicas***; medidas tomadas para asegurar los activos, por ejemplo personal de seguridad.
- ***Técnicas***; medidas para asegurar servicios y elementos que soportan las tecnologías de la información, por ejemplo, seguridad en el cuarto de servidores.
- ***Operacionales***; medidas de seguridad comunes antes de ejecutar una operación, como es el análisis de amenazas sobre una actividad e implementar contramedidas apropiadas.

La seguridad física no es una tarea de una sola persona, en algunas organizaciones las personas encargadas de la seguridad física son también las encargadas de la seguridad de la información, las siguientes personas pueden ser los responsables de la seguridad en una organización.

- Oficial de seguridad de planta.
- Analista de sistemas de información.
- Jefe de información.
- Administrador de la red.

Algunos componentes que deben ser considerados en la seguridad física deben ser:

- Selección de un sitio seguro, su diseño y configuración.

[30] John E. Canavan, Fundamental of Network Security, Artech House 2001, pág. 109

- Asegurar la instalación contra acceso físico no autorizado.
- Asegurar los equipos e instalaciones contra robos dirigidos a ellos y a la información.
- Protección ambiental.
- Regla primordial: asegurar la vida humana.

La seguridad lógica en una organización no sirve de nada si no se ha contemplado la seguridad física, la necesidad de implementar seguridad física es considerada para:

- Prevenir un acceso no autorizado a sistemas de cómputo.
- Prevenir falsificar o robar datos de un sistema de cómputo así como equipos.
- Para proteger la integridad de los datos almacenados en las computadoras y equipos activos.
- Para prevenir la pérdida de datos y daño a los sistemas contra desastres naturales.

3.5.1 Factores que afectan la seguridad física

Los siguientes factores afectan la seguridad física de una organización en particular:

- ***Vandalismo**:* sólo con la finalidad de destruir los bienes.
- ***Robo**:* extracción del equipo de la organización para la obtención del bien propio, el bien de cómputo más robado al año sigue siendo los equipos portátiles, las compañías de medio a gran tamaño pierden en promedio 11.65 portátiles por año.[31]
- ***Desastres humanos*:** pueden ser provocados por personas internas o externas a la organización, generado incidentes como:
    - Amenazas de bomba.
    - Huelgas.
    - Plantones.
    - Empleados mal capacitados.
    - Disturbios sociales.
- ***Desastres naturales*:** fenómenos provocados por la naturaleza, éstos no se pueden estimar de forma exacta.
    - Inundaciones.
    - Temblores.
    - Climas extremos.
- ***Incendios***: provocados o accidentales.
- ***Agua***.
- ***Explosiones***.
- ***Ataques terroristas***.
- ***Fallas de alimentación***.
- ***Acceso no autorizado***.

[31] CEH módulo 21, versión 6, seguridad física.

- ***Tempest**:* Se refiere a (Transient Electro Magnetic Pulse Emanation Surveillance Technology – Tecnología de vigilancia para la emanación de pulsos electromagnéticos), cualquier aparato eléctrico emite radiación, con el equipo adecuado esta emanación se puede capturar y reproducir.

Se recomienda un *check List – listado de procedimiento*s, de las actividades y activos de una empresa, para determinar los activos que se deben de proteger, por ejemplo:

- ***Alrededores de la compañía***: la entrada a la compañía será restringida por medio de un mecanismo de control de acceso, además de contemplar medidas como vallas, muros, guardias y alarmas, cerraduras, sistemas detectores de intrusos, alarmas antirrobo, botones de pánico y sistemas de circuito cerrado principalmente.
- ***Recepción**:* el área de recepción se supone debe ser un espacio donde existe un mayor número de personas, el área de recepción puede ser protegida de las siguientes formas:
    - Archivos y documentos, dispositivos removibles entre otros, deberán permanecer en recepción.
    - No permitirá el acceso a personal no autorizado dentro de áreas administrativas.
    - Las pantallas de los equipos de cómputo deben ser posicionados de tal forma que las demás personas no puedan observar lo que muestra la pantalla en el escritorio de recepción.
    - Monitores, teclados y otros equipo en el escritorio de recepción, deberán ser bloqueados después de que él o la recepcionista deje de utilizar el equipo cierto tiempo.
- ***Servidores**:* tal vez el punto más importante de una red, deberá tener un alto nivel de seguridad, en un lugar seguro con clima adecuado, previniendo movimiento físico, evitar permitir iniciar los servidores de manera remota, deshabilitar el arranque de unidades extraíbles como USB, CD-ROM, floppy y en lo posible anular el hecho de tener estos dispositivos en los servidores.
- ***Área de trabajo**:* los empleados deberán ser educados acerca de la seguridad física, el área de trabajo puede ser asegurada por circuitos cerrados de TV, bloqueo de pantallas de PC, plantillas en el diseño de estaciones de trabajo y evitar dispositivos extraíbles.
- ***Redes inalámbricas**:* prevenir accesos no autorizados y colocar los equipos en lugares seguros, asegurándolos físicamente, verificar el tráfico de la red inalámbrica, cifrado punto a punto, autenticación personalizada,VPN.
- ***Equipos como switch, gateway, fax y dispositivos extraíbles**:* cada equipo deberá ser asegurado, las áreas cercanas a los equipos de recepción de fax deberá ser de acceso restringido, los faxes deberán ser archivados apropiadamente, dispositivos removibles no deberán ser colocados en lugares públicos.
- ***Control de acceso**:* Por medio de los cuatro factores utilizables algo que se es, algo que se sabe, algo que se tiene y ubicación.
- ***Intervención de línea telefónica**:* Permitir generar bitácoras de las llamadas realizadas lo cual permita rastrear y verificar la información transmitida por este medio.

- ***Accesos remotos**:* Delimitar los puntos permitidos para realizar accesos remotos hacia algún punto interno de la organización.

3.6. Mecanismos de monitoreo, de control y seguimiento

El monitoreo es una de las actividades que permite tener mejor acotada la seguridad de la organización debido a que permite observar los comportamientos normales y anormales en los sistemas. Los mecanismos que se emplean para monitorear varían con base en los requerimientos y alcances que planee dar la organización, dentro de éstos se encuentran bitácoras de acceso al sistema, tráfico de red, errores en los sistemas, límites de cuotas, intentos fallidos de sesión, etcétera.

Si se enfoca al monitoreo de la red de una organización los dispositivos que permiten realizar esta tarea son escogidos a partir de la propia arquitectura de red, por medio de puertos mirror, firewall, IDS, sniffer's, appliance, protocolos de monitoreo como SNMP, RMON principalmente, las características de cada uno de éstos es muy específica y la elección depende sólo de los responsables de la seguridad de la organización.

Muchos de los equipos activos en la actualidad permiten su administración y definición de servicios tanto de hardware, como de software, un ejemplo de estos son las diferentes maneras de administración por medio de TELNET, SSH, terminal, y Web, así como el manejo de protocolos como SNMP, RMON, redes virtuales y puertos espejo principalmente. El Puerto monitor o puerto espejo es una más de las prestaciones de algunos equipos, la cual permite transmitir el tráfico de un puerto específico del equipo, en otro puerto del mismo, esto con la finalidad de analizar el tráfico que pasa.

El alcance de los puertos monitores es demasiado, ya que permite analizar en tiempo real las conexiones de un equipo sin afectar el tráfico, así como colocar otro equipo que permita interpretar todo el tráfico que se está analizando, software que se puede emplear en equipos con estas características contemplan:

- Propósitos de diagnóstico.
- Análisis de tráfico: Identificar el tipo de aplicaciones que son más utilizadas.
- Flujo: conjunto de paquetes con la misma dirección IP origen y destino, mismo puerto y tipo de aplicación.
- Sniffer de todos los tipos.
- Appliance: Hardware con una funcionalidad dedicada, como los son los analizadores de tráfico, equipos de almacenamiento, servidores web, firewall, etcétera.
- Detectores de Intruso.
- Creación de bitácoras por hora, día, mes, etcétera.

Los mecanismos de control y seguimiento son utilizados en parte para determinar la integridad de la información y equipos, comportamiento, generación de estadísticas, tendencias así como registrar todos los eventos que se produzcan.

3.7 Firewall[32]

Surgieron como un primer mecanismo de protección perimetral de las redes y hosts, debido al incremento de las redes en los distintos ámbitos comerciales para protegerse de los ataques provenientes de otras redes.

Un firewall es un primer mecanismo de defensa perimetral a considerar en el momento que se desee implementar una red, sin embargo, sólo es una primera línea de defensa, actualmente se ha incrementado en gran escala el uso de estos mecanismos para protegerse de ciertos ataques y con ello reducir el riego en la red que se encuentra conectada a internet.

Un firewall es un sistema o conjunto de sistemas que permiten implementar políticas para el control de acceso entre dos redes, puede ser software o hardware, que permiten o niegan el paso de tráfico proveniente de una dirección IP a otra.

Dentro de él, se establecen reglas que permiten el acceso o salida de paquetes a la red, las reglas establecidas están directamente relacionadas con el tipo de datos que se permitirán dejar pasar a una red interna o salir de ella. En la figura 3.17 se muestra un esquema de un firewall básico, cuya función es permitir o bloquear el tráfico de datos de una red a otra, sin embargo, es importante mencionar que conforme ha pasado el tiempo, se han desarrollado una gran cantidad de variantes de firewalls con nuevas características.

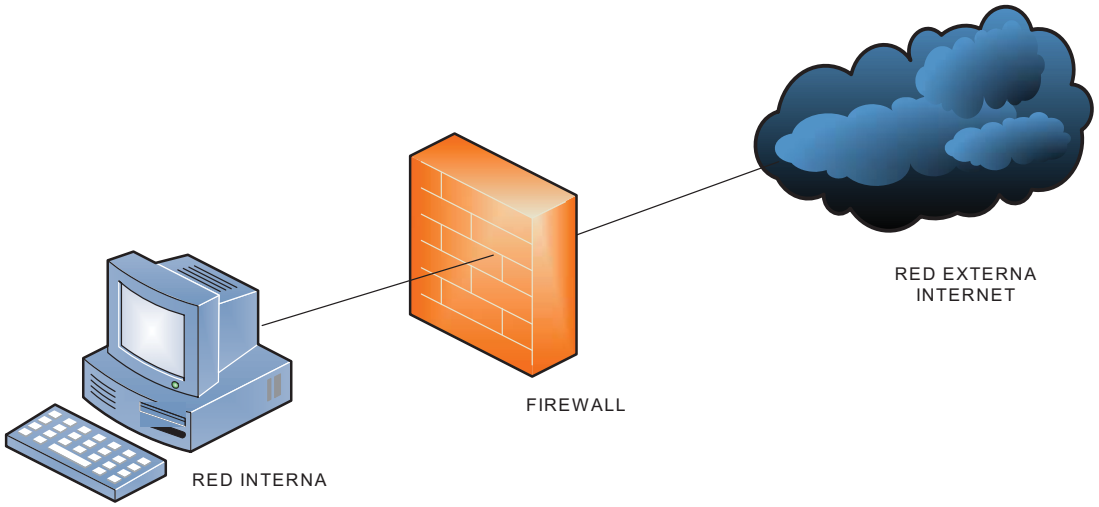

Figura 3. 17 Firewall.

Algunas ventajas que se obtienen al implementar un firewall son:

- Reducir riesgos, el camino para el intruso se vuelve complicado, aumentando con ello el grado de seguridad de la red.

[32] Para información más detallada ver apéndice C.

- En el momento que se instala un firewall se tiene mayor control, pues se crea un punto por donde fluye todo el tráfico entrante y saliente el cual puede ser analizado en caso de un posible ataque y con ello mitigar el ataque.
- Protección contra servicios vulnerables que pudiesen estar instalados y corriendo en algún servidor, los cuales pueden ser aprovechados por algún atacante para explotar alguna vulnerabilidad. Con el firewall se pueden evitar ciertos tipos de ataques a servicios como NFS Network File System- Sistema de archivos de red para entrar o salir de una red segura. También se pueden prever ataques basados en ataques de enrutamiento a través del protocolo ICMP. Un firewall puede rechazar todos los paquetes fuente y destino ICMP y a continuación informar a los administradores de los incidentes.
- Establecer un control de acceso por medio de direcciones IP.
- Concentrar la seguridad, implementar un firewall perimetral puede resultar menos costoso en la actualidad por la diversidad de mecanismos que tiene esta función, además de que se tiene concentrada la seguridad en un solo punto.
- Mayor privacidad, con el uso de firewall se puede evitar que los intrusos obtengan información a través de técnicas como fingerprinting, evitar obtener información acerca de los servidores DNS y con ello reducir la posibilidad de un ataque.
- Bitácoras sobre el uso de la red, así como uso indebido de la misma, las bitácoras son esenciales para cualquier administrador ya que pueden ser de gran utilidad para determinar los motivos de alguna falla o de un comportamiento anómalo del sistema, así como para deslindar responsabilidades.

Las estadísticas y bitácoras del uso de la red, permiten conocer el comportamiento común de la red y en caso de un posible ataque sirven como referencia para determinar las nuevas medidas a tomar, para evitar futuros ataques, así como futuros requerimientos para la red.

Se refuerzan las políticas del uso de la red, dado que un esquema de seguridad incluye políticas del uso de la red, el firewall ayuda a reforzar estas políticas restringiendo el uso de cierto software, restricción para visitar ciertos sitios, o cualquier otra política establecida ya que sin ello las políticas dependerían completamente de la cooperación de los usuarios.

Sin embargo, la implementación de un firewall también tiene limitantes entre las que destacan:

- Imposible evitar ataques que no pasen a través de éste, es decir, ataques internos.
- No es posible detectar ataques de personas que sustraigan información en cualquier tipo de dispositivo de almacenamiento, ataques de ingeniería social, tampoco puede garantizar la integridad de la información, además de que no puede proteger a un equipo de virus transportados en dispositivos de almacenamiento, tampoco es posible evitar ataques como wardriving, wireless hacking.

a) Firewall de red

Cuando se desea proteger cualquier red corporativa de posibles ataques provenientes de otras redes, uno de los puntos más importantes para los profesionales de la seguridad es elegir la opción más adecuada para dar solución al problema, por lo que se buscan estrategias de acuerdo con las necesidades, implementar un firewall para proteger la red es una opción, sin embargo, es un primer

mecanismo de todo un esquema de seguridad, existen distintas configuraciones y esto depende del grado de seguridad u objetivos de la organización.

Un firewall de red es un mecanismo utilizado como una barrera entre la red interna y el internet, por lo que un firewall de red protege a todo un conjunto de equipos dentro de un determinado perímetro, dado que las redes son interconectadas a través de routers, estos dispositivos generalmente cuentan con características de firewalls, también se pueden utilizar firewalls llamados Appliance-Dispositivos de Hardware integrados con software o cualquier otro equipo capaz de actuar como firewall.

Los firewalls de red, están pensados para entornos empresariales, con algunos cientos o miles de usuarios, los cuales pueden estar geográficamente dispersos, éstos pueden ser configurados en una sola etapa, además de que es posible generar múltiples reportes emitidos por estos mecanismos.

b) Firewalls de host

Un firewall de host también llamado firewall personal, es un tipo de software que se instala en cada equipo, el cual permite proteger un equipo de ataques provenientes de la red externa o de software instalado en el equipo que busque realizar alguna conexión hacia el exterior, aunque no ofrece grandes ventajas en cuanto a la administración se refiere, resulta ser de utilidad para evitar cierto tipo de ataques, la mayoría de los sistemas operativos cuentan con esta herramienta la cual es recomendable mantenerla activada.

Las funciones básicas de éstos, es funcionar como un monitor y lanzar alertas cuando algún programa intenta abrir algún puerto o intenta conectarse a Internet, además de los firewalls que ofrecen los sistemas operativos es posible instalar algunos otros gratuitos o comerciales, los cuales ofrecen mayores funcionalidades, existen varias soluciones de antivirus que ofrecen esta característica, sin embargo, se recomienda que sólo se encuentre activado uno solo para evitar conflictos.

A pesar de que una red cuente con un firewall para proteger los equipos que la integran no le es posible bloquear ataques locales, por lo que contar con un firewall personal reduce las posibilidades del atacante.

3.8 Auditoría, monitoreo y detección de intrusos

Aunque se cuente con todo un conjunto de mecanismos para garantizar un nivel de seguridad de la información, procesos como auditoría y monitoreo forman parte del ciclo de administración de la seguridad, dentro de los procesos de monitoreo es posible utilizar sistemas detectores de intrusos los cuales permiten detectar algún comportamiento fuera de la normalidad, la revisión continua de bitácoras, así como las auditorías de los sistemas juegan un papel primordial para determinar posibles anomalías y brindar opciones de mejora en el funcionamiento de cualquier sistema y con ello tomar nuevas medidas para mejorar.

Una auditoría está muy relacionada con el tipo de actividades que un usuario realiza, además verifica que no se estén violando el uso de ciertos recursos o cualquier actividad que esté relacionada con las políticas de la institución, monitorear actividades que se consideren críticas permiten determinar medidas a tomar para mejorar las medidas de seguridad incluyendo cambios en las políticas.

Los sistemas detectores de intrusos son un mecanismo de defensa utilizados para determinar posibles ataques, aun contando con firewalls que bloquean cierto tipo de flujo de datos, no siempre se puede garantizar que éstos estén funcionando como se espera, cuando no es posible bloquear cierto tipo de tráfico y éste logra entrar a la red, el sistema detector de intrusos lanza una alarma indicando alguna anomalía alojando esta información en bitácoras o a través de la generación de reportes específicos.

a) Auditoría

Auditoría 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 cumple las condiciones que le han sido prescritas. [33]

La auditoría informática, la cual tiene como objetivo el análisis de sistemas informáticos, planes de contingencia, su finalidad es determinar la eficiencia de acuerdo con las normas establecidas, se divide en dos grupos principalmente cualitativos y cuantitativos.

Las auditorías cuantitativas tienen como objetivo principal generar listas de todos los riegos posibles los cuales son comparados con datos numéricos y modelos matemáticos para estimar la probabilidad de ocurrencia de un evento que se extrae de un riesgo de incidencias, aunque este tipo de auditorías en la práctica terminan aplicándose de manera subjetiva.

Las metodologías cualitativas también conocidas como subjetivas están basadas en métodos estadísticos y lógica difusa humana, se apoya en personas con experiencia en el área. Es posible realizar auditorías de controles generales basadas en estándares internacionales y de metodologías de auditores internos.

Durante los procesos de auditorías se requiere de un plan a seguir, una vez finalizada la auditoría se presenta el informe con las debilidades encontradas y las recomendaciones adecuadas para tomar nuevas medidas, por lo que requiere que este proceso sea realizado por algún experto en el área.

Dentro de un plan de auditoría se contemplan funciones como tipo de auditoría, completa o correctiva, por lo que un esquema de seguridad incluye el proceso de auditorías para ver si éste cumple con los objetivos establecidos y con ello determinar las nuevas medidas a tomar para corregir los posibles fallos.

Existen modelos para realizar auditorías como Control Objectives for Information Systems and related Technology - Objetivos de Control para Tecnología de Información y Tecnologías

[33] **G**OVERNANCE, **C**ONTROL *and* **A**UDIT *for* **I**NFORMATION *and* **R**ELATED **T**ECHNOLOGY

relacionadas (COBIT), que permite auditar la gestión y control de los sistemas de información, en éste se incluyen todos los sectores de una organización, recursos humanos, sistemas, así como instalaciones.

b) Sistema detector de intrusos.[34]

Anteriormente se describió de manera muy general en qué consiste un sistema detector de intrusos, un IDS no es más que una herramienta capaz de leer e interpretar las bitácoras de dispositivos como firewalls, servidores, routers y otros dispositivos de red.

De manera más específica, un IDS cuenta con una base de datos con los ataques más comunes que utiliza para comparar con el tráfico que circula a través de la red, los sistemas detectores pueden tomar distintas medidas dependiendo de su configuración o alcance del mismo desde lanzar una alerta o incluso tomar medidas de manera automática como eliminar conexiones, emisión de alertas, además de registrar bitácoras para un posterior análisis.

En general, la detección de intrusos permite ubicar el uso no autorizado, indebido o ataques contra la red, de manera semejante a los firewalls, un IDS puede estar basado en solo software o una combinación de hardware y software pre configurado, los IDS por software pueden funcionar instalados en un mismo dispositivo.

Los IDS pueden presentar dos tipos de respuesta pasiva y activa, cuando sólo se lanza una alerta de anomalías o mal uso está actuando de manera pasiva, sin embargo, cuando además de lanzar una alerta toma otras medidas como mitigar el ataque, se dice que actúa de manera activa.

Un sistema detector de intrusos puede ser utilizado para detectar intentos de ingreso a los sistemas, monitoreo de actividades anormales, monitoreo de acceso a bases de datos, monitorear servicios así como proteger a éstos.

En la figura 3.18 se muestra el funcionamiento de un sistema de detección de intrusos.

[34] Para información más detallada ver apéndice C.

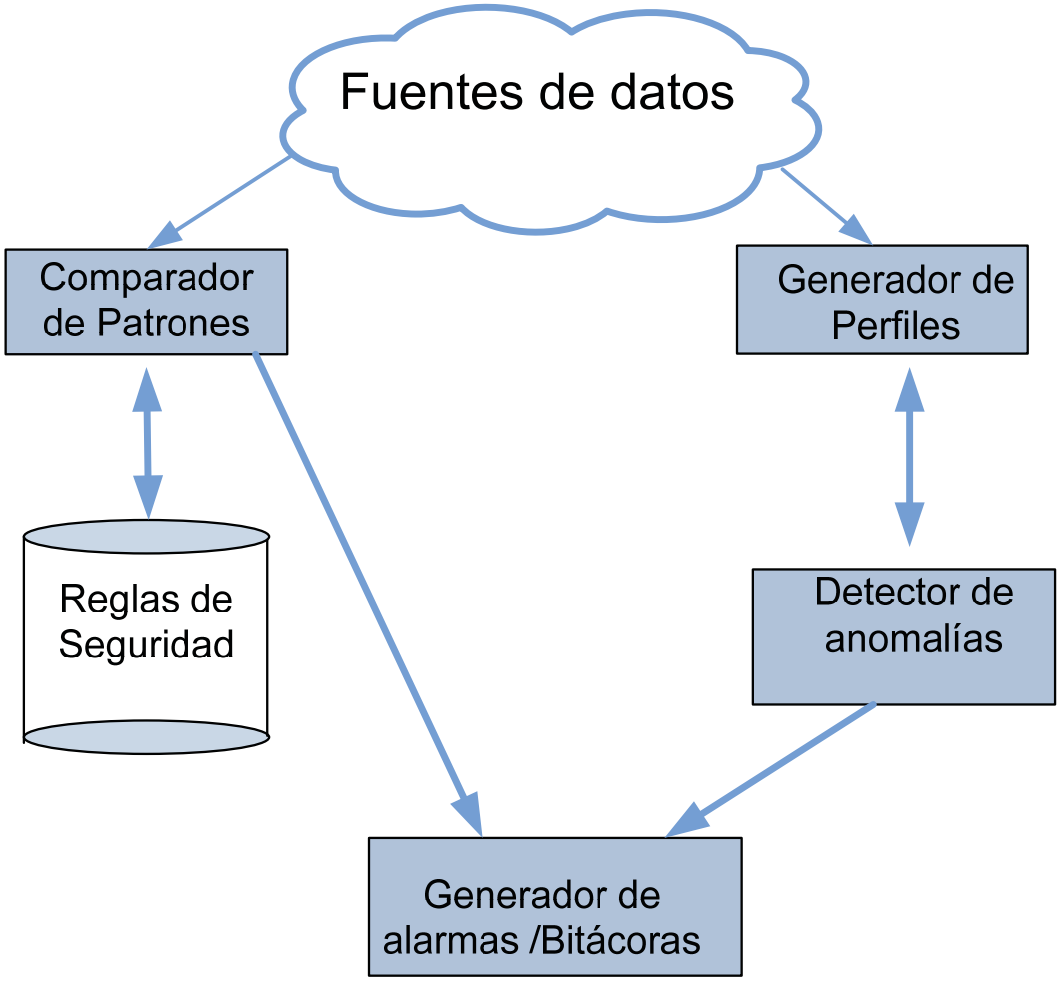

Figura 3. 18 Esquema general de un Sistema Detector de Intrusos.

3.9. Seguridad en redes inalámbricas

En los últimos años se ha incrementado el uso de las redes inalámbricas a pesar de las limitaciones en cuanto a velocidad se refiere, sin embargo, ofrece otras ventajas como son movilidad y la facilidad de implementación, además de que la tendencia del uso de dispositivos móviles aumenta cada día, por tal razón conocer las debilidades de éstas, así como la forma de protegerse en la actualidad es de gran importancia.

El objetivo principal de este tema es identificar amenazas y vulnerabilidades que puedan afectar las redes WiFi (Wireless Fidelity – Fidelidad Inalámbrica), para poder establecer mecanismos de seguridad que permitan la continuidad y minimizar el impacto de incidentes de seguridad.

Las redes inalámbricas poseen debilidades inherentes, debido a su naturaleza de diseño y funcionamiento.

- Una WLAN (Wireless Local Area Network – Red inalámbrica de área local) utiliza una serie de componentes físicos, incluyendo los puntos de acceso, cables que conectan a la red los

puntos de acceso, antenas, adaptadores inalámbricos y software, los daños a estos componentes podrían reducir la intensidad de las señales, limitar el área de cobertura o reducir el ancho de banda, poniendo en cuestión la capacidad de los usuarios para acceder a los datos y a los servicios de información.

- El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere, cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica, en el estándar 802.11g, claro que la distancia depende del estándar utilizado.
- Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la cualquier institución, la mala configuración de un punto de acceso inalámbrico es muy común, actualmente muchos de los puntos de acceso sólo se instalan con la configuración que traen de fábrica lo que los hace muy vulnerables.

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible, esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.
- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Contemplando las redes inalámbricas como un medio de transmisión de datos, se plantearon medidas que garantizaran cubrir las debilidades de este medio, tomando en cuenta la autenticación y confidencialidad, los mecanismos utilizados en mayor parte en la actualidad son WEP, WPA, WPA2, RADIUS, TACACS y Hotspot principalmente.

a) WEP

El algoritmo WEP (Wired Equivalent Privacy – Privacidad equivalente a cableado), forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel dos del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas. El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro:

- La mayoría de las instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, de manera automática), esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.

- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen actualmente diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP, el primer programa que hizo esto posible fue WEP Crack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

b) WPA

WPA (Wi-Fi Protected Access –Acceso inalámbrico protegido), es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporal Key Integrity Protocol – Protocolo de integridad de clave temporal). Este protocolo se encarga de cambiar la clave compartida entre el punto de acceso y el cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs – Vectores de iniciación de cifrado, con respecto a WEP. El mecanismo de autenticación usado en WPA emplea 802.1x y EAP.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

1. **Modalidad de red empresarial:** Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red, el punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las llaves compartidas que se usarán para cifrar los datos.

2. **Modalidad de red casera, o PSK (Pre-Shared Key – Clave pre compartida):** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas, debido a que ya se ha comprobado que WPA es vulnerable a ataques de diccionario.

c) WPA2

WPA2 es el nombre que recibe el estándar 802.11i, el cual fue adoptado en junio del 2004, introdujo varios cambios fundamentales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de redes corporativas.

La nueva arquitectura para las redes wireless se llama RSN (Robust Security Network – Red de seguridad robusta) y utiliza autenticación 802.1X, distribución de claves robustas y nuevos mecanismos de integridad y privacidad. Además de tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica.

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas.

La autenticación 802.1X para WLAN se basa en tres componentes principales:

- El solicitante (generalmente el software cliente).
- El autenticador (el punto de acceso).
- El servidor de autenticación remota (por lo general, pero no necesariamente, un servidor RADIUS - Remote Authentication Dial-In User Service).

El estándar 802.11i hace pequeñas modificaciones a IEEE 802.1X para que las redes inalámbricas estén protegidas frente al robo de identidades. La autenticación de mensajes se ha incorporado para asegurarse de que tanto el solicitante, como el autenticador calculen sus claves secretas y activen el cifrado antes de acceder a la red.

d) Hotspot

Hotspot es un mecanismo alternativa utilizada para asegurar redes cableadas e inalámbricas, ofrece ventajas ya que permite utilizar cuentas de usuarios personalizadas, es decir, cada usuario que desee tener acceso a la red pública deberá de autenticarse, empleando RADIUS para esta tarea.

Cuando se desea garantizar un nivel de seguridad mayor, lo conveniente es contar con una lista de control de acceso en la cual se mantienen las cuentas y contraseñas de los usuarios que pueden hacer uso de la red, a través de la implementación de este esquema es posible tener un mejor control sobre los usuarios que tienen acceso a la red, permitiendo la navegación libre a sitios definidos.

Es posible contar con distintos esquemas, cada usuario que requiera conectarse a internet deberá de autenticarse con el punto de acceso haciendo uso de WEP, WAP, WAP2 y posteriormente con un Hotspot en el cual se encuentran almacenadas las cuentas de usuario y contraseñas.

En caso de que el punto de acceso no solicite un llave WEP, WPA, WPA2 la autenticación estará a cargo del Hotspot, por lo que esta arquitectura ofrece mayores beneficios con respecto a la autenticación que ofrece un AP, ya que la clave que se maneja para este caso es compartida para todos los usuarios, con el uso de un Hotspot es posible tener un control acerca de los usuarios específicos que hacen uso de la red y llevar un seguimiento de sus actividades (figura 3.19).

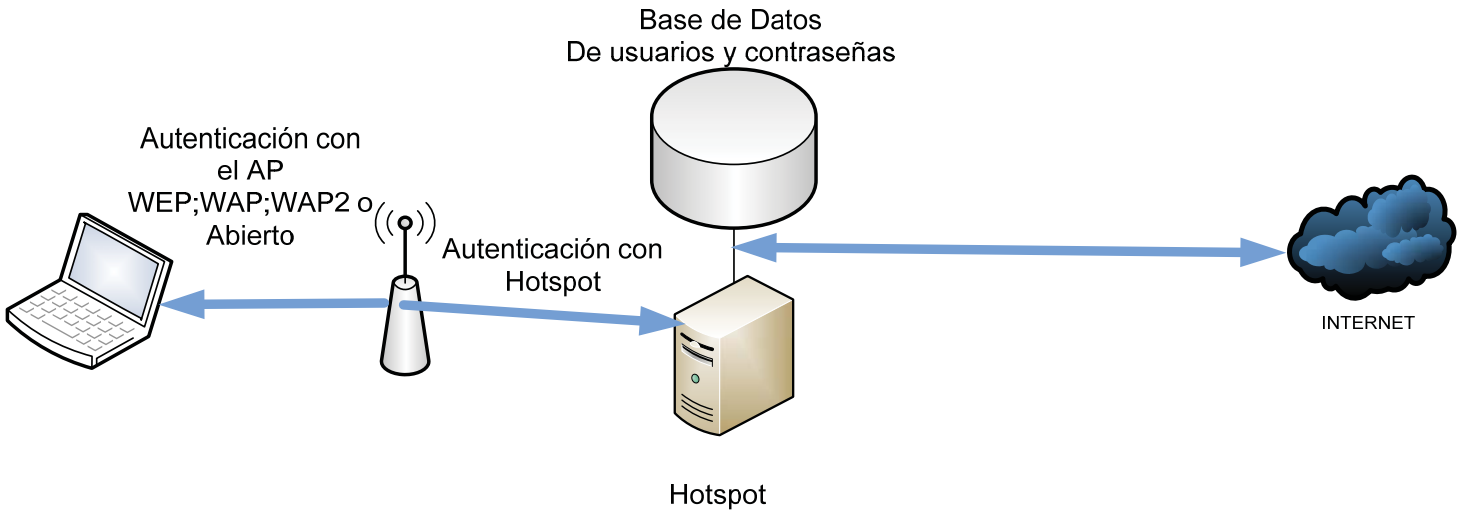

Figura 3. 19 Hotspot.

3.10. Sensores y herramientas

Implementar un esquema de seguridad requiere de varias herramientas basadas en software o una combinación de software y hardware, las cuales pueden ser comerciales o de código abierto, el uso de sensores permite conocer el comportamiento del uso de la red, y con ello determinar si se está haciendo un uso adecuado de la misma.

Existen una gran cantidad de herramientas útiles para llevar a cabo este tipo de actividades, a continuación sólo se describen algunas de estas herramientas de manera general:

a) Snort

Snort es un sistema detector de intrusos basado en red NIDS, desarrollado por Martin Roesch, se ha convertido en una herramienta indispensable tanto en medianas como grandes instituciones, ya que es una herramienta de gran utilidad, es posible configurarla para que ésta lance alertas en tiempo real, considerado un NIDS ligero y potente, pero ello no le resta funcionalidades, el análisis de paquetes y la generación de bitácoras forman parte de este IDS.

Esta herramienta puede ser utilizada en tres formas diferentes:

- Sniffer.
- Generador de bitácoras.
- NIDS.

Esta herramienta puede ser complementada con algún visualizador gráfico para hacer más amigable la administración.

b) Cacti

Herramienta de software libre, funciona como un sensor, la cual permite obtener información del comportamiento de la red, como conexiones, puertos más utilizados de manera gráfica, estado de los puerto en un equipo, consulta de manera remota, entre otros, todos los datos que se pueden visualizar con el uso de esta herramienta son obtenidos a través del protocolo SNMP.

Otra ventaja que ofrece es el hecho de poder manejar un control de acceso, con lo cual se asignan privilegios para visualizar información.

c) Nagios

Es un sistema de código abierto para la monitorización de redes el cual se ha convertido en una herramienta muy utilizada para administrar la red. Monitorea servidores y servicios que le sean especificados notificando los cambios que se hayan producido en los dispositivos. El nombre inicial de este proyecto fue Netsaint el cual fue creado por Ethan Galstad y hasta la fecha él y otro grupo de desarrolladores mantiene este proyecto activo. Fue diseñado originalmente para sistemas Linux, pero también es usado en variantes de tipo Unix. Tiene licencia GNU publicada por la Free Software Fundation.

Otra característica que ofrece es la posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles. Notifica vía correo electrónico, mensajes de texto SMS, o cualquier otro método definido por el usuario a un grupo de contactos cuando ocurre un problema con un servicio o en un host.

d) Ntop

Ntop es otra herramienta de código abierto utilizada para monitorear la red en tiempo real, así como el uso de recursos de diferentes aplicaciones, la eficiencia de esta herramienta permite además detectar si algún equipo se encuentra mal configurado, también tiene la capacidad de detectar problemas de seguridad, simplificando la tarea al administrador.

Otras características interesantes y de gran utilidad para optimizar la red, Ntop tiene la capacidad de realizar escaneos pasivos con la finalidad de identificar routers, servidores, conocer la distribución de tráfico, obtener características de equipos (Host Fingerprint), conocer el estado de los equipos, estadísticas particulares de cada equipo, también es posible monitorear voz sobre IP.

e) Herramientas útiles para el monitoreo.

Hasta el momento se ha comentado del uso de herramientas para monitorear las actividades de los equipos que integran una red, con la finalidad de corregir y mejorar la calidad del servicio.

Además de las herramientas antes mencionadas, es posible utilizar otras que ofrecen menos funcionalidades pero que permiten determinar fallos en los sistemas o posibles errores de configuración, Tabla 3.2.

Tabla 3. 2 Herramientas útiles para el monitoreo.

Herramienta	Características	Distribución
NMAP	Herramienta para explorar la red útil para auditorías de seguridad. Determina puertos abiertos. Sistemas operativos utilizados entre otras características. Es una herramienta portable, de gran utilidad y bien documentada. Disponible para diferentes sistemas operativos.	Software libre.
Nessus	Utilizada para determinar vulnerabilidades en sistema Unix. Durante un tiempo fue una herramienta gratuita y de código abierto. Disponible para Linux y Windows.	En la actualidad tiene un costo aproximado de $1200 por año.
Wireshark	Antes denominada Ethereal. Es una potente herramienta utilizada para analizar protocolos de red. Disponible para Windows y Unix. Es posible utilizarse desde la línea de comando o a través de una interfaz gráfica.	Software libre.
Netcat	Intérprete de comandos y con una sintaxis muy sencilla abrir puertos TCP/UDP en un equipo.	Software libre.
Superscan	Permite determinar puertos abiertos. Permite ejecutar comandos ping , traceroute y whois.	Versión gratuita.
Hping2	Útil para realizar pruebas a los firewalls. Realizar escaneo avanzado de puertos.	Versión gratuita.

3.11. Seguridad en equipos finales

La seguridad en equipos finales implica asegurar de manera lógica y física cada componente que forma parte de la red, ya que no tendría impacto contar con un esquema robusto para garantizar la seguridad si dichos dispositivos no cuentan con una configuración adecuada.

El concepto Hardening – fortalecimiento, se utiliza para referirse al aseguramiento de los equipos, el fortalecimiento de cada componente de la red implica evitar utilizar configuraciones que los dispositivos traen por default, dispositivos como switches, AP, routers, hosts, entre otros, muchos de estos equipos son administrables remotamente por lo que si éstos no se configuran adecuadamente pueden ser una puerta de entrada para los intrusos, contar con las especificaciones de los distintos equipos para conocer la manera de operar es recomendable ya que esto permite conocer características y alcance del mismo, además de mantenerlos actualizados y en revisión constante.

3.11.1 Actividades de fortalecimiento

Cada dispositivo que integra la red deberá de asegurarse de acuerdo con la funcionalidad que éste desempeña dentro de la infraestructura, a pesar de que no existe una guía como tal para el fortalecimiento de cada equipo, los principios básicos de aseguramiento prácticamente son los mismos y se deben de adecuar a los servicios que se ofrecen y a las políticas establecidas.

El proceso de aseguramiento entre un sistema y otro se rige bajo los mismos principios, por lo que sólo será necesario conocer el sistema y las características específicas de cada uno para asegurar cuestiones particulares de cada uno, algunas de las recomendaciones para asegurar hosts son las siguientes:

- Remover o desinstalar programas o componentes innecesarios, si no existe la necesidad de tener programas que no son utilizados y debido a esto no se actualizan constantemente pueden ser un riesgo para el equipo, varios sistemas operativos ofrecen esta facilidad, de elegir lo mínimo para su funcionamiento, los sistemas Unix y Microsoft, ofrecen la posibilidad de instalar sólo características necesarias permitiendo al usuario elegir esos componentes.
- Eliminar servicios de red innecesarios, los cuales generalmente abren puertos que un atacante podría aprovechar para vulnerar el sistema.
- Los servicios compartidos son otro punto a considerar, si no existe la necesidad de compartir impresoras o archivo sería adecuado deshabilitar este servicio.
- Los accesos a servicios remotos a considerar, ya que esto le facilita la tarea al atacante para poder entrar al sistema, el sistema operativo Windows ofrece el servicio de escritorio remoto aunque es necesario autenticarse si éste no es necesario es conveniente se mantenga deshabilitado.
- Las plataformas UNIX también implementan servicios remotos como telnet que permiten ejecutar comandos, por lo que es necesario deshabilitarlo puesto que las comunicaciones viajan en claro, y en su lugar es posible instalar SSH que es un servicio que garantiza confidencialidad en sus comunicaciones.
- También es posible aceptar o negar la comunicación de direcciones IP específicas a través de la configuración de los archivo *host.deny* y *host.allow* de los sistemas operativos Unix.
- Los servicios instalados como SSH también es necesario asegurarlos para evitar brechas de seguridad, en general cualquier servicio que sea instalado será necesario que éste sea configurado y no dejarlo con la configuración por defecto.
- Evitar fuga de información a través de las sesiones nulas, deshabilitar cuentas de usuarios que no tengan establecida alguna contraseña, para evitar que tengan acceso al sistema y puedan obtener información que permita escalar privilegios o información que pueda ser de utilidad.
- En los servidores Windows NT y 2000 el usuario anónimo era comúnmente aprovechado para obtener información de recursos compartidos y grupos, a partir de versiones 2003 y posteriores esta cuenta de usuario se encuentra bloqueada aunque para versiones anteriores a 2003 existen actualizaciones que evitan esta funcionalidad.

- Limitar el acceso a los datos o archivos de configuración modificando los permisos y dueño de los mismos, con esto se está protegiendo información crítica, en caso de que algún intruso logre entrar con alguna cuenta con privilegios mínimos esto evitará perder información importante.
- Aún existen sistemas funcionando bajo el sistema de archivos FAT32 el cual no maneja permisos en los archivos, pero por otro lado a partir de NTFS ya es posible manejarlos.
- Mantener una administración adecuada de cuentas de usuarios en los sistemas operativos, ya que en ocasiones existen cuentas que no son utilizadas y que además las contraseñas son débiles o nulas, lo conveniente es eliminar estas cuentas para disminuir el riesgo de que algún intruso pueda sacar provecho de las mismas.
- Verificar que las cuentas de los usuarios posean contraseñas robustas para evitar que éstas sean obtenidas a través de fuerza bruta o ataques de diccionario, crear conciencia en el usuario final de la responsabilidad de su contraseña y los problemas que implicaría si éste no toma en cuenta las recomendaciones dadas.
- Realizar auditorías para determinar si las contraseñas son lo suficientemente robustas, de gran utilidad para reforzar la seguridad en las mismas, llevar a cabo recomendaciones para evitar que los usuarios utilicen contraseñas débiles, además de que éstas deberán cambiarse periódicamente.
- Un manejo de grupos para establecer las restricciones adecuadas a cada grupo permite llevar un mejor control de asignación de privilegios.
- Análisis periódico de bitácoras de los servicios instalados, así como del mismo sistema operativo permite determinar las causas de fallas, y con ello establecer y realizar mejoras en las soluciones por lo que son realmente importantes, en caso de un incidente son una buena evidencia para determinar las causas o actividades realizadas.
- Uso de firewalls personales, antivirus, es otra medida que se debe tomar, además de que éstos se deben mantener actualizados.
- Actualizaciones tanto a los sistemas operativos y cualquier otro servicio instalado, permite cubrir posibles fallos de seguridad, con ello se evitará que los intrusos aprovechen debilidades y hagan mal uso de las mismas.

Switches y routers son dispositivos que también deben asegurarse, sin embargo, en esta sección se dan recomendaciones generales debido a que esto dependerá de las características que cada dispositivo cuente por lo que en este caso se recomienda contar con las especificaciones de cada dispositivo.

- Actualizar el firmware de los dispositivos esto permite manejar nuevas características de administración y seguridad generalmente.
- Establecer contraseñas robustas para el acceso de los dispositivos, además de cambiarla periódicamente.
- Limitar los accesos remotos si éstos no son necesarios.
- Limitar los accesos locales.

- Verificar que los dispositivos funcionen como se espera, esto es, verificar que las configuraciones establecidas funcionen de manera adecuada.
- Eliminar servicios innecesarios.
- Habilitar contraseñas robustas en todas las interfaces.
- Limitar las capacidades de administración a través de cuentas con privilegio mínimos.
- Realizar auditoría para detectar fallas de configuración.
- Verificar que los dispositivos estén ubicados en lugares adecuados y seguros físicamente.
- Mantener en un lugar seguro de fácil acceso para los administradores las guías de configuración de los equipos.

A pesar de que se podría enumerar una gran cantidad de consideraciones a realizar, en este tema se hizo mención de las principales actividades a tomar en cuenta para asegurar los equipos que integran la red.

3.12. Estándares internacionales

A pesar de que no existe una guía específica la cual se deba seguir fielmente para implementar algún esquema de seguridad en redes debido a que las necesidades para cada institución o empresa son distintas, sin embargo, existen estándares internacionales a seguir además de recomendaciones de organizaciones expertas en el área de seguridad.

Organizaciones como National Institute of Standards and Technology –Instituto Nacional de Estándares y Tecnología (NIST) e International Organization for Standardization –Organización Internacional para la Estandarización (ISO) cuentan con documentos realizados y analizados por expertos en el área.

Por ejemplo, la norma BS 7799 se refiere al sistema de administración de la seguridad de la información- Information Security Management System, (ISMS) en la cual se contemplan los aspectos que cada institución debería cubrir para garantizar la seguridad. Algunos de los puntos que se toman en cuenta son:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de continuidad del negocio
- Verificación de su cumplimiento.

NIST maneja sus propios estándares y recomendaciones, cabe aclarar que no sólo se enfocan al área de las tecnologías de la información, sino a todo lo relacionado con la tecnología, por mencionar algunas de los estándares y recomendaciones que maneja se encuentran Computer Security Incident Handling –Guía de seguridad en cómputo y manejo de respuesta a incidentes, publicada en el año

2004, en la cual se detallan recomendaciones a seguir para la respuesta a incidentes, políticas y procedimientos, así como del manejo de los tipos de incidentes.

Los estándares y recomendaciones tienen como objetivo garantizar calidad, donde las instituciones pueden contar con un punto de referencia para identificar las necesidades y problemas de seguridad en las que éstas pueden verse involucradas. El uso de estándares de manera continua permite obtener beneficios para las organizaciones.

NIST ofrece estos documentos de forma gratuita, y pueden ser descargados directamente desde su página, por otro lado, la serie ISO también puede ser descargada con un costo.

a) Serie ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO 27000 es una lista de estándares, en la cual se manejan ciertos rangos que van desde 27000 a 27019 y de 27030 a 27044, entre los que destacan ISO 27001, estándar cuyo objetivo es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

En este estándar se hace referencia sobre la importancia de:

- Entender los requerimientos de la seguridad de la información de una organización.
- Implementar y operar controles para manejar los riesgos de la seguridad, 133 controles generales de seguridad definidos, 11 áreas referidas a la seguridad física, ambiental y de los recursos humanos.
- Monitorear y revisar el desempeño y la efectividad del SGSI.

b) Recomendaciones NIST serie 800

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de incrementar la productividad, facilitar el comercio, mejorar la calidad de vida.[35]
La serie 800 del NIST es un conjunto de documentos de interés general sobre Seguridad de la Información. Estas publicaciones comenzaron en 1990 y son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad. La serie 800 incluye una lista de documentos que pueden ser descargados de manera gratuita desde el sitio oficial.
NIST SP800-53 Recommended Security Controls for Federal Information Systems – controles de seguridad recomendados para sistemas de información federal, en éste se especifican los controles necesarios para la protección de los sistemas de información entre los que se encuentran:

[35] Special Publications (800 Series), http://csrc.nist.gov/publications/PubsSPs.html

- Control de acceso.
- Concientización y entrenamiento.
- Responsabilidad y Auditoría.
- Administración de la seguridad.
- Planes de contingencia.
- Identificación y autenticación.
- Respuesta a incidentes.
- Mantenimiento.

c) Suite B de criptografía. [36]

La evolución de los equipos en cuanto a procesamiento se refiere ha permitido romper algoritmos criptográficos, por lo que ha dado lugar al surgimiento de algoritmos criptográficos denominados suite B de NSA National Security Agency - Agencia nacional de seguridad, anunciados el 16 de febrero del 2005, los cuales incluyen los siguientes grupos :

Tabla 3. 3 Suite B criptografía.

Servicio	Mecanismo
Cifrado	Advanced Encryption Standard - Estándar de Cifrado Avanzado (AES) - FIPS 197
Firma digital	Elliptic Curve Digital Signature Algorithm- Algoritmo de Firma Digital con Curvas Elípticas - FIPS 186-2
Intercambío de claves	Elliptic Curve Diffie-Hellman – Curvas Elípticas Diffie-Hellman
HASH	Secure Hash Algorithm – algoritmo De Hash Seguro - FIPS 180-2

Dentro de la suite B se especifica el ámbito de aplicación de dichos algoritmos criptográficos, los cuales pueden ser utilizados en software, hardware o firmware, en requerimientos asociados al gobierno de los Estados Unidos, aplicable tanto nacional como internacionalmente.

La base de los sistemas criptográficos son las matemáticas, puesto que es un problema que se considera difícil de resolver computacionalmente hablando.

El estudio de los distintos algoritmos criptográficos como ECC (por sus siglas en inglés Criptografía con Curvas Elípticas), ha permitido comprobar su robustez e incluso es un estándar que maneja ISO éste también requiere menos poder de cómputo para su procesamiento ofreciendo la misma robustez que RSA- sistema criptográfico con clave pública.

[36] NSA Suite B Cryptography, NSA, nov 8 2010 http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

3.13. Políticas de seguridad

Las políticas de seguridad son implementadas como medios para apoyar los controles y mecanismos empleados, cuando el alcance de éstos no permite cubrir todos los aspectos de seguridad considerados. Permiten definir lineamientos para establecer un límite entre lo que está permitido hacer a los usuarios dentro de la institución y fuera de ella. Las políticas de seguridad establecen el canal formal de actuación del personal en relación con los recursos y servicios informáticos, importantes de la organización.

La definición de política de seguridad enfocada para entornos de cómputo, es la descripción bajo la forma de regla, en las que se incluyan propiedades de confidencialidad, integridad y disponibilidad, en la medida requerida por una organización, se le conoce como política de seguridad.

Dentro de las organizaciones se debe determinar una figura encargada de regir las políticas de seguridad, el cual será el responsable de mantener actualizadas las políticas, estándares, procedimientos y los controles para garantizar la protección de los activos de la organización.

Las políticas de seguridad deben considerar entre otros, los siguientes elementos:

- Los activos o bienes involucrados.
- Alcance de la política; incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivo de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidad de los usuarios con respecto a la información a la que ella tiene acceso.

En las políticas de seguridad se definen posturas, las cuales determinan la forma que se empleará para determinar las reglas, son divididas en permisivas y prohibitivas. La postura permisiva permite todo excepto lo que está expresamente prohibido y la prohibitiva prohíbe todo excepto lo que está expresamente permitido. Evidentemente la segunda postura es mucho mejor ya que sólo se permite aquello que es necesario, es decir, las actividades que se pueden realizar y el resto serán consideradas ilegales.

Al momento de redactar las políticas es indispensable elegir una de las dos posturas, pero debe quedar claramente definido qué postura es la que se utilizará, ya que no se deben combinar posturas, esto con la finalidad de evitar confusiones.

Adicional a la filosofía elegida, existen principios fundamentales de una política de seguridad, que deben ser contemplados:

- **Responsabilidad individual**: las personas son responsables de sus actos.
- **Autorización**: reglas explícitas acerca de quién y de qué manera se utilizan los recursos.

- **Mínimo privilegio**: Sólo otorgar los permisos necesarios para que realice su tarea cada individuo.
- **Separación de obligaciones**; las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad y función.
- **Auditoría**: El trabajo y los resultados deben monitorearse durante su inicio y hasta después de ser terminados.
- **Redundancia**: Redundancia al implementar respaldo, conexiones redundantes, sistemas de emergencia, etcétera.
- **Reducción de riesgos**: reducir el riesgo a un nivel aceptable.

El propósito de las políticas busca reforzar en todos los aspectos de seguridad, aquellos huecos o puntos débiles que se deben considerar con el fin de brindar una seguridad integral en la institución.

Se contemplan políticas de:

- Comportamiento.
- Integridad.
- Uso.
- Seguridad física.
- De cuentas de usuario.
- Administradores.
- Trabajadores en general.
- Seguridad lógica.
- Políticas de respaldo.
- Políticas de correo.

Se definen también responsabilidades (determinar qué individuo de una organización es responsable directo en cuanto a los recursos de cómputo e información) y separación de tareas (indica la participación de dos mecanismos que trabajan de forma coordinada para realizar un proceso específico).

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización, responden a intereses y necesidades organizacionales basadas en la visión del negocio que lleve un esfuerzo conjunto de sus actores por administrar sus recursos.

Cuando se definen políticas de seguridad se debe contemplar un ciclo de vida, éste consta de cuatro procesos:

- Definición de la política: especificar una regla que busque cubrir un punto débil el cual no fue cubierto por un control o busca reforzar el alcance de un control.
- Implementación de la política: Presentar por escrito a las diferentes áreas el documento de políticas de seguridad con la finalidad de que lo conozcan y pongan en práctica.
- Verificación de su cumplimiento: deben existir personas responsables de cumplir y hacer cumplir el reglamento.
- Revocación de la política: las políticas de seguridad requieren revisiones continuas con la finalidad de afinar su alcance y adaptarlos a los ambientes y tiempos actuales.

El alcance de las políticas va ligado con las causas de fallo frecuentes, los puntos más comunes de falla son:

- No existen políticas de seguridad.
- Desconocer que son necesarias.
- Existen, pero no han sido difundidas entre el personal.
- Argumentos de presupuesto, implican inversión de tiempo y dinero.
- Pensar que el tamaño de la organización no lo amerita.
- No se cuenta con el personal capacitado en seguridad informática.

Es importante mencionar que se puede recurrir a estándares o recomendaciones al momento de escribir las políticas con la finalidad de apegarse a un lineamiento global y éste llevarlo a lo particular en el caso de cada organización.

3.14 Planes de contingencia y recuperación

En todo esquema de seguridad se debe contar con un plan de contingencia en caso de que se presente algún incidente de seguridad, en este plan se deberán de contemplar las medidas y acciones a realizar durante y después del incidente. La elaboración de dicho plan deberá de contemplar todos los posibles incidentes que se puedan presentar, desde un desastre natural, fallas en los sistemas, ataques lógicos o cualquier otra anomalía que afecte la operación normal, así como todos los aspectos para llegar a ofrecer servicio ante un desastre.

Los planes de contingencia y recuperación forman parte del ciclo de seguridad, contar con los planes adecuados permitirá una recuperación mucho más rápida y con ello la continuidad de los servicios que cada institución ofrece, evitando pérdidas económicas o continuidad en el servicio, garantizando con esto una alta disponibilidad, las etapas que marca un plan de contingencia son:

a) Evaluación.
b) Planificación.
c) Pruebas.
d) Ejecución.
e) Recuperación.

Si la recuperación no es inmediata no sólo se tienen pérdidas económicas, existen otras cuestiones que también son importantes como perder la confianza del cliente, niveles de servicios acordados con otras instancias, e incluso implicaciones legales.

Los planes deben darse a conocer a los integrantes del equipo para que cada uno analice las medidas a seguir en caso de ser necesario utilizar dicho plan.

Los planes de recuperación ante desastres han ido evolucionando a lo largo de la historia, esto debido a que día con día los desastres técnicos y humanos son más comunes, por lo que con ello surge la necesidad de mejorar los planes de recuperación además de que cada vez son más específicos.

Existe toda una teoría sobre los planes de recuperación y evolución de cada uno de ellos entre los planes más comunes, en orden de evolución se encuentran:

- Disaster Recovery Planning- Plan de recuperación ante desastres (DRP).
- Business Recovery Services Recuperación de los servicios del negocio (BRS).
- Business Recovery Planning- Plan de recuperación del negocio (BRP).
- Business Continuity Planning- Plan de continuidad del negocio (BCP).
- Business Continuity Management - Continuidad en la administración del negocio (BCM).

El plan de recuperación ante desastres (DRP), es un plan orientado a recuperar en el menor tiempo posible los sistemas críticos, utilizando equipos alternos para reducir en gran medida el impacto, se aplica cuando los sistemas han dejado de funcionar por completo, en este caso se debe contar con alternativas, como sitios alternos. Cuando se presenta un desastre de falla total sólo debe implicarse al equipo que se encuentra contemplado en el plan de recuperación, BCP está orientado a recuperar en el menor tiempo posible la operación de las funciones críticas del negocio, estén o no automatizadas.

Dependiendo del ámbito de aplicación del plan éste debe ser analizado por todos aquellos que participarán para poder realizar mejoras en el mismo, con ello se tiene la garantía de que al menos todos los participantes lo conocen, los planes de recuperación de desastres, al igual que los documentos de seguridad deben actualizarse constantemente.