UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PERIMETRAL PARA REDES DE DATOS. CASO PRÁCTICO: DIRECCIÓN GENERAL DEL COLEGIO DE CIENCIAS Y HUMANIDADES.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTAN:

JOSÉ MIGUEL BALTAZAR GÁLVEZ

JUAN CARLOS CAMPUZANO RAMÍREZ

DIRECTOR DE TESIS: M.C. CINTIA QUEZADA REYES

México, D.F. FEBRERO 2011

Mamá, te agradezco por las enseñanzas que me has dado, me diste fortaleza, me enseñaste a luchar y ser mejor persona cada día, sin tus enseñanzas no sería posible cumplir esta meta; fue un largo camino, pero finalmente se cierra una etapa más en mi vida.

A mis amigos y familiares, gracias por el apoyo que me han brindado durante este proceso de formación, no sólo profesionalmente, sino como ser humano.

También agradezco a la Universidad Nacional Autónoma de México, a mi Facultad de Ingeniería, por la valiosa formación que me han brindado así como a mi directora de tesis, M.C. Cintia Quezada Reyes.

José Miguel Baltazar Gálvez

A mis padres, hermanos y familia, que fueron esenciales para alcanzar este objetivo, gracias por apoyarme en todo momento y enseñarme que lo realmente importante es contar con nuestro apoyo y cariño.

A Juventino y Alberto, gracias por permitirnos realizar este trabajo, quienes más que compañeros de trabajo, son grandes amigos, gracias por su apoyo y consejos.

A la M.C. Cintia Quezada Reyes por todo su valioso tiempo invertido en este trabajo, enseñanzas, comentarios y sugerencias.

Es difícil agradecer a todos sin olvidar ningún nombre, pero sé muy bien que la gente que quiero y ha sido importante en mi vida, saben el aprecio y agradecimiento que les tengo por estar conmigo en todo momento, con quienes he compartido momentos buenos y malos, enseñanza e intercambio de experiencias.

Juan Carlos Campuzano Ramírez

Contenido

Introducción

A. Antecedentes

El crecimiento de las redes locales en los últimos años ha permitido incrementar el flujo de información a grandes escalas, permitiendo con ello agilizar procesos educativos, personales y comerciales, pero también con ello nuevas amenazas y vulnerabilidades. En la actualidad es imprescindible la implementación de una red en cualquier sector, ya que la existencia de una empresa que no cuente con dicha infraestructura no le será posible garantizar su productividad ni mucho menos su existencia en el mercado.

Todo este tipo de actividades que involucran el uso de las computadoras y telecomunicaciones están relacionados con información, dado que la información es un bien al cual es asociado un valor, por lo tanto están sujetos a riesgos, impactando de manera económica, comercial, de prestigio y confianza y existencia de la organización, principalmente. En este escenario hay factores a tomar en cuenta, los equipos de cómputo y protocolos de comunicación empleados de manera inicial, no fueron creados con la seguridad en mente por *default*, así mismo la venta de equipo de cómputo de forma masiva, pone la capacidad de amenaza en manos de más personas, por esta razón no existe un momento en el que no importe la seguridad, para cualquier organización.

A pesar de la gran utilidad y todas las ventajas que ofrecen las redes no se puede dejar a un lado y mucho menos dar por hecho que la seguridad de la organización se encuentra en optimas condiciones, actualmente cada vez mas empresas reconocen tener incidentes de seguridad en sus organizaciones, lo que demuestra que es importante invertir en su seguridad, tomando en cuenta conceptos como administración, seguridad informática y todo lo que ello implica.

Dada la importancia de las redes y su indiscutible necesidad, han permitido el desarrollo de nuevas tecnologías así como una nueva forma de lucrar con la información ajena, de manera general se han mostrado las ventajas que éstas ofrecen, sin embargo, se deben tomar en cuenta ciertas cuestiones como garantizar que la información que circula a través de la red, así como aquella que es almacenada en un equipo final sea confiable, integra, disponible y confidencial.

Las instituciones actualmente están buscando mecanismos que permitan minimizar el riesgo al cual puedan estar expuestos, ya que no existe como tal un proceso que se debiera seguir y que con ello garantice o se considere una red 100% segura, pues la práctica demuestra lo contrario, aunque al implementar mecanismos de control, como lo son el uso de estándares de seguridad, políticas internas, legislación informática, respaldos, planes de contingencias, esquemas de seguridad perimetral, servicios de seguridad, recomendaciones de instituciones como NIST, SANS, ISO, entre otras, todo esto ayuda a reducir riesgos.

Mantener la información íntegra, disponible y de manera confidencial es de gran importancia para cualquier organización, ya que de ello depende que dicha organización cumpla con sus objetivos establecidos. Por otro lado, no es posible garantizar la seguridad global, pero sí es posible disminuir los riegos dentro de una red de área local, ¿cómo lograrlo?, existen distintas formas aunque como se mencionó, no necesariamente existe un camino, es decir, se pueden tener distintos esquemas de seguridad de acuerdo con las necesidades propias de cada organización.

B. Definición del problema

Considerando que día con día la mayoría de los servicios brindados por cualquier organización, se están migrando a entornos que involucran el uso de equipos de cómputo, servidores y redes de datos, también se deben considerar los múltiples ataques que sufren las organizaciones, enfocados al robo de información, falsificación, modificación, denegaciones de servicio, suplantaciones, vulnerabilidades en sistemas, uso de equipos de cómputo para actividades maliciosas, entre muchas otras, debido a un descuido o de manera intencional. Las organizaciones deben planear contar con un esquema de seguridad perimetral, basado en las necesidades de negocio y sus objetivos.

El hecho de implementar un esquema de seguridad perimetral, para el Colegio de Ciencias y Humanidades, tiene como objetivo proteger la red de la organización, partiendo de un análisis de riesgos que permita identificar los activos de mayor valor, realizar un inventario de la red actual, identificar amenazas, vulnerabilidades, ponderando los riesgos, buscando posteriormente plantear el diseño que permitirá minimizar riesgos.

Un esquema de seguridad perimetral para la red de una institución puede contemplar mecanismos de control de acceso, implementación de estándares, monitoreo, políticas, procedimientos, inventario de los equipos, firewall, IDS, IPS, DRP, prevención, auditorias, administración, detección y respuesta a incidentes, capacitación, entre muchos otros, ya que éstos en conjunto brindarán a la organización un nivel de confianza mayor, todo esto debe ser analizado y determinado a nivel directivo. Por estos motivos se busca seguir una metodología para implementar un esquema de seguridad. Cabe mencionar que mientras más controles se tengan, el nivel de confianza que alcanzará la institución será mayor, sin dejar de contemplar las vulnerabilidades de los controles que se agreguen.

El esquema que se analiza, desarrolla e implementa está basado en las necesidades de la Dirección General del Colegio de Ciencias y Humanidades, a la fecha es impredecible contar con un esquema de seguridad perimetral que proteja los servicios e información de la institución, como entidad central de los 5 colegios que la conforman, la información transmitida y almacenada tiene cierto grado de importancia. El esquema a diseñar puede ser aplicado a otras instituciones si no de manera total, sí parcialmente, ya que como se mencionó, la implementación depende directamente de los objetivos y activos de cada institución.

Al ser una institución educativa, se cree que sus activos principales caen en los registros escolares, base de datos de sus trabajadores, inventario, nómina, publicaciones educativas, servicios electrónicos brindados a la comunidad, así como garantizar la disponibilidad de los servicios tanto para académicos, administrativos y alumnos, buscando limitar las actividades que no tengan ninguna relación con la finalidad de la institución, tanto actividades internas como externas.

C. Objetivos

- Realizar un análisis de riesgos que permita priorizar necesidades de seguridad, con base en el NIST 800-30.
- Estudiar diferentes propuestas para ofrecer seguridad, tanto a nivel de red, transporte y aplicación.
- Elaborar un estudio de la infraestructura de red con que cuenta la Dirección General del Colegio de Ciencias y Humanidades, para determinar el esquema que permita administrar, auditar e identificar información relevante en el segmento de red, de manera centralizada implementado herramientas de software libre y propietario.
- Diseñar un esquema de seguridad perimetral para la Dirección General del Colegio de Ciencias y Humanidades, que permita minimizar los riesgos contra los ataques más frecuentes.
- Realizar la implementación del esquema de seguridad propuesto para la Dirección General del Colegio de Ciencias y Humanidades.

D. Contribuciones

- Realización de un primer análisis de riesgos para la institución, basado en el estándar NIST 800-30.
- Implementación en su conjunto de un primer esquema de seguridad perimetral para la institución.
- Implementación de controles, que permitan identificar y solucionar problemas en la red de manera clara y precisa.
- Desarrollo de políticas de uso de la red para la Dirección general del Colegio de Ciencias y Humanidades.
- Reducir los incidentes de seguridad relacionados con amenazas lógicas, así como físicas.
- Que este estudio sea una base para realizar una implementación de esquema de seguridad perimetral para cualquier otra organización, en particular para los planteles que conforman el colegio.

E. Estructura de la tesis

La tesis se divide en 5 capítulos:

Capítulo I. Conceptos básicos:

Se describen los conceptos básicos de redes, considerando los modelos OSI, TCP/IP y los protocolos de servicio más utilizados, considerando protocolos como DNS, HTTP, TELNET, SSH, DHCP, FTP, TFTP, SNMP, SMTP, entre otros.

Capítulo II. Conceptos generales de seguridad:

Cubre los conceptos generales de la seguridad, considerando sus principios, definiciones básicas, fases de un ataque, tipos de ataques, controles de seguridad y la importancia del análisis de riesgos.

Capítulo III. Mecanismos de seguridad en red:

muestra los mecanismos de seguridad que se pueden aplicar a una red, considerando tipos de estrategias, servicios, mecanismos de autenticación, factores relacionados a la seguridad física, cifrado, firewall, IDS, auditorias, monitoreo, seguridad en redes inalámbricas, sensores, estándares, políticas de seguridad y planes de contingencia.

Capítulo IV. Buenas prácticas de seguridad:

Observa las recomendaciones que se emiten de manera general en la seguridad de la información, por organizaciones con experiencia en la implementación de políticas, procedimientos, mecanismos y acciones, que permitan brindar un control efectivo en la organización.

Capítulo V. Propuesta de implementación, caso práctico:

Una vez comprendidos los conceptos y aspectos básicos de redes y seguridad la información, se realizará el análisis de riesgos basado en el estándar NIST 800-30 (Risk Management Guide for Information Technology Systems - Guía de Administración de Riesgos para Sistemas en Tecnologías de la Información), el cual será la base para la definición e implementación del esquema de seguridad perimetral.

Además el trabajo de tesis contiene un conjunto de apéndices que dan más detalle sobre algunos temas específicos, glosario, lista de acrónimos frecuentes, así como la bibliografía empleada para la realización de este trabajo.

Tres reglas en seguridad.

- **No existen sistemas absolutamente seguros.**
- **Para reducir su vulnerabilidad a la mitad se tiene que doblar el gasto en seguridad.**
- **Típicamente, los intrusos *brincan* la criptografía, no la rompen.**

[Francisco Rodríguez Enríquez]

CAPÍTULO 1
Conceptos Básicos

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, incluyendo fraudes por medios tecnológicos, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad significa que el costo para romperla excede al costo del bien de cómputo asegurado, esto es, el tiempo requerido para romper la seguridad excede el tiempo de vida útil del bien de cómputo, siendo éste último hardware, software o información.

1.1. Redes de datos

El concepto red actualmente es mencionado prácticamente en cualquier lugar, la razón es simple y sencilla, se vive en un mundo rodeado de redes y no se hace referencia sólo en el ámbito de la computación, pues el concepto se amplía más allá, como lo es en el hogar, la educación, el transporte, comunicaciones, banca, transacciones y servicios. Por ejemplo, una red carretera que permite conectar ciudades, redes telefónicas, redes eléctricas entre otras más.

Desde el punto de vista de la computación, una red de datos es un conjunto de computadoras autónomas interconectadas física y lógicamente para facilitar el intercambio y procesamiento de la información.

La importancia radica en el hecho de que se han convertido desde hace algunas décadas en una necesidad en cualquier ámbito, por ejemplo, el crecimiento económico de una empresa mucho se debe al adecuado uso de la mercadotecnia haciendo uso de la redes para alcanzar nuevos mercados, por lo que han permitido un impacto económico en las distintas áreas. Actualmente las redes de datos son una indiscutible necesidad en cualquier sector, por lo que cada día seguirán evolucionando y alcanzando nuevas fronteras.

Actualmente las redes de datos brindan comunicación inmediata casi en cualquier parte de la tierra, esto gracias a la versatilidad de la misma, emplean diferentes medios que se utilizan para su transmisión por medios físicos e inalámbricos, siendo estos últimos empleados día a día en mayor volumen. En el caso de los medios físicos, éstos tienen características especiales que los diferencian de los inalámbricos, como mayor velocidad de transferencia, disponibilidad y área de cobertura.

Las redes de datos se clasifican con base en su forma de transmisión en redes cableadas e inalámbricas, dentro de éstas existen clasificaciones tomando en cuenta su topología, alcance, medio de transmisión y velocidad.

Las características más importantes de las redes cableadas son:

- Se utilizan cables como medios para la transmisión (fibra óptica y cables de cobre como UTP [Unshielded Twisted Pair - Cable de par trenzado] y coaxial).
- Existen distintos estándares como son IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring), del estándar 802.3 se derivan otros estándares de acuerdo con la velocidad de transferencia de datos y tipo de medio utilizado como son Fast Ethernet IEEE 802.3, Gigabit Ethernet IEEE 802.3z.
- Por su alcance se clasifican en redes LAN (Local Area Network –Redes de Área local), WAN (Wide Area Network- Redes de Área Amplia), MAN (Metropolitan Area Network-Redes de Área Metropolitana) entre algunas otras.
- Las topologías comunes son: Bus, estrella, anillo, árbol, malla, etcétera.
- Permiten grandes velocidades de transmisión hasta 1 Gbps, actualmente existe equipos que permiten enlaces 10Gps.

Las características más importantes de las redes inalámbricas son:

- Utiliza el aire como medio de transmisión.
- Diferentes velocidades de transmisión, desde 2 hasta 300 Mbps.
- Movilidad.
- Flexibilidad en la instalación.
- Escalabilidad.
- Bajo costo de implementación.

En la figura 1.1 se observa un diagrama en el cual se muestra la clasificación de las redes.

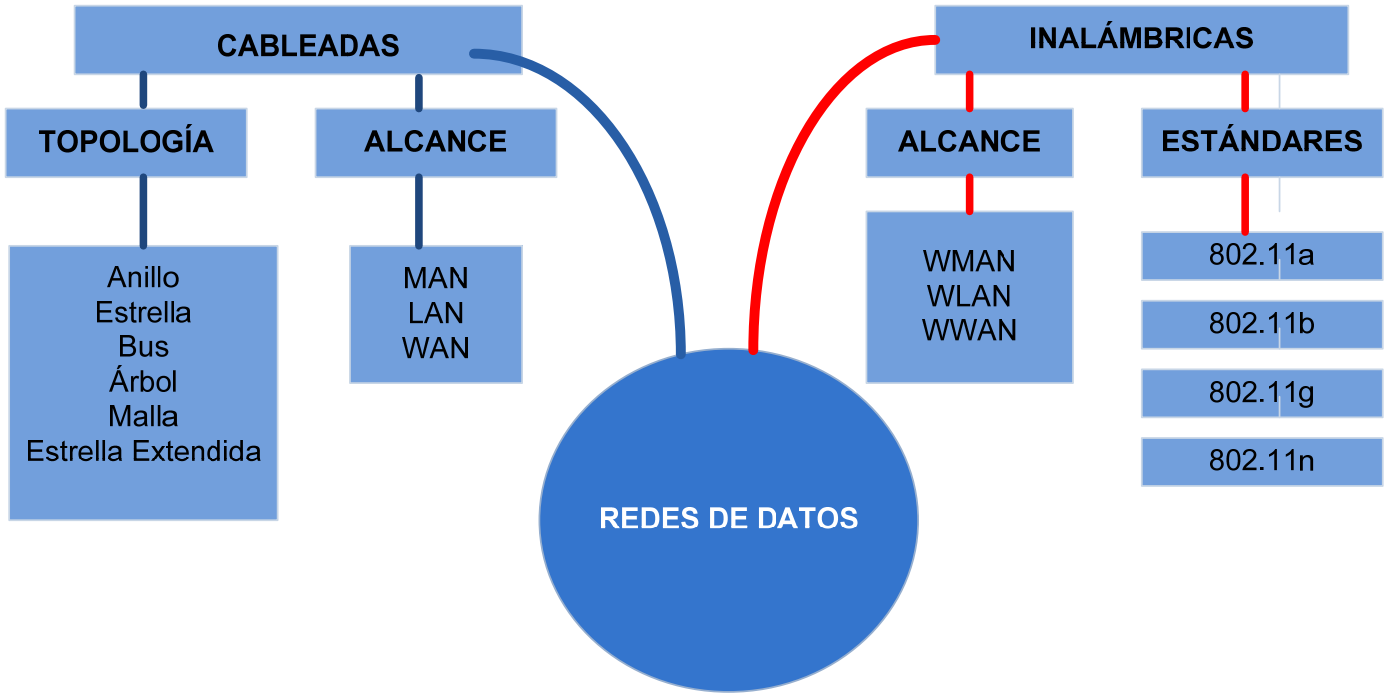


Figura 1. 1 Clasificación de las redes por alcance, topología y estándar.

1.1.1. Conceptos básicos

Dentro del mundo de las redes se manejan conceptos que permiten comprender el proceso de interacción entre los distintos dispositivos que comprenden una red.

Enseguida se describen algunos conceptos que frecuentemente se encuentran relacionados con las redes datos.

a) Dirección física

La dirección física es un término de uso común en las redes de datos, de acuerdo con la definición de redes de datos, para formar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, esta interfaz se conoce como tarjeta de red o también denominada NIC (Network Interface Controller – Controlador de interfaz para red).

Cada tarjeta de red NIC tiene asignado un identificador único llamado MAC (Media Access Control – control de acceso al medio), o dirección física, dicha dirección está formada por 48 bits y para mayor facilidad de su representación se utiliza el sistema hexadecimal, por lo que se utilizan 12 dígitos.

Los seis primeros dígitos hexadecimales, que son administrados por el IEEE (Institute of Electrical and Electronics Engineers - Instituto de ingenieros eléctricos y electrónicos), identifican al fabricante o proveedor y, de ese modo, abarcan el *Identificador Exclusivo de Organización* (*OUI*). Los seis dígitos hexadecimales restantes abarcan el *número de serie de interfaz,* u otro valor administrado por el proveedor específico. Las direcciones MAC, como identificador, son grabadas en una memoria de sólo lectura en la tarjeta de red. Un ejemplo de dicha dirección se presenta en la figura 1.2.

Figura 1. 2 Dirección física (MAC Address).

No existen direcciones físicas iguales, sin estos identificadores únicos sería complicado determinar a quién le será entregado un paquete, por lo que cuando un equipo envía información, ésta es encapsulada agregando las direcciones MAC Address origen y destino. La información no se puede enviar o entregar de forma adecuada en una red si no tiene esas direcciones.
Si se desea obtener el nombre de algún fabricante a partir de la dirección MAC Address, se puede realizar la búsqueda desde el sitio http://standards.ieee.org/regauth/oui/index.shtml, es importante este dato en auditorías y seguimiento de incidentes.

b) Dirección IP

Cuando un equipo de cómputo desea enviar un paquete a otro equipo, dicho paquete deberá contener la dirección destino y origen, ya que sin esto no sería posible que el paquete llegue a su destino. La dirección IP (Internet Protocol – Protocolo de internet) contiene la información necesaria para enrutar un paquete a través de la red TCP/IP (Transmission Control Protocol/Internet Protocol – Protocolo de control de transmisión/ Protocolo de Internet).

La dirección IPv4 es representada por 32 bits, dicha dirección comúnmente es representada utilizando notación decimal, se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal máximo de cada octeto es 255, reservando este número para envió broadcast.

Los campos que componen a una dirección IP son identificador de red (Network ID) e identificador de host (host ID), el número de red de una dirección IP identifica la red a la cual pertenece dicho dispositivo. El host ID de una dirección IP identifica el dispositivo específico de una red.

Existen tres clases de direcciones IP A, B, C, que una organización puede recibir de parte del Registro Americano de Números de Internet (ARIN) o ISP de la organización (Ver tabla 1.1).

Tabla 1. 1 Direcciones IP.

Tipo	Dirección menor	Dirección más alta	Máscara de Red	Numero de host por red
A	0.0.0.0	126.0.0.0	255.0.0.0	16,777,214
B	128.0.0.0	191.255.0.0	255.255.0.0	65,534
C	192.0.0.0	223.255.255.0	255.255.255.0	254
D	224.0.0.0	239.255.255.255	No aplica	No aplica
E	240.0.0.0	247.255.255.255	No aplica	No aplica

Adicional a estas direcciones IP, existe otra clasificación, utilizada en la asignación de IP mediante NAT, para generar intranet en las organizaciones, las direcciones privadas son:

Tabla 1. 2 Direcciones IP privadas.

Tipo	Dirección menor	Dirección más alta	Máscara de Red
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

c) Resolución de direcciones

Cada equipo conectado a la red tiene una dirección física única, además de tener una dirección IP, por lo que cuando un equipo desea transmitir un paquete de información a otro debe existir un mecanismo que relacione ambas direcciones mencionadas, la dirección física con la dirección IP para que la información llegue al destino correcto (Figura 1.3).

Este proceso se realiza en la capa de red (modelo OSI) o en la capa de enlace de red (modelo TCP/IP) mediante el protocolo ARP (Address Resolution Protocol – Protocolo de resolución de dirección), el cual se encarga de asociar la dirección física a una determinada dirección IP, si el equipo destino está ubicado dentro de la red local, el equipo origen envía un mensaje a todos los equipos preguntando a quién le corresponde dicha dirección IP, el equipo destino responde a dicho mensaje agregando su dirección MAC.

Sin embargo, cuando la dirección destino no pertenece al mismo segmento de red, para que un dispositivo envíe datos a la dirección MAC de un dispositivo que está ubicado en otro segmento de la red, el dispositivo origen envía los datos a un gateway por defecto. El gateway por defecto es la dirección IP de la interfaz del router conectada al mismo segmento de red física que el host origen. El host origen compara la dirección IP destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran ubicadas en el mismo segmento. Si el dispositivo receptor no está ubicado en el mismo segmento, el dispositivo origen envía los datos al gateway por defecto.

Si la dirección de subred es distinta, el router responderá con su propia dirección MAC a la interfaz que se encuentra directamente conectada al segmento en el cual está ubicado el host origen. Dado

que la dirección MAC no está disponible para el host destino, el router suministra su dirección MAC para obtener el paquete. Luego el router puede enviar la petición ARP (basándose en la dirección IP destino) a la subred adecuada para que se realice la entrega.

Existe otro protocolo RARP (Reverse Address Resolution Protocol –Protocolo de resolución de dirección de retorno) que funciona de manera inversa, para este caso debe existir un servidor que mantiene una base de datos de correspondencia de direcciones MAC a direcciones IP.

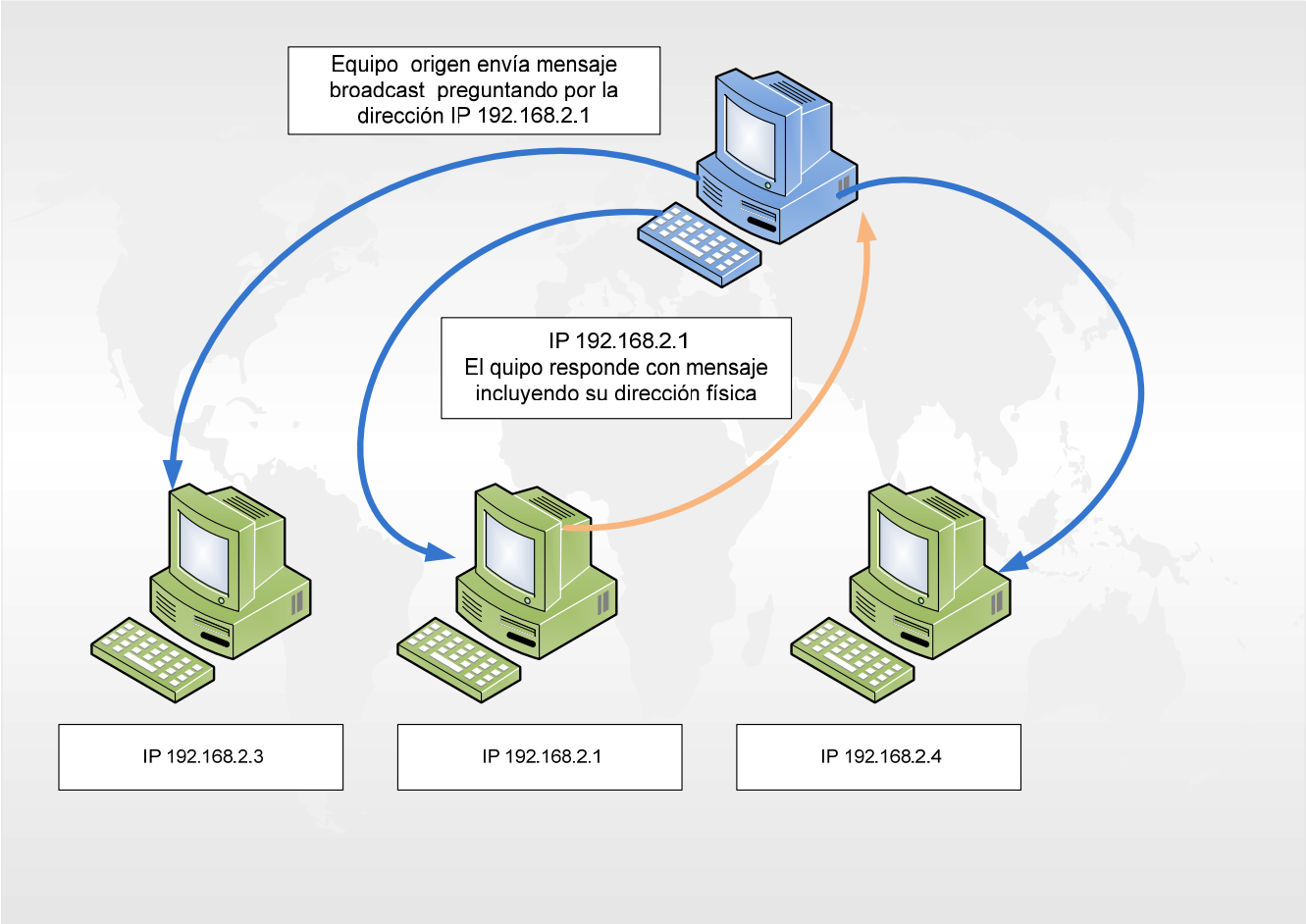


Figura 1. 3 Resolución de direcciones.

d) Definición de protocolo

En todo proceso de comunicación es necesario seguir reglas para poder comprender el intercambio de información, por ejemplo para poder entablar una conversación es necesario que los interlocutores hablen el mismo idioma , ya que si no fuese así no podrían comunicarse entre ellos.

Se presenta la misma situación en las redes de datos, en el momento en que dos equipos intenten comunicarse deberán seguir ciertas reglas para establecer el proceso de intercambio de información, a este proceso se le conoce como protocolo.

Un protocolo, en el contexto de las telecomunicaciones, es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Una definición técnica de un protocolo de

comunicaciones de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.[1]

Cabe mencionar que existen distintos protocolos y cada uno de ellos tiene una tarea en específico.

e) Definición de puertos

Cuando un programa cliente necesita de un servicio particular de un servidor, además del tipo de servicio y localización del servidor, debe indicar el puerto por el que se establecerá la conexión. En este sentido, un puerto es un canal lógico de comunicación que permite a dos equipos intercambiar información.

Los puertos son representados con un valor numérico y se representan mediante una palabra de 2 bytes, por lo que existen 2^{16}, es decir 65535 puertos, existe una organización que se encarga de regular dichos puertos conocida como IANA (Internet Assigned Numbers Authority -Agencia de asignación de números de internet), dicha organización realiza una clasificación de los puertos en:

- Puertos bien conocidos, definidos del puerto 1 al 1023, utilizados para servicios bien conocidos como web, correo electrónico, etcétera.
- Puertos registrados, definidos del puerto 1024 al 49151, utilizados por aplicaciones conocidas y registrados en IANA, como es el caso de DB (Database – Base de datos), escritorio remoto, RADIUS, etcétera.
- Puertos dinámicos y/o privados del puerto 49152 al 65535.

f) Definición de puerta de enlace

El gateway o puerta de enlace es el encargado de interconectar distintas redes utilizando distintos protocolos, es el punto de la red que permite la entrada a otra red, el gateway se asocia al router (dispositivo de capa tres) sin embargo, el gateway es capaz de enlazar redes con diferentes protocolos, además de que este dispositivo puede trabajar en los siete niveles del modelo OSI.

Los gateways pueden ser personalizados para realizar una función específica, por ejemplo para una conversión de protocolos, aplicación de conversión de datos etcétera.

1.2. Modelo OSI y TCP/IP

En redes de datos existen modelos que determinan la manera en la cual es interpretada la información, como es el caso de los modelos OSI (Open System Interconnection –Sistema de interconexión abierta) y TCP/IP, el modelo OSI es la base de un conjunto de protocolos además de

[1] Programa de la academia Cisco Networking, material multimedia, 2006.

ser la plataforma de un programa internacional para el desarrollo de protocolos de red y otros estándares que faciliten la intercomunicación de los dispositivos ofrecidos por diferentes vendedores.

1.2.1 Modelo OSI

Durante las últimas décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes, muchas de ellas se desarrollaron utilizando implementaciones de hardware y software diferentes, como resultado, muchas de las redes eran incompatibles y se volvió muy difícil la comunicación entre ellas, debido a que utilizaban especificaciones distintas. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

El modelo de referencia OSI es el modelo utilizado para las redes de datos. Sin embargo, no es el único modelo que existe, ya que existen otros modelos de referencia como lo es el modelo TCP/IP.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red.

1.2.1.1 Esquema del modelo OSI

En el modelo de referencia OSI, existen siete capas como se muestra en la figura 1.4.

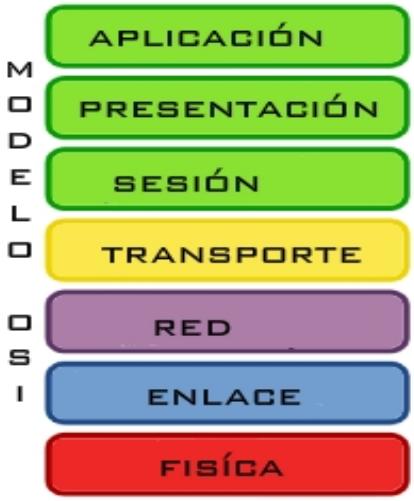


Figura 1. 4 Capas del modelo OSI.

El modelo de capas permite comprender de manera sencilla el proceso de comunicación entre equipos, además de que esto implica identificar y solucionar problemas de comunicación de manera más eficiente, permite la interoperabilidad de las tecnologías, estandariza las interfaces y permite un desarrollo mucho más rápido. Las capas que conforman al modelo OSI son:

1) Presentación.
2) Aplicación.
3) Sesión.
4) Transporte.
5) Red.
6) Datos.
7) Física.

a) Capa física

Enumerando el modelo OSI de forma ascendente, la capa física ocupa el lugar número uno, recordando que una computadora o cualquier dispositivo electrónico funciona a base de voltaje, por lo que en esta capa se consideran los dispositivos encargados de transportar la señal de un dispositivo a otro y que a su vez son convertidos en ceros y unos para que el dispositivito pueda interpretarlos.

La capa física es la capa que define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas finales.

A lo largo de la historia de las redes se han utilizado distintos medios para interconectar los equipos que conforman la red, esto debido a que se encuentran mejoras en los medios de transmisión, lo cual permite tener un mejor desempeño, desde luego el medio no es el único factor que interviene en el tiempo de retardo para trasmitir datos ya que existen otros factores.

Dentro de los elementos que componen a la capa física se encuentran los distintos medios de transmisión como son fibra óptica, cable UTP (Unshielded Twisted Pair – Cable de par trenzado) en sus distintas categorías, atmósfera que es un medio para transmitir ondas de radio además del cable coaxial que prácticamente desaparece. También ha cambiado la topología, por lo que los medios de enlace físico han evolucionado, ofreciendo nuevas ventajas como mayor alcance, mayor velocidad de transmisión, fácil instalación, etcétera, incluyendo estándares que se han desarrollado en función del tipo de red.

Enseguida se enumeran los componentes pertenecientes a la capa física:

- Medios de transmisión (coaxial, UTP, fibra óptica, ondas magnéticas en general, DSL, ADSL, etcétera).
- Repetidores.
- Concentradores (router, switch, hub).
- Tarjeta de Red.

b) Capa de enlace

Los bits que son transportados independientemente del medio que se utilice, no serían de utilidad si no fuese posible identificar quién los genera y cuál es su destino, he aquí la importancia de la capa de enlace de datos.

La capa de enlace de datos se divide en dos partes:

- Estándar LLC (Logical Link Control- Control de enlace lógico), se define en la especificación IEEE 802.2. independiente de la tecnología.
- Las partes específicas, que dependen de la tecnología e incorporan la conectividad de la capa uno.

El *IEEE* divide la capa de enlace OSI en dos subcapas separadas, las subcapas IEEE reconocidas son:

- Control de acceso al medio (MAC) (realiza transiciones hacia los medios).
- Control de enlace lógico (LLC) (realiza transiciones hasta la capa de red).

Estas capas son de vital importancia ya que garantizan que las tecnologías sean compatibles y que las computadoras puedan establecer la comunicación.

En la tarjeta NIC se encuentra la dirección MAC o dirección física, aunque la tarjeta de red es un dispositivo de capa uno, este dispositivo funciona en las dos capas ya que se conecta directamente con el medio físico.

La capa de enlace lógico permite que la capa de enlace de datos funcione independientemente de las tecnologías existentes, por lo que esta capa proporciona versatilidad en los servicios de los protocolos de la capa de red que está sobre ella, mientras se comunica de forma efectiva con las diversas tecnologías que están por debajo. El LLC, como subcapa, participa en el proceso de encapsulamiento. La PDU (Protocol Data Unit- Unidad de datos de protocolo) del LLC a veces se denomina paquete LLC.

LLC define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

El LLC transporta los datos del protocolo de la red, un paquete IP, y agrega más información de control para ayudar a entregar ese paquete IP en el destino. Agrega dos componentes de direccionamiento de la especificación IEEE 802.2: el punto de acceso al servicio destino (DSAP) y el punto de acceso al servicio fuente (SSAP). Luego este paquete IP re empaquetado viaja hacia la subcapa MAC para que la tecnología específica requerida le adicione datos y lo encapsule. Un ejemplo de esta tecnología específica puede ser una de las variedades de Ethernet, Token Ring o FDDI (Fibber Distributed Data Interface – Interfaz de Datos Distribuida por Fibra).

La subcapa LLC de la capa de enlace de datos administra la comunicación entre los dispositivos a través de un solo enlace a una red. LLC se define en la especificación IEEE 802.2 y soporta tanto servicios orientados a conexión como servicios no orientados a conexión, los cuales son utilizados por los protocolos superiores. IEEE 802.2 define una serie de campos en las tramas de la capa de enlace de datos que permiten que múltiples protocolos de las capas superiores compartan un solo enlace de datos físico.

De manera general la capa dos realiza las siguientes funciones:

- Suministra un tránsito confiable de datos a través de un enlace físico.
- Usa un sistema denominado Control de acceso al medio (MAC).
- Usa la dirección MAC, que es la dirección física que se ubica en una NIC.
- Usa el entramado para organizar o agrupar los bits.

c) Capa de red

La tercera capa del modelo OSI es la capa de red, ésta es la encargada de la navegación de los datos a través de la red, se encarga de encontrar la mejor ruta a través de la misma.

A medida que las redes crecen surge la necesidad de interconectarlas entre sí para formar nuevas redes creando el ya conocido Internet, para poder lograr esta comunicación entre las distintas redes, surge la necesidad de nuevos dispositivos encargados de realizar esta operación como los routers.

Los routers son dispositivos de interconexión que operan en la capa tres del modelo OSI. Estos dispositivos unen o interconectan segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de enlace.

Los routers cuentan con algoritmos capaces de tomar decisiones como calcular la mejor ruta de envío de datos, luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman paquetes de dispositivos LAN, basándose en información de la capa tres la información es enviada a través de la red, además de que estos dispositivos pueden calcular la menor ruta basándose en la densidad del tráfico y la velocidad del enlace.

Para que un router pueda encontrar la mejor ruta, lo puede realizar de dos maneras, empleando direccionamiento plano o direccionamiento jerárquico. Un esquema de direccionamiento plano asigna a un dispositivo la siguiente dirección disponible mientras que un direccionamiento jerárquico se asigna a través de la ubicación, el protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico.

Los routers requieren direcciones de red para garantizar el envío correcto de los paquetes, por lo que la dirección IP contiene la información necesaria para enrutar un paquete a través de la red. Cada dirección origen y destino que contiene está compuesta por 32 bits.

d) Capa de transporte

Una vez que el router ha elegido la mejor ruta para el envío de datos a través de la red, pasan a la capa de transporte, la cual es la encargada de regular el flujo de información desde el origen hasta el destino de manera confiable y precisa, para llevar a cabo este proceso entran en juego dos protocolos TCP (Transmission Control Protocol – Protocolo de control de transmisión) y UDP (User Datagram Protocol – Protocolo de datagrama de usuario).

Una característica tajante que diferencia TCP de UDP es que el primero es un protocolo orientado a conexión.

a) Las características de TCP

- Orientado a conexión.
- Confiable.
- Divide los mensajes salientes en segmentos.
- Re ensambla los mensajes en la estación destino.
- Vuelve a enviar lo que no se ha recibido.
- Re ensambla los mensajes a partir de segmentos entrantes.
- Forma parte de la pila de protocolos TCP/IP.

b) Las características de UDP:

- No orientado a conexión.
- Poco confiable.
- Transmite mensajes (llamados datagramas del usuario).
- No utiliza acuses de recibo.

Tanto TCP como UDP utilizan diferentes puertos que les permiten dar seguimiento a la comunicación y pasar información a capas superiores.

e) Capa de sesión

La capa de sesión establece, administra y termina las sesiones entre las aplicaciones. Esto incluye el inicio, la terminación y la re sincronización de dos computadoras que están manteniendo una "sesión". La capa de sesión coordina las aplicaciones mientras interactúan en dos hosts que se comunican entre sí. Las comunicaciones de datos se transportan a través de redes conmutadas por paquetes, al contrario de lo que ocurre con las llamadas telefónicas que se transportan a través de redes conmutadas por circuitos. La comunicación entre dos equipos involucra una gran cantidad de pequeñas conversaciones, permitiendo de esta manera que las dos computadoras participen de forma efectiva. Un requisito de estas conversaciones es que cada host tenga que jugar un doble papel: el de solicitar el servicio, como si fuera un cliente y el de contestar como servicio, como lo hace un servidor. La determinación del papel que están desempeñando en un preciso momento se denomina *control de diálogo*.

Las peticiones y respuestas de los equipos que han establecido una sesión son coordinadas por protocolos implementados en la capa cinco.

f) Capa de presentación

Esta capa permite la comunicación entre aplicaciones en diversos sistemas informáticos, de tal forma que sean transparentes para las aplicaciones.

Se ocupa del formato y de la representación de datos, entre las principales funciones de esta capa se encuentran:

- Formateo de datos
- Compresión de datos
- Cifrado de datos

Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta algunas funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión.

Por otro lado, en la estación receptora, la capa de presentación toma los datos de la capa de sesión y ejecuta las funciones requeridas antes de pasarlos a la capa de aplicación.

La capa de presentación también se ocupa de la compresión de los archivos.

g) Capa de aplicación

La capa número siete del modelo OSI es llamada capa de aplicación, los usuarios finales interactúan directamente con esta capa, en ella se encuentran todos los programas con los que puede interactuar el usuario que hacen uso de la red.

Por lo que esta capa es la encargada de identificar la disponibilidad de los participantes de la comunicación, sincronizar aplicaciones y controlar la integridad de los datos. La capa de aplicación no brinda servicios a ninguna otra capa OSI. Sin embargo, brinda servicios a los procesos de aplicación que se encuentran fuera del alcance del modelo OSI.

1.2.2 Modelo TCP/IP

Todos quienes utilizan un equipo de cómputo e Internet, ingenieros, académicos, profesionistas, gente de negocios, estudiantes y muchos más, emplean de manera invisible el uso de los protocolos TCP/IP para realizar cualquiera de sus actividades que impliquen comunicación con otros equipos de cómputo.

El nombre de TCP/IP se refiere a una suite completa de protocolos de comunicación, esta suite obtiene su nombre de los protocolos que le pertenecen; el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP), TCP/IP es el nombre tradicional para este conjunto de protocolos, éste en ocasiones es llamado Internet Protocol Suite (IPS), ambos nombres son aceptables aunque en este caso se hará referencia al protocolo como TCP/IP.

1.2.2.1 Introducción al modelo TCP/IP

El origen de los protocolos TCP/IP se remonta al año de 1969, por medio de un proyecto de desarrollo e investigación fundado en la Agencia de Proyectos de Investigación Avanzada (ARPA) por sus siglas en inglés, el proyecto consistía en crear un red de intercambio de paquetes la cual fue llama ARPANET, fue construida para estudiar técnicas para brindar comunicaciones de datos robusta, confiable e independientes de los vendedores.

Estas redes experimentales fueron tan exitosas que muchas de las organizaciones comenzaron a utilizarlas en sus comunicaciones de datos diariamente. En 1975 el ARPANET fue convertido de una red experimental a una red operacional y la responsabilidad para administrar esta red fue asignada a DCA (Defense Communications Agency-Agencia de defensa para las comunicaciones) ahora

conocida como DISA (Defense Information Systems Agency- Agencia para la defensa de sistemas de información), división que pertenece al Departamento de Defensa de los Estados Unidos.

Los protocolos TCP/IP fueron desarrollados después de que la red se volviera operacional, estos protocolos fueron adoptados como estándares militares en 1983 y todos los nodos conectados a la red se convirtieron al nuevo protocolo. Al mismo tiempo de que TCP/IP fue adoptado como un estándar, el término Internet comenzó a ser utilizado de manera común. En 1983 el viejo ARPANET fue dividido en MILNET, la parte no clasificada de la red de datos de defensa y en un nuevo y más pequeño ARPANET, Internet fue utilizado para referirse a la red entera, actualmente internet es el término genérico utilizado para referirse a toda la red.

La popularidad de TCP/IP creció rápidamente ya que este modelo fue la base para la conexión a Internet, además de ser un protocolo estándar abierto, ser independiente de la conexión física de red (Ethernet, DSL, dial-up, fibra óptica, inalámbrica y cualquier otro medio de transmisión), además de su compatibilidad con diferentes sistemas operativos y hardware, un esquema de direccionamiento común que permite a cualquier dispositivo una dirección única que cualquier otro dispositivo en la red entera, inclusive al ser empleado en redes que no tienen conexión a Internet y una estandarización en los protocolos de capa superior.

1.2.2.2 Arquitectura del protocolo TCP/IP

La arquitectura del protocolo TCP/IP está compuesta de menos capas que las siete utilizadas en el modelo OSI, las 4 capas del modelo TCP/IP se ilustran en la figura 1.5.

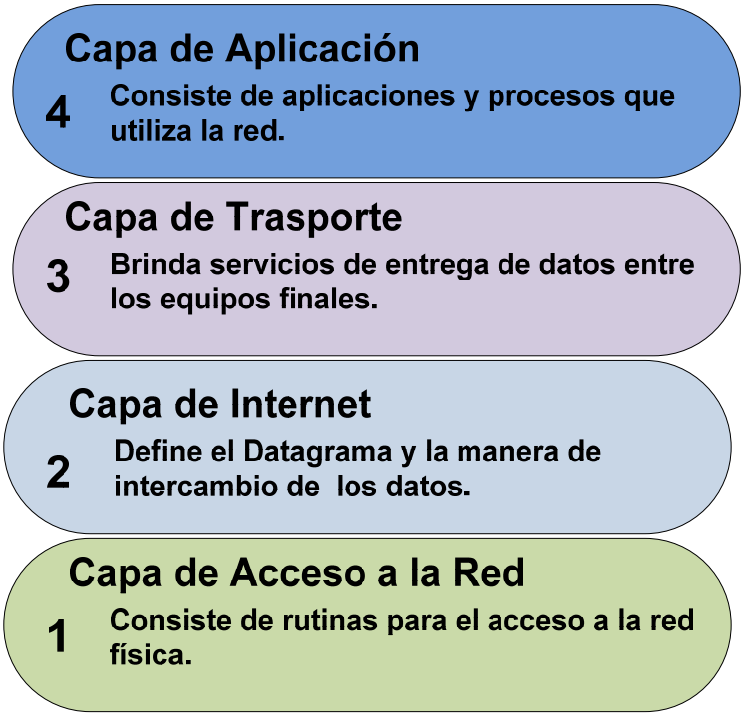


Figura 1. 5 Arquitectura TCP/IP.

Como en el modelo OSI, los datos pasan de la capa inferior hacia la superior, es decir, de la capa de *acceso a red* hasta llegar a la *capa de aplicación*, cada capa de la pila agrega controles a la información para garantizar la apropiada entrega, este control de información es llamado encabezado, porque éste es colocado frente a los datos que serán trasmitidos, cada capa trata toda la información que ésta recibe como datos y le agrega su propia cabecera al principio de la información, esto también es conocido como encapsulado, cuando los datos se reciben, cada capa quita su encabezado de los datos hasta llegar a la capa de aplicación, la cual interpreta los datos(figura 1.6).

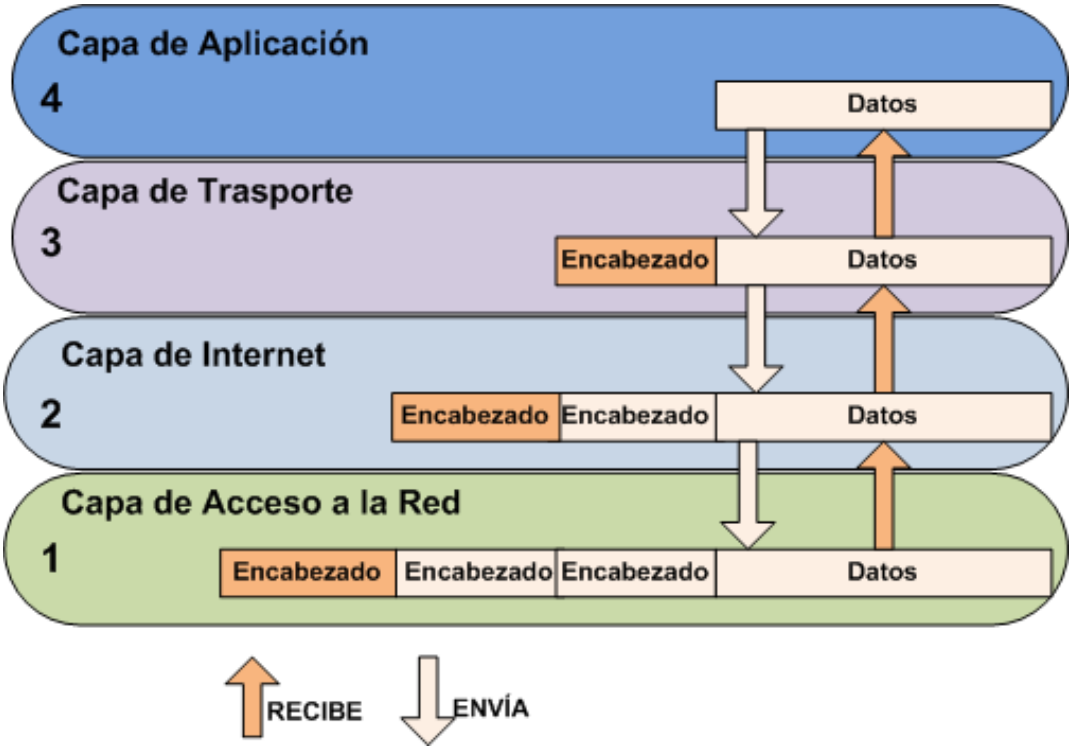


Figura 1. 6 Encapsulado de los datos.

Cada capa tiene su propia estructura de datos, la cual está diseñada para ser compatible con las capas que la rodean. Mostrando los términos utilizados por las diferentes capas para definir que los datos sean enviados, las aplicaciones utilizan TCP (Transmission Control Protocol – Protocolo de control de transmisión) para referirse a datos como un flujo (stream), mientras que las aplicaciones que utilizan UDP (User Datagram Protocol Protocolo de datagrama de usuario) llaman a estos datos paquete como mensaje (message), dentro de la capa de transporte para TCP la estructura se conoce como segmento (segment) y para UDP paquete (packet). En la capa de internet se conocen todos los bloques como datagrama tanto para TCP y UDP, y la capa de acceso a la red la estructura de datos se conoce como frame- marco (figura1.7).

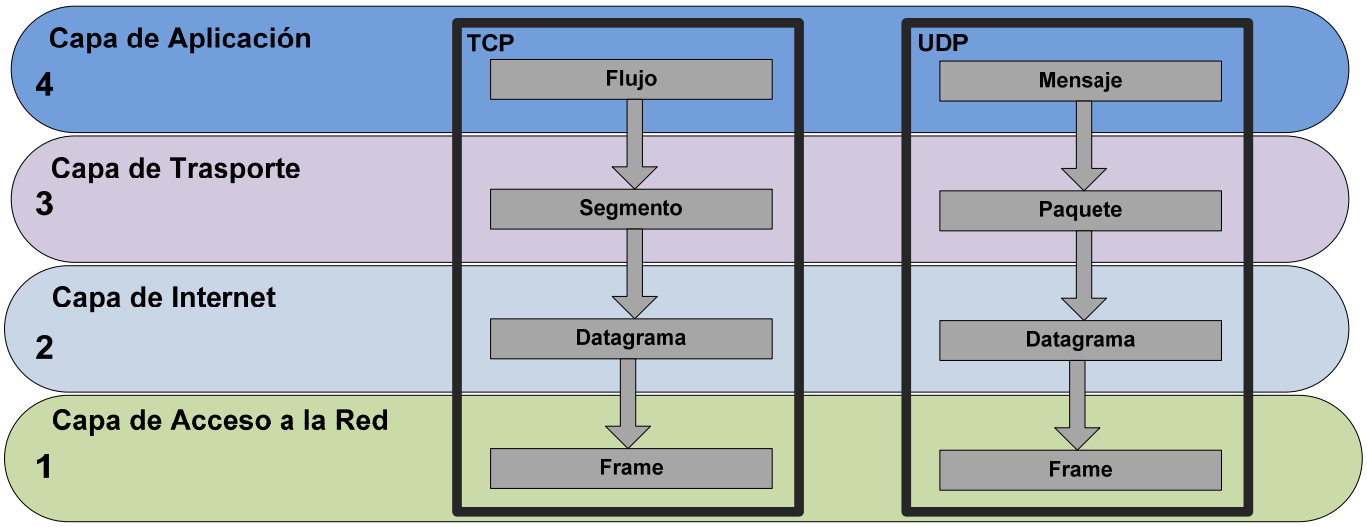


Figura 1. 7 Estructura de datos.

a) Capa de acceso a red

Es la capa más inferior del modelo TCP/IP, los protocolos en esta capa brindan el significado para que el sistema entregue datos a otros dispositivos, esta capa define cómo utilizar la red para trasmitir un datagrama IP, a diferencia de los protocolos de nivel superior, el protocolo de acceso a red deberá conocer los detalles de todo el paquete (estructura del paquete, dirección IP, MAC Address, etcétera) para que el dato pueda ser transmitido correctamente. Esta capa es equivalente a las 3 capas inferiores del modelo OSI (Red, Enlace de datos y Física) (figura 1.8).

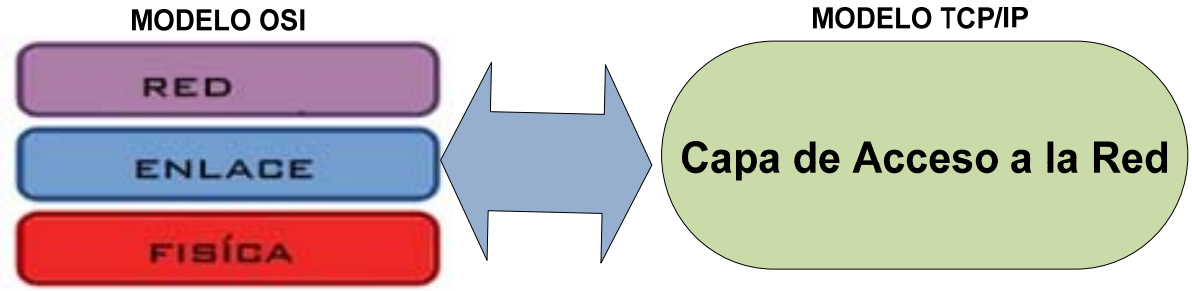


Figura 1. 8 Equivalencia de la capa de acceso a red del modelo TCP/IP con las tres primeras capas del modelo OSI.

Las funciones ejecutadas en este nivel incluyen encapsulamiento de datagramas IP dentro de los frames transmitidos, mapeo de direcciones IP a direcciones físicas *MAC Address*, dos RFC (Request For Comment – Petición de comentario) que definen protocolos en la capa de *acceso a la red* son:

- RFC 826, Address Resolution Protocol –Protocolo de resolución de direcciones (ARP).

- RFC 894, Un estándar para la transmisión de datagramas IP sobre redes Ethernet, que especifica cómo los datagramas IP son encapsulados para trasmitirse sobre redes Ethernet.

1. Protocolo ARP

Mientras TCP/IP encuentra otros equipos de cómputo en la red con base en la dirección IP única de cada equipo, la transmisión de datos tuvo que ocurrir sobre algún tipo de enlace de datos, el cual debe ser debidamente identificado y relacionado con la dirección IP, la identificación de este medio se realiza por medio del protocolo ARP definido en el RFC 826, comúnmente ubicado en la capa dos del modelo OSI o en la capa uno del modelo TCP/IP.

Las direcciones utilizadas por este protocolo se conocen como MAC Address (Media Access Control Address –Dirección de control de acceso al medio), todas las tarjetas de red para redes Ethernet tiene este identificador, constituido por 48 bits o seis números en formato hexadecimal, los primeros seis números se refieren al fabricante del dispositivo y los últimos seis representan al identificador del dispositivo, también son utilizadas por algunos routers, switches, firewalls, este número es único a nivel mundial para cada dispositivo.

Cuando una máquina envía un paquete, éste es encapsulado por el protocolo IP, el cual contiene la MAC Address de la máquina que se encuentra enviando, para obtener la MAC Address del destino del paquete, se envía un paquete ARP a todo el segmento de red preguntando por algún host con base en su dirección IP, una vez que el host destino es encontrado, éste contesta enviando la relación de su IP con la MAC Address(figura 1.9).

Source	Destination	Protocol	Info
AsustekC_3c:de:50	Broadcast	ARP	Who has 192.168.16.10? Tell 192.168.16.15
00:23:8b:19:f8:c8	AsustekC_3c:de:50	ARP	192.168.16.10 is at 00:23:8b:19:f8:c8

Figura 1. 9 Protocolo ARP.

Es importante mencionar que debido a la manera en la que trabaja el protocolo ARP, permite la ejecución de ataques de hombre en el medio, es permitido debido a la vulnerabilidad en el diseño del protocolo.

b) Capa de internet

La capa que sigue en jerarquía después del acceso a red es la capa de internet, en esta capa el protocolo IP (Internet Protocol) es el más importante, la versión de IP utilizada actualmente es la versión 4 (IPv4) definida en el RFC 791, actualmente se busca migrar IPv4 a una versión más reciente llamada IPv6 que se encuentra en crecimiento, ya que brinda mayores beneficios como lo es una gama más grande de direcciones, calidad en el servicio y seguridad desde el diseño, en este tema sólo se considera al protocolo IPv4 ya que es el estándar utilizado actualmente en la mayoría de las redes mundiales.

1. Protocolo IP

El protocolo IP (Internet Protocol – Protocolo de Internet), definido en el RFC 791 dentro de sus funciones incluye:

- Define el datagrama, que es la unidad básica de transmisión en Internet definida por el protocolo de internet (Internet Protocol).
- Define el esquema de direccionamiento de Internet.
- Mueve datos entre la capa de enlace a red (Network Access Layer) y la capa de transporte (Transport Layer).
- Determina la ruta a seguir para equipos en otro segmento.
- Ejecuta fragmentación de paquetes y re ensambla los mismos (cada tipo de red define su unidad de transmisión máxima).

Para realizar el intercambio de paquetes o datagramas, se hace uso de la dirección física (MAC Address) y la dirección IP determinada en esta capa, cada paquete viaja en la red independientemente de cualquier otro paquete. El datagrama es el paquete formado definido por el protocolo de internet el cual contiene una cabecera y los datos, esto implica que mensajes grandes como una enciclopedia sean fragmentados en mensajes más pequeños para su transporte, en la cabecera se tienen los datos necesarios para que el paquete pueda ser entregado, con base en la dirección IP destino, el datagrama está formado por 6 palabras de 32 bits cada una, como se muestra en la figura 1.10.

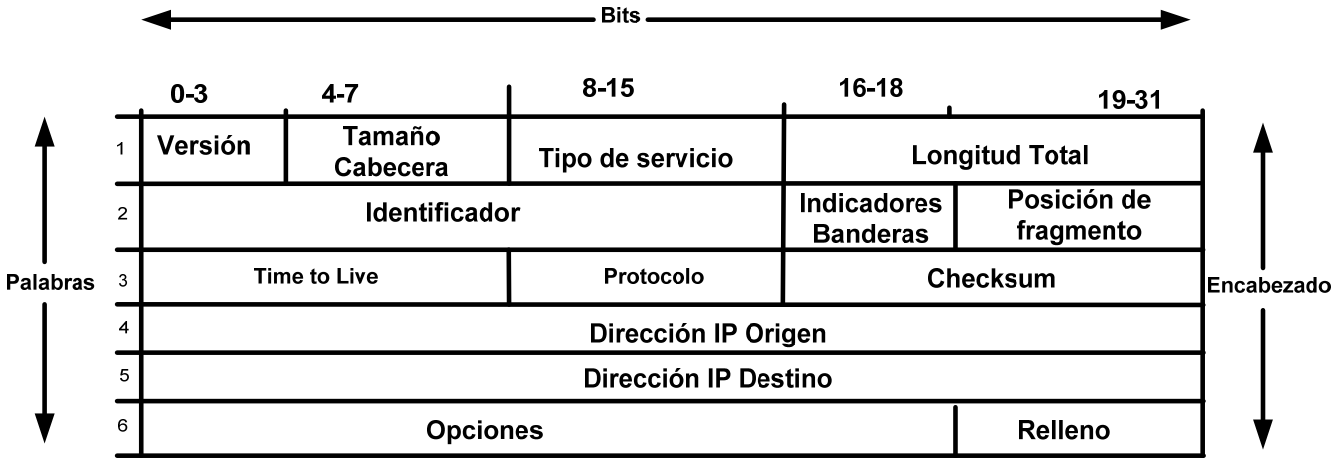


Figura 1. 10 Datagrama IP.

La cabecera IP está formada por los campos que se ilustran en la imagen anterior, cada uno tiene usos específicos que ayudan a encaminar la tarea del protocolo. En caso de que el paquete se envíe a un equipo del mismo segmento, el paquete es enviado directamente al host, si el paquete va dirigido a un equipo que no es de la red local, éste es enviado al gateway para que procese su entrega.

2. Protocolo ICMP

Una parte integral de la capa de Internet es el protocolo ICMP (Internet Control Message Protocol – Protocolo de mensaje de control de Internet) definido en el RFC 792, este tipo de protocolos realizan un seguimiento de control que determinan errores y funciones informativas de TCP/IP, además de ser un protocolo no orientado a conexión, es decir, no realiza un seguimiento de los paquetes que han sido enviados.

ICMP es un protocolo no orientado a conexión, una de sus utilidades primordiales es solucionar problemas en la red por medio de la aplicación ping, ping generalmente utiliza un paquete ICMP especial *petición – echo tipo (8)* (echo-request type (8)) en sus banderas, el cual pregunta si está activo el equipo, en caso de que el host solicitado esté disponible envía una *repetición – echo tipo (0)* (echo-replay type (0)) en sus banderas, el seguimiento de este tipo de prueba se observa en la figura 1.11.

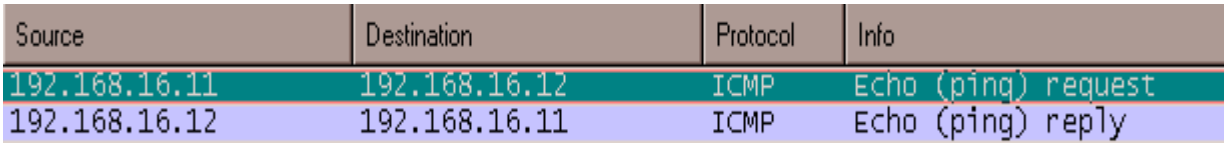


Figura 1. 11 Protocolo ICMP.

Existen en total 11 tipos de mensajes ICMP, cada que hay comunicación en la capa de internet, los cuales tienen utilidades específicas, los usos principales que se le dan a este protocolo se muestran en la tabla 1.3.

Tabla 1. 3 Mensajes ICMP.

Nombre	Descripción
Flow Control (Control de flujo).	Cuando el datagrama llega demasiado rápido para ser procesado.
Detecting unreachable destinations, (Detectando destinos inalcanzables).	Cuando un destino no es encontrado.
Redireting routes (redireccionando rutas).	Es enviado para avisar a un host que utilice otro gateway, posiblemente por mejor elección.
Checking remote host (checando host remoto).	Para verificar si un host remoto se encuentra en operación.

c) Capa de transporte

Después de la capa de Internet, está definida la capa de transporte equipo a equipo - Host to Host Transport Layer, usualmente conocida como capa de transporte, los protocolos más importantes en esta capa son protocolo de control de transmisión *TCP* y protocolo de datagrama de usuario *UDP*. *TCP* brinda servicio de entrega de datos confiable en cada punto final con detección y corrección de errores, a diferencia de *UDP* que brinda un servicio de entrega de datos sin conexión, ambos protocolos entregan datos entre la capa de aplicación y la capa de Internet.

1. Protocolo TCP

El protocolo *TCP* es utilizado en aplicaciones que requieren la garantía de entrega en sus paquetes, verificando que los datos sean entregados, por lo tanto *TCP* es un protocolo orientado a conexión, la unidad de datos intercambiada entre cada módulo de datos *TCP* es llamada segmento, cada segmento contiene un *checksum* (suma de verificación) para verificar que los datos no tengan daño, si el segmento enviado contiene daños, éste es rechazado hasta recibir un segmento en buen estado, el encabezado de este protocolo es de 32 bits formado por 6 palabras (figura 1.12).

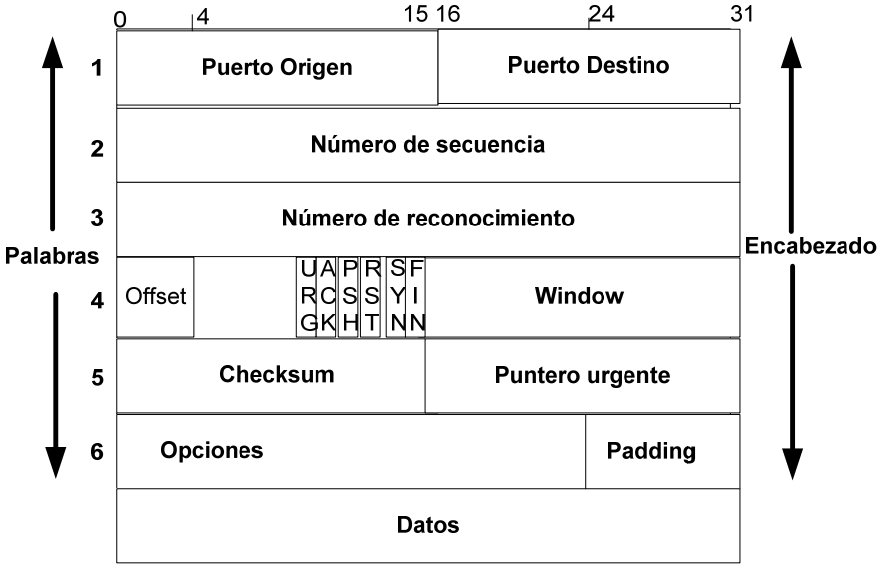


Figura 1. 12 Cabecera TCP.

El protocolo TCP establece una conexión punto final a punto final, entre dos equipos, la información de control de esta conexión recibe el nombre de handshake (saludo de mano) es un intercambio entre los 2 puntos finales para establecer un diálogo. El tipo de handshake utilizado por *TCP* recibe el nombre de Three-way handshake o (Saludo de *3* vías), porque tres segmentos son intercambiados.

TCP ve los datos que envía como un flujo continuo de bytes, no como paquetes independientes, por lo tanto *TCP* tiene cuidado en mantener la secuencia en que los datos son enviados y recibidos. El estándar *TCP* no requiere que cada sistema comience numerando los bytes con un número específico, cada sistema elige el número que éste utilizará como punto de comienzo, para mantener el flujo de datos correctamente, cada punto final debe conocer el *ISN* (Initial Sequence Number - número inicial de secuencia) del otro punto final, por razones de seguridad este número es elegido aleatoriamente.

2. Protocolo UDP

El protocolo *UDP* definido en el *RFC 768*, permite la entrega de datagramas con un mínimo de carga, es un protocolo sin garantía de entrega y no orientado a conexión, es decir, no tiene mecanismos para verificar que la información ha sido entregada al punto final, utiliza un encabezado de 32 bits donde define el puerto origen y destino en una palabra, cada uno utilizando 16 bits, el formato de mensajes *UDP* es el siguiente (figura 1.13).

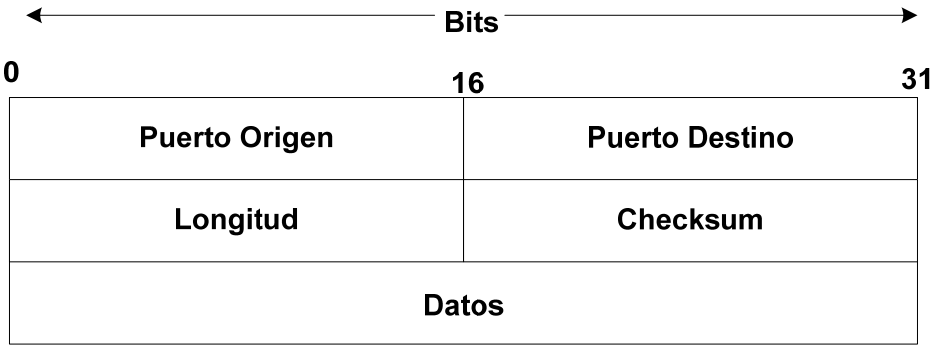


Figura 1. 13 Cabecera UDP.

Uno de los protocolos más conocidos el cual emplea como transporte *UDP* es el protocolo *DNS*, debido a las ventajas de transporte que éste brinda para su finalidad.

3. Three-Way Handshake

El Three-way handshake – saludo de tres vías, es el proceso mediante el cual el protocolo *TCP* inicializa una conexión, el *host A* comienza la conexión al enviar un segmento al *host B* con el bit *SYN* (Sychronize sequence number – Número de secuencia de sincronización) activado, este bit indica a *B* que *A* desea comenzar una comunicación con él, enviándole un número de secuencia el cual indica a *B* el número de secuencia utilizado para mantener los datos en orden apropiado. El host *B* responde al host *A* con un segmento que tiene el bit *ACK* (Acknowledgment -Reconocimiento) y *SYN* (Sychronize sequence number – Número de secuencia de sincronización) activado, el segmento *B* reconoce la recepción del segmento *A* e informa a *A* qué número de secuencia comenzará con *B*, finalmente el *host A* envía al *host B* un segmento que reconoce la recepción del segmento *B*, al término de estos tres envíos se concreta el inicio de la comunicación (figura 1.14).

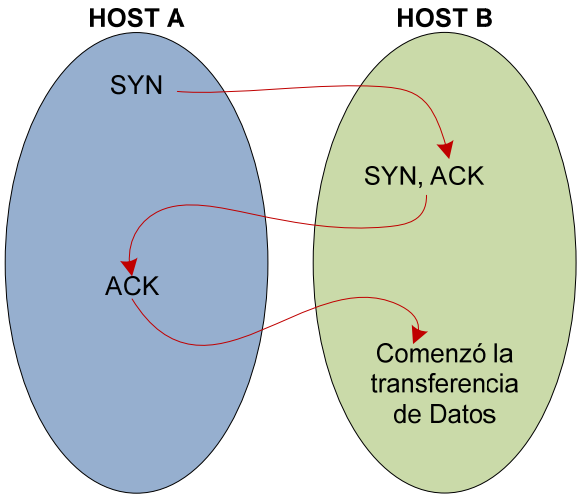


Figura 1. 14 Three-way handshake.

Después de este intercambio el *host A* tiene evidencia suficiente de que el *host B* está listo para recibir datos, tan pronto como la conexión es establecida, esta conexión se mantendrá hasta que alguno de los dos hosts envíe un segmento con la bandera de FIN (Finalize – finalizar, bandera para dar por terminada una conexión) activada, esto es el final del intercambio que brinda la conexión

lógica entre los 2 sistemas de una manera formal, aunque existe la posibilidad de concluir la comunicación con la bandera de reset.

d) Capa de aplicación

En la parte superior de la arquitectura *TCP/IP* se encuentra la capa de aplicación, esta capa incluye todos los procesos que utilizan los protocolos de la capa de transporte para la entrega de datos, aquí existen muchos protocolos de aplicación, muchos de éstos brindan servicios a los usuarios, suelen generarse nuevos servicios que se agregan continuamente a esta capa.

Los protocolos más conocidos e implementados son TELNET, *FTP, HTTP, SMTP, SMTP, POP3, DNS, SSH DHCP, NFS*, entre muchos otros que se generan con el paso del tiempo y las necesidades que surgen en el mismo.

1. Protocolo TELNET

Este protocolo está definido en el RFC 854 desde el año de 1983, conocido como *The Network Terminal Protocol – Protocolo de terminal para la red*, protocolo orientado a conexión utilizando por lo tanto transporte TCP, brinda autenticación remota sobre la red, es un protocolo inseguro ya que toda la información que viaja por este protocolo está en claro, es decir se puede interpretar todos los datos que fluyen, por lo tanto es punto fácil de ataque, actualmente ya es un protocolo muy poco utilizado pero algunos dispositivos y sistemas lo siguen utilizando como mecanismo de acceso remoto.

El protocolo TELNET le asigna al servidor el puerto 23 *TCP*, el cliente puede elegir el que desee, mayor a 1024, es muy útil cuando se desea ver alguna información que brinda un servicio por algún otro puerto conocido.

2. Protocolo FTP

Conocido como File Transport Protocol -Protocolo de transferencia de archivos, definido en el RFC 959 la primera propuesta de este protocolo data de 1971, es un protocolo simple cliente / servidor, que permite al servidor publicar un directorio para compartir sus archivos utilizado para realizar transferencia de archivos de manera interactiva, entre sus objetivos principales esta el permitir compartir archivos o datos, transferir datos confiable y eficazmente además de brindar autenticación.

El proceso de conexión es mediante el protocolo *TCP*, el servidor utiliza el puerto 21 TCP para la autenticación y la ejecución de comandos especificados en el protocolo, conocido como *control port*- puerto de control, además emplea el puerto 20 TCP para la transferencia de datos conocido como data port- puerto de datos.

El protocolo FTP tiene 3 principales debilidades, la comunicación viaja en claro, es decir, se puede interpretar a su paso por la red la información transmitida, los servidores FTP permiten conexiones anónimas en ocasiones, dicho con otras palabras, cualquier persona u equipo puede acceder a los

recursos si se tiene dicha configuración habilitada, y las vulnerabilidades propias ya conocidas de las versiones de servidores FTP que tienen que ver con errores en su programación.
Existe una versión similar conocida como *TFTP*, definida en el RFC 1350, The *TFTP* Protocol – Protocolo de transporte de archivo trivial, el cual no brinda autenticación y acceso al listado de directorios, además de emplear UDP en el puerto 69 para su transporte.

3. Protocolo HTTP

Hypertext Transfer Protocol – Protocolo de transferencia de hipertexto, definido en el RFC 2616, este protocolo es el encargado de traducir el código de los documentos *HTML* en páginas web, fue utilizado por World Wide Web – Red global mundial, desde 1990, especificado como *HTTP* /1.1, está diseñado para el acceso público, considera que la seguridad no es importante (figura 1.15).

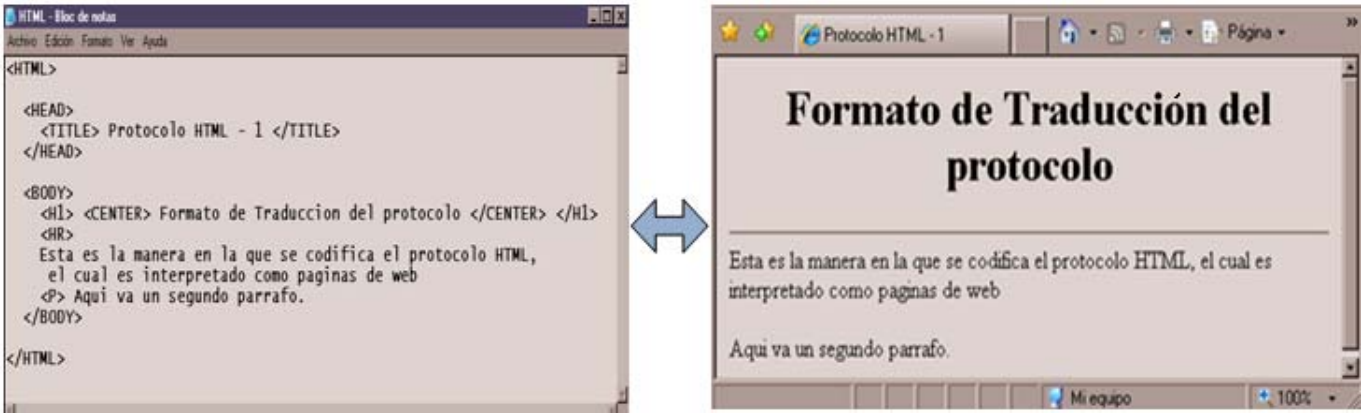


Figura 1. 15 Protocolo HTTP.

Es un protocolo orientado a conexión, utiliza el protocolo *TCP* y su servicio se brinda en el puerto 80, actualmente este protocolo combina el protocolo *HTML* con otros lenguajes de programación como aspx, php, jsp, entre otros, razón por la cual, el protocolo se vuelve más vulnerable al añadirle las vulnerabilidades propias de cada uno de los lenguajes de programación.

4. Protocolo SMTP

El protocolo Simple Message Transport Protocol – Protocolo de transporte de mensajes simple, es uno de los protocolos más utilizados ya que es el encargado del envío y recepción de correos electrónicos, actividad primordial hoy en día, está definido en el RFC 821, es utilizado para intercambiar mensajes entre servidores, su uso data de 1982, es una conexión TCP que emplea el puerto 25 para el servidor.
Además de *SMTP* existen otros protocolos de correo electrónico, como es el caso de POP (Post Office Protocol) utilizando el puerto 110 en el servidor, *IMAP* (Internet Message Access Protocol – Protocolo de acceso a mensajes de internet) utilizando el puerto 143, los tres tienen debilidades en común ya que todos envían sus mensajes y datos en claro, es decir se puede obtener fácilmente contraseñas y el contenido de los mensajes.
A la fecha muchos proveedores brindan el servicio a través de webmail, empleado los puertos 80 y 443 TCP.

5. Protocolo DNS

Todas las máquinas que trabaja sobre *TCP/IP* deben tener una dirección *IP* única para comunicarse con los otros hosts, las computadoras operan fácilmente con direcciones *IP*, a diferencia de las personas que les es más sencillo aprender un nombre, por esta razón los usuarios deberán identificar las direcciones *IP* por un nombre. En los inicios cercanos a *ARPANET* y comienzo de internet, el número de nombres de equipos conectados a la red fue pequeño, por lo tanto la traducción de nombres se realizaba por medio de un archivo llamado *HOST.TXT* que contenía el nombre y direcciones de cada host, este archivo fue alojado en un servidor a cargo de The Network Information Center –Centro de información sobre la red (*NIC*) del Instituto de Investigaciones de Stanford, como la red *ARPANET* siguió creciendo, se creó la necesidad de generar el concepto de servicio de distribución de nombres y dio origen al protocolo *DNS* (Domain Name Server –Servidor de nombres de dominio), el cual fue una manera más eficiente de distribuir los nombres de dominio, esta arquitectura fue liberada en el RFC 882 y 883. (figuras 1.16 y 1.17).

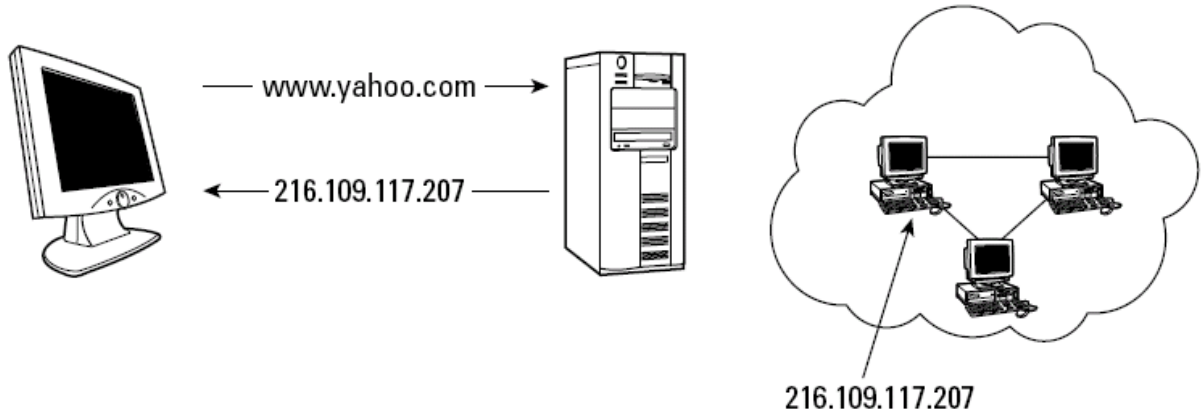


Figura 1. 16 Traducción DNS.

Este protocolo es un protocolo de traducción de nombres de dominio a direcciones *IP* y viceversa, aplicado a todos los servicios que hagan uso de los nombres de dominio como es *FTP*, *HTTP*, *SMTP*, *NetBIOS* y muchos más, está definido en los *RFC's* 1034 y 1035 actualmente, es un protocolo no orientado a conexión UDP el cual utiliza el puerto 53 del lado del servidor para atender las consultas, hoy en día a nivel mundial se cuenta con 13 servidores *DNS* raíz registrados en http://www.root-servers.org/.

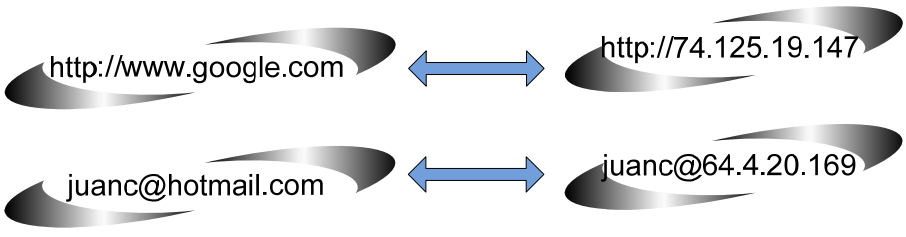


Figura 1. 17 DNS.

Dentro de los ataques a este protocolo se tiene la modificación de la base de datos del servidor, suplantación y denegación de servicio principalmente, ataques que se explicarán en capítulos posteriores.

6. Protocolo DHCP

El protocolo *DHCP* (Dynamic Host Configuration Protocol –Protocolo de configuración dinámica de host) es utilizado para asignar un conjunto de configuraciones de red, de manera centralizada y dinámica, evitando al usuario o administrador configurar los datos de cada equipo de manera manual, es un protocolo definido en el RFC 2131, no orientado a conexión UDP hace uso del protocolo *BOOTP* (Bootstrap Protocol – Protocolo Bootstrap) que es un protocolo de configuración de host anterior a *DHCP* resolviendo las limitaciones propias de *BOOTP*, ambos protocolos utilizan el puerto 67 para atender peticiones, los clientes normalmente reservan el puerto 68 dentro de los parámetros que determina este protocolo se encuentran dirección *IP*, servidor *DNS*, gateway, máscara de red.

Este protocolo fue pensado para equipos de red que cambian continuamente de ubicación, dentro de sus vulnerabilidades se tiene el seguimiento de actividades por parte de un cliente, denegación de servicio así como la posible suplantación de un servidor *DHCP* para varios propósitos (figura 1.18).

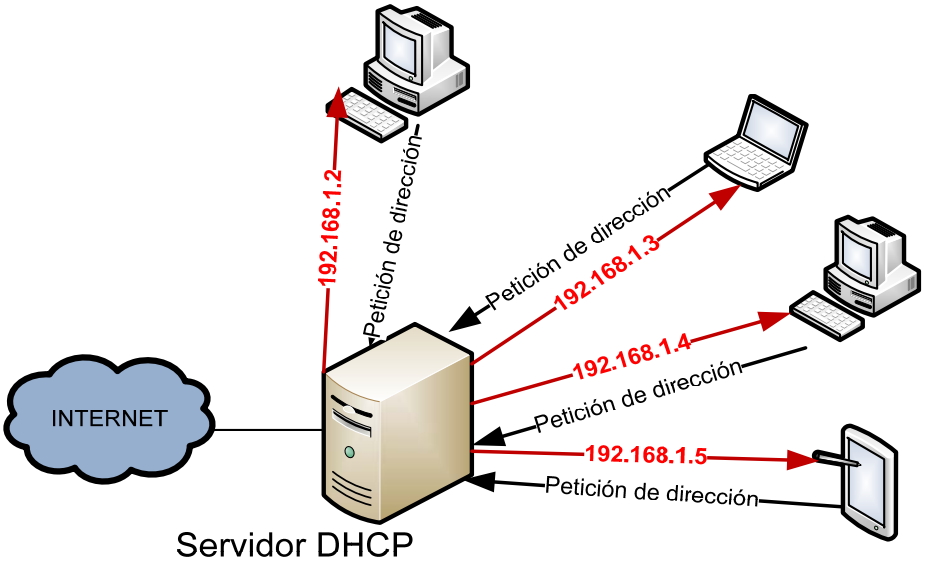


Figura 1. 18 DHCP.

1.3 Protocolo de administración SNMP

Un punto importante que debe ser considerado dentro de los protocolos tiene que ver con aquellos que pueden simplificar la administración de la red, como es el caso de los protocolos SNMP y RMON protocolos empleados para tratar de tener una mejor control.

El protocolo SNMP (Simple Network Management Protocol- Protocolo simple de administración de red) es un estándar de administración de redes ampliamente utilizado, brinda de manera centralizada la administración de hosts, servidores, switches, router, sistemas de respaldo de energía, además de sistemas operativos que tengan instalado el protocolo de administración como

es el caso de los sistemas operativos de Windows y Unix desde un equipo que tenga el software para la administración del protocolo (figura 1.19).

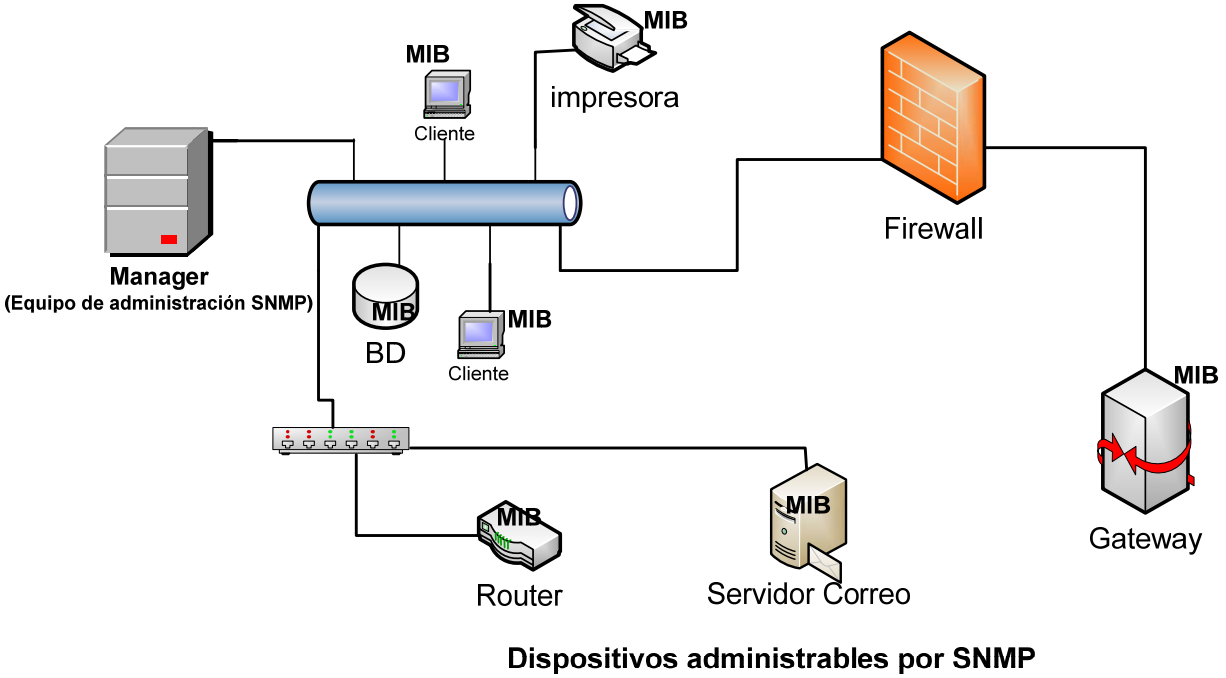


Figura 1. 19 Protocolo SNMP.

SNMP puede ser utilizado para configuración remota de dispositivos, rendimiento de la red, detectar fallas en la red o acceso inapropiado, auditoría de la red, pero una de las más importantes es el monitoreo de la red. Este protocolo consta de tres versiones hasta la fecha, la primera versión de este protocolo definida en el RFC 1157, sólo se definían comunidades, las cuales son el nombre con el cual se establece el intercambio de información entre los *agentes* que son los equipos que envían información relevante de su estado y los *managers*, equipos que se encuentran ejecutando alguna aplicación para interpretar la información enviada por los clientes y administrar la misma.

A partir de la versión uno de SNMP se determinaban tres tipos de acceso, escritura, lectura y trap *(alertas que informan algún cambio en el sistema)*, éstos dependen de la comunidad a la que se pertenezca, la mayoría de los fabricantes que brindan este servicio tienen configurado por defecto la comunidad *public* para sólo lectura y *private* para lectura y escritura, en el caso de los *traps* son alertas que emiten los equipos de comunicación para informar entre algunas cosas lo siguiente:

- Deja de funcionar una interfaz.
- Se estropea el ventilador de un router.
- Inventario y estado actual de los nodos en el segmento.
- El ancho de banda consumido en cierto intervalo de tiempo.
- La carga de procesos excede un límite.
- Se llena una partición de disco.
- Un UPS (Uninterrumtible Power Supply–Entrega de alimentación ininterrumpida) cambia de estado.

Existe más información que es entregada, pero es importante contar con un mecanismo que sólo entregue la información indispensable.

La versión 2 de este protocolo le agregó seguridad, es definida en el RFC 1905, 1906, 1907 y la versión 3, brinda las mayores opciones de seguridad que incluyen cifrado en la comunicación y autenticación segura, se recomienda la utilización de SNMP versión 3 por las opciones de seguridad que ofrece.

Este protocolo consta de tres componentes básicos llamados *manager* y *agente*, además de una base de información MIB (Management Information Base – Base Información gestionada) utiliza los puertos UDP 162 para el envío de alertas o eventos denominadas *trap* y 161 para enviar y recibir peticiones, conocidas como *query*. La MIB está definida en el RFC 1156, la cual fue actualizada en el RFC 1213, ésta contiene la estructura de la información que entrega el protocolo.

Algunas aplicaciones que son utilizadas como administradores o *managers* para el protocolo son los siguientes:

- Nagios (UNIX).
- PRTG (Windows).
- Cacti (UNIX).
- MIB Browser SolarWinds (Windows).
- Net-SNMP (UNIX).
- Netscan Tools (Windows).
- AdRem SNMP Manager (UNIX).

1.4 Protocolo de administración RMON

Entre los protocolos de administración de red además de SNMP existe el protocolo RMON (Remote Monitoring – Monitoreo remoto), la especificación de este protocolo se encuentra en el RFC 2819, sin embargo, existe una versión mejorada de dicho protocolo llamado RMON2 y sus especificaciones se localizan en el RFC 2021.

El protocolo RMON se convirtió en un estándar en 1992 y cinco años más tarde se terminó la versión RMON2, el protocolo RMON1 o simplemente RMON trabaja en la capa de enlace de acuerdo con el modelo OSI, sin embargo, RMON2 agrega nuevas capacidades ya que opera a nivel de aplicación proporcionando mayores ventajas para la administración de la red, permitiendo con ello resolver problemas de red de manera más eficiente.

Este protocolo también es capaz de recolectar datos con mayor detalle, puede ser configurado para que éste proporcione información, como utilización de la red, obtener información de los datos intercambiados entre dos equipos etcétera.

Las diferencias entre RMON y SNMP son:

- RMON es utilizado para operar en hardware.
- RMON es un protocolo proactivo capaz de enviar datos en lugar de esperar a ser analizados, permitiendo que el ancho de banda sea más eficiente.

- Es capaz de recolectar datos con mayor detalle.
- RMON puede ser implementado de distintas maneras y esto depende del tamaño o tipo de dispositivo a ser monitoreado, además de que éste reemplaza las costosas unidades analizadoras de red.

Las formas en las que puede ser implementado son:

- RMON MIB utilizada para monitorear dispositivos de hardware llamados también agentes embebidos.
- Como un módulo adicional de un dispositivo de monitoreo.

Es importante mencionar que existen otros protocolos de administración de redes adicionales a NMTP y RMON, como es el caso de Netflow (Cisco) y sflow (RFC 3176).

1.5 Protocolos utilizados en menor volumen

Existe una infinidad de protocolos y servicios que se utilizan y que se siguen utilizando, generados con base en las necesidades que van surgiendo, como todos los protocolos anteriores que tienen una finalidad específica estos también son protocolos comúnmente utilizados en un volumen menor, los cuales dependen en esencia de las actividades propias de cada institución. algunos servicios utilizados en menor volumen son escritorio remoto que utiliza el puerto 3389 TCP, secure shell utilizando el puerto 22 TCP, HTTPS utilizando el puerto 443 TCP, NetBIOS para los sistemas operativos de Microsoft utilizando los puertos TCP/135, TCP/139, TCP/445, TCP/1025-1030, UDP/137,UDP/138, UDP/445 y UDP/1025-1030, en el caso de los sistemas operativos Unix se tienen TCP/21,TCP/22, TCP/23, TCP/25, TCP/80, TCP/111, UDP/53, UDP/67-69, UDP/111, en el caso de impresoras de red 515 TCP/UDP, BD ms-SQL 1433 TCP, citrix 1494 TCP, tinbuktu 407 TCP, MySQL 3306 TCP, NTP puerto 123 UDP, IRC puerto 6667 TCP, LDAP puerto 389 TCP, RTSP entre muchos otros.

Sería una tarea muy complicada conocer todos los protocolos de comunicación que existen, pero es muy importante por lo menos saber los protocolos que comúnmente se utilizan en el segmento de red que se administra, esto con la finalidad de tener más control sobre el tráfico que se genera en el segmento de red.

CAPÍTULO 2
Conceptos Generales de Seguridad

La mejor forma de predecir el futuro es crearlo.
[Peter Drucker]

En un entorno, donde cada vez mas dispositivos se incorporan a una misma red para el intercambio de información, debemos conocer los riesgo que se generan.

La seguridad significa que el costo para romperla excede al costo del bien de cómputo asegurado, esto es, el tiempo requerido para romper la seguridad, excede el tiempo de vida útil del bien de cómputo, siendo éste último hardware, software o información.

2.1. Principios básicos de seguridad

Se ha observado que los sistemas relacionados o no con la computación tienen debilidades reales, el propósito de la seguridad en cómputo es brindar caminos para prevenir las debilidades que puedan ser explotadas en los sistemas que involucren el uso de hardware, software, transporte e información digital. Actualmente se emplea el término *Seguridad* en muchas actividades de la vida diaria, proteger las casas, pago y compras en Internet, en el automóvil, uso de controles contra desastres y en casos más especiales, hacer uso de seguros que garanticen recuperar el valor de los bienes.

Cuando se hace referencia a la palabra *Seguridad* tiene definiciones como certeza, firmeza, confianza, sin riesgo, dícese de las cosas ciertas, firmes y libres de peligro o riesgo, estado de las cosas bajo protección, confianza, tranquilidad de una persona, procedente de la idea de que no hay ningún peligro que temer.

Cuando se habla a cerca de seguridad en cómputo se hace referencia a todas las medidas para prevenir pérdidas de cualquier clase, significa que se contemplan tres aspectos básicos de cualquier sistema relacionado con el cómputo, confidencialidad, integridad y disponibilidad (figura 2.1).

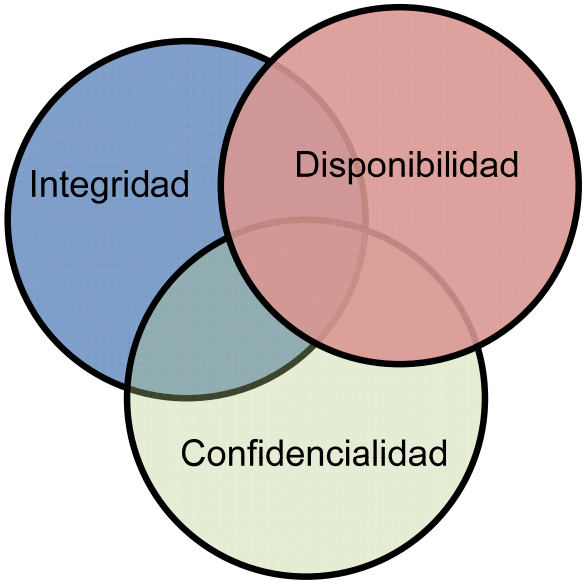


Figura 2. 1 Principios de seguridad.

La seguridad en cómputo intenta asegurar los tres principios, sobre tres activos principales, software, hardware e información, además de la comunicación entre ellos y las debilidades humanas que interactúen con éstos, esto constituye la base de la seguridad en cómputo. Realizar un análisis de la situación actual brinda el panorama para la construcción de un sistema seguro, ayuda a encontrar el balance correcto de los tres factores (integridad, disponibilidad y confidencialidad) para una implementación óptima de seguridad, al definir cuál es el pilar primordial que se desea asegurar sin dejar de pensar en los otros dos.

Como un profesional en la seguridad es importante brindar un balance entre agregar barreras de seguridad para prevenir ataques y permitir que el sistema siga siendo funcional a los usuarios. La seguridad, funcionalidad y facilidad de uso, deben ser contempladas para generar este balance. En general, cuando se incrementa la seguridad, la funcionalidad del sistema y facilidad de uso disminuyen.

1. Integridad

Significa que los activos pueden ser modificados sólo por partes autorizadas o caminos autorizados, en este contexto se incluye escribir, cambiar, modificar estado, borrar y crear.

El término integridad, tiene diferentes significados en distintos contextos, por ejemplo, si se refiere a conservar la integridad de algún elemento, puede significar que el mismo es:

- Idéntico.
- Certero, exacto.
- Sin modificaciones, alteraciones o agregaciones.
- Modificado sólo en formas aceptables.
- Modificado sólo por personas autorizadas.
- Modificado sólo por procesos autorizados.
- Consistente.
- Con sentido.

Integridad puede también significar dos o más de estas propiedades, la integridad está protegida en la mayoría de las ocasiones con controles de acceso que determinan que personas, procesos o entidades tienen acceso a los recursos para lograr escribir, cambiar, modificar, borrar y crear. En los sistemas de cómputo la integridad de los archivos es garantizada empleando algoritmos hash y firma digital.

2. Disponibilidad

Se refiere a que los activos están accesibles para las partes autorizadas en tiempos apropiados, en otras palabras, si una persona o sistema tuvo acceso legítimo a un conjunto de objetos particulares, este acceso no deberá impedirse.

Disponibilidad aplica tanto a datos como a servicios, se dice que un objeto o servicio está disponible si:

- Éste está presente en una forma útil.
- Si tiene capacidad suficiente para prestar el servicio.
- El servicio se completa dentro de un periodo de tiempo aceptable.
- El servicio involucra una filosofía de tolerancia a fallas.
- Tiene concurrencia, que es un acceso simultáneo, administrando tiempos muertos.

En sistemas de cómputo no existe una medida a tomar que garantice la disponibilidad de algún activo al 100%, por las implicaciones en gasto que puede tener esta propiedad de la seguridad, así como las nuevas debilidades que se detectan día a día en los diferentes sistemas en general. En tiempos pasados la seguridad en cómputo fue exitosa enfocándose a la confidencialidad y la integridad, la implementación de disponibilidad es uno de los siguientes grandes cambios.

3. Confidencialidad

Asegura que los activos sean accedidos sólo por partes autorizadas, es importante definir qué se entiende por "acceso", acceso no sólo se refiere a leer, sino también a ver, imprimir o simplemente conocer la existencia de un activo particular. Confidencialidad en algunas ocasiones es también llamada privacidad o secreto.

La confidencialidad es uno de los principios de seguridad que más importancia se le ha dado desde la antigüedad, en el campo militar, diplomático y político se empleaban distintas formas para transportar la información y en caso de caer en manos de un tercero éste no pudiera interpretarla.

Algunas de las maneras que se utilizan para garantizar la confidencialidad son:

- ***Valija Diplomática*** (Mecanismo empleado para enviar información de tal manera que sólo la persona involucrada pueda tener acceso a la información).
- ***Cifrado simétrico*** (Emplean una misma contraseña para ocultar y para recuperar la información).
- ***Cifrado asimétrico*** (Emplea dos contraseñas diferentes, una para ocultar la información y otra para recuperarla).
- ***Mecanismos para ocultar la información de los propietarios.***

2.2. Vulnerabilidades, amenazas, riesgo y control

Cuando se prueba un sistema de cómputo, una de las tareas principales es pensar cómo el sistema podrá tener un mal funcionamiento, de esta manera se busca mejorar el diseño del mismo. Un sistema de cómputo consta de tres componentes que se valoran por separado; hardware, software y datos, cada uno de estos activos tiene un valor propio el cual afecta al sistema de diferente manera, esta estimación es necesario realizarla ya que lleva a determinar la prioridad de atención de los activos. En este proceso intervienen cinco factores: vulnerabilidades, amenazas, riesgo, ataques y control.

Las **vulnerabilidades** son debilidades en el sistema de seguridad, por ejemplo, un procedimiento, diseño, implementación, que pueden ser explotados causando pérdidas o daños, un ejemplo claro es cuando un sistema particular puede tener acceso a datos sin autorización, debido a que éste no verifica la identidad del usuario antes de permitirle el acceso a los datos.

Una **amenaza** a un sistema de cómputo es un conjunto de circunstancias que pueden ser potencialmente causa de pérdidas o daños, para ver la diferencia entre vulnerabilidad y amenaza, se

puede considerar el siguiente ejemplo; un contenedor de agua está limitado por una pared, dicha pared presenta una fisura, el agua al subir de nivel comenzará a ejercer presión en la fisura y causará un daño a la persona que se encuentra fuera al momento que se produzca un desborde de agua, la fisura del muro es una vulnerabilidad que es aprovechada por la fuerza del agua y puede ocasionar lesiones a la persona (figura 2.2).

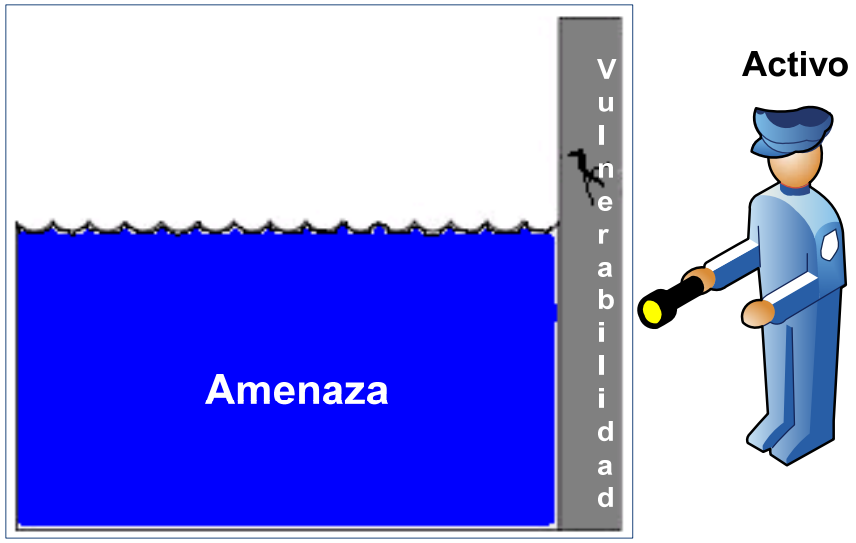


Figura 2. 2 Diagrama amenaza, vulnerabilidad y activo.

Un ***riesgo*** está definido como la probabilidad de que una amenaza explote una vulnerabilidad, además si una amenaza explota una vulnerabilidad se lleva a cabo un ataque, en el caso anterior el riesgo está definido con base en la velocidad de aumento en el nivel de agua.

El ***control o mecanismo*** se define como una medida de protección empleada, un control es un dispositivo, acción, procedimiento o técnica que elimina o reduce una vulnerabilidad, en el caso anterior se podría sellar la fisura con la finalidad de disminuir el riesgo.

Las amenazas presentan cuatro tipos básicos de operación (intercepción, interrupción, modificación y fabricación) enfocados a los tres activos de sistemas de cómputo (figura 2.3).

La ***interrupción*** se refiere a impedir la comunicación entre dos entidades, esto atenta directamente a la disponibilidad.

La ***intercepción*** permite la comunicación entre dos entidades, pero los datos que son trasmitidos pueden ser vistos por un tercero, atenta contra la confidencialidad.

La ***modificación*** involucra a una tercera entidad entre los dos punto principales de una comunicación, permitiéndole modificar la información que se transmiten en ambas direcciones, atenta contra la integridad.

La ***fabricación,*** es muy similar a la modificación, solo que en ese caso la información transmitida es completamente generada por una tercera entidad, atenta contra la integridad.

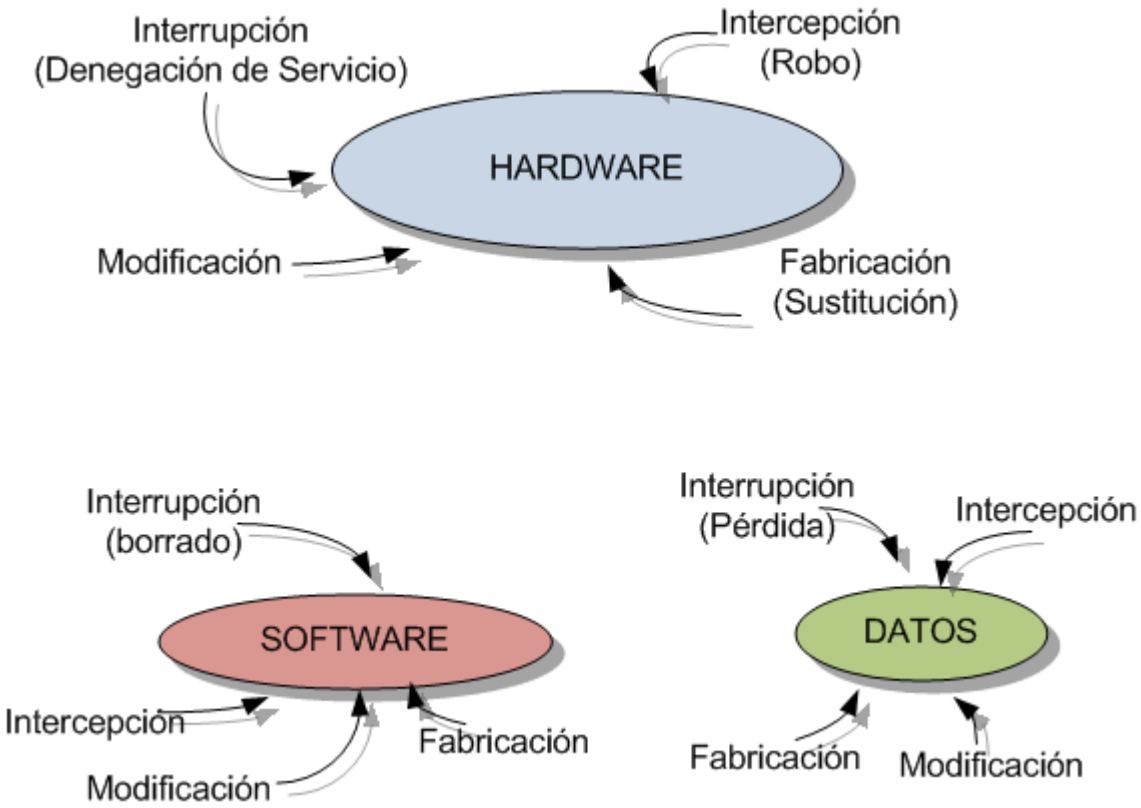


Figura 2. 3 Vulnerabilidades de los sistemas de cómputo.

Las vulnerabilidades de hardware son mayores debido a que están compuestas de objetos físicos los cuales son más fáciles de atacar, al agregar un dispositivo, cambiando el mismo, eliminándolo, interceptando el tráfico de él, inundándolo de tráfico hasta que deje de funcionar, ataques físicos al mismo, mojarlo, corto circuito, quemarlo, congelarlo y robo principalmente, sin embargo, su diseño e implementación puede colocarlo como dispositivo seguro.

Profesionales de la seguridad en cómputo repetidamente encuentran que la más grande amenaza de seguridad son de origen interno, debido a la cantidad de datos a los que tienen acceso para hacer su trabajo los empleados, además de conocer las vulnerabilidades de la institución de una manera más sencilla.[2]

El equipo de cómputo es de uso limitado si no se cuenta con software (Sistemas operativos, controladores, servicios y aplicaciones en general), cualquiera de este software puede ser reemplazado, cambiado, destruido y explotado maliciosamente o accidentalmente al provocar un comportamiento anómalo. Accidentalmente o no, las amenazas explotan las vulnerabilidades de software, En el caso de los datos, éstos pueden ser interpretados en ocasiones por el público en general, ataques a este activo tienen mayor impacto que ataques al software y hardware, ya que en ocasiones los datos se convierten en información que contiene secretos empresariales, cuentas bancarias, bases de datos inmensas con identificaciones personales, registros escolares, historias médicas y muchos más, los cuales si caen en manos equivocadas pueden provocar un daño

[2] Robert Richardson, CSI Computer Crime & Security Survey, 2008, pág. 16-17.

impresionante o al ser utilizada para provocar otros ataques a partir de la obtención, modificación y divulgación de ésta.

2.3. Ataques

Los ataques son la culminación de una amenaza al explotar una vulnerabilidad, estos en general son acciones que atentan contra la disponibilidad, integridad y confidencialidad de algún activo, éstas son las razones primordiales por las cuales actúa la seguridad buscando limitar la acción de éstos o minimizando su alcance, pueden ser realizados de diferentes maneras como robo, ingeniería social, ataque remoto, acceso físico, ataques internos, penetración, entre otros, así como por diferentes tipos de entidades, humanas, lógicas y naturales.

En general los ataques son producidos por diversas entidades físicas y lógicas, dentro de las físicas se encuentran las personas que buscan realizar algún daño, a éstas se les conoce como atacantes o perpetradores en términos generales (Véase apéndice A).

La consecuencia de los ataques depende del tipo de impacto sobre el activo, algunas de las más comunes son:

- Pérdidas económicas.
- Pérdida de imagen pública.
- Responsabilidades legales.
- Daño o pérdida de la vida.
- Incumplimiento de acuerdos de servicio para el público o departamentos de gobierno.
- Violación de acuerdos de confidencialidad.
- Incapacidad para llevar a cabo tareas críticas.
- Modificación o pérdida de datos.

El impacto es una representación del daño o percepción de los daños, una vez que se ha culminado el ataque, en relación con la confidencialidad, integridad y disponibilidad.[3]

Para llevar a cabo un ataque se requiere una planeación previa del mismo, es decir, el atacante debe contar con un esquema en el cual se detalle el objetivo y la metodología a emplear, actualmente las razones por las que un atacante desea concretar un plan de ataque son principalmente obtener ganancias económicas y fraudes.

Los ataques comprometen directamente la integridad, confidencialidad y disponibilidad de un sistema o red, en mayor volumen actualmente son virus, accesos no autorizados a recursos digitales, phishing, pharming, DoS, bots, abuso de redes wireless, ataques a DNS, sniffers.[4]

Muchas de las herramientas utilizadas para ejecutar ataques son herramientas empleadas en el campo de la administración, adicional a esto, hay herramientas de uso dedicado para obtener un

[3] Mike Horton Clinton Mugge, Hacknotes network security, McGraw-Hill, 2003, pág 30.
[4] Robert Richardson, CSI Computer Crime & Security Survey, 2008, pág. 19.

beneficio directo, algunas de estas herramientas son *ping, traceroute, whois, finger, rusers, nslookup, rcpinfo, telnet, dig.*

2.3.1. Fases de un ataque

Para llevar a cabo un ataque se sigue una metodología, ésta consta de cinco pasos y está definida por *Certified Ethical Hacker* – Hacker Ético Certificado, reconocimiento, escaneo, obtención del acceso, manteniendo el acceso y encubrimiento de rastros, esta metodología se contempla sólo para ataques lógicos aunque puede ser adaptada para ataques físicos (figura 2.4).[5]

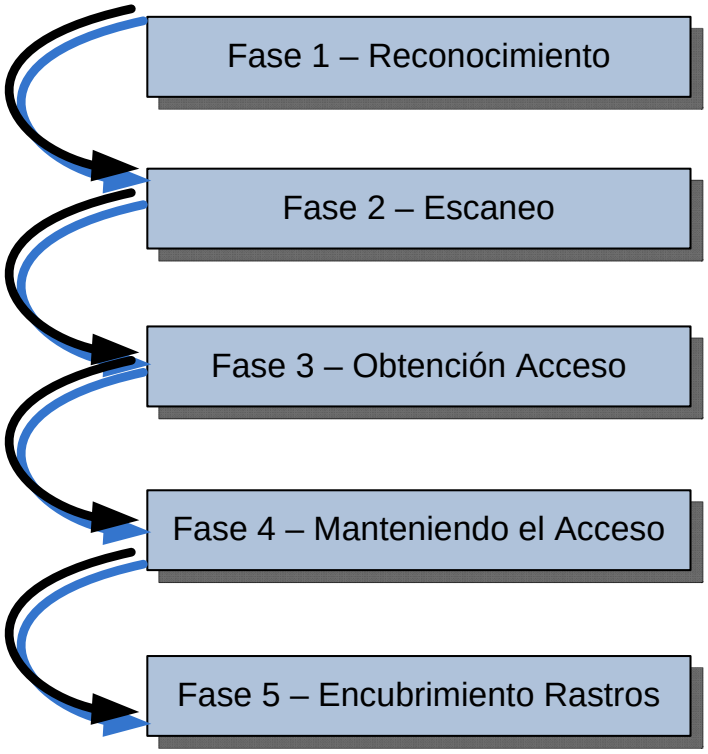


Figura 2. 4 Fases de un ataque.

Los ataques en general tienen dos clasificaciones (figura 2.5), en el caso de la primera se dividen en ataques internos y externos, ésta se refiere al origen donde se lleva a cabo el ataque, es decir, desde el interior de la organización o desde el exterior. En la segunda clasificación intervienen ataques pasivos y activos, los pasivos son ataques que sólo intentan obtener información del sistema sin provocar perturbaciones en él, atentando únicamente en contra de la confidencialidad, a diferencia de los activos que modifican el estado de integridad, disponibilidad y confidencialidad del sistema.

[5] Kimberly Graves, CEH Official Certified Ethical Hacker, Sybex 2007 pág. 31.

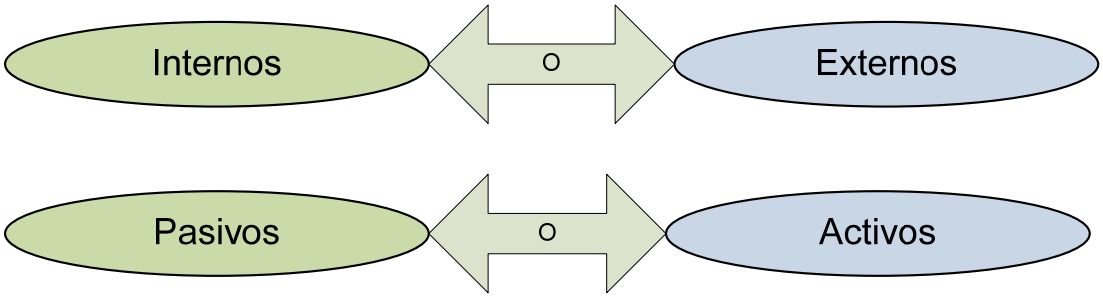


Figura 2. 5 Tipos de ataques.

En la ***fase uno reconocimiento***, se involucra la obtención de información que se encuentra de manera pública del objetivo, se emplean dos tipos de reconocimiento: pasivo y activo. En el caso de los reconocimientos pasivos, éstos consisten en obtener información sin alterar los principios básicos de la seguridad, como métodos de implementación se utilizan búsquedas en Internet, google y en el sitio de la organización donde muestre información sin autenticarse, como es directorio de ejecutivos, características del software empleado en su sitio, principalmente, también es llamado obtención de información, la ingeniería social y dumpster diving (husmear en la basura para localizar documentos importantes) se consideran métodos de obtención de información pasiva. Observar el tráfico de la red es otra forma de reconocimiento pasivo, ya que no se generan paquetes adicionales que puedan observarse, pero existen otros métodos de detección para estos casos, siendo éste un campo de información muy útil, ya que dentro de la información que se brinda están los rangos de IP, convención de nombre, servidores o redes ocultas.

El reconocimiento activo involucra el descubrimiento de la red sobre hosts individuales, direcciones IP, servicios, versiones de los servicios, sistema operativo, observar el trafico de red, servidores, redes ocultas o intranets, principalmente, este tipo de escaneo genera un riesgo mayor al crear paquetes en la red para obtener información, este tipo de reconocimiento puede darle al atacante indicadores de medidas de seguridad empleadas en el lugar como es el caso de los firewalls.

Dentro de la fase dos, ***escaneo***, se toma la información descubierta durante la fase de reconocimiento y se utiliza ésta para examinar la red. Algunas de las herramientas que se emplean para esta fase pueden incluir escaneo de puertos, mapeo de red y escaneo de vulnerabilidades.

En la fase tres***, obtención del acceso,*** se lleva a cabo el ataque real, las vulnerabilidades descubiertas durante el reconocimiento y el escaneo, la información encontrada es explotada para obtener acceso, los métodos principales que se emplean en esta fase son el acceso local a una computadora, Internet, acceso fuera de línea, denegación de servicio, robo de sesión, entre otros. [6]

Manteniendo el acceso es la cuarta fase, una vez obteniendo el acceso se busca generar un mecanismo que permita ingresar al sistema para generar ataques futuros, en ocasiones los mismos atacantes protegen al equipo para evitar que otros puedan atacarlo una vez que se tiene acceso a éste, cuando el equipo es comprometido se le conoce como un sistema zombi.

[6] Para información detallada véase el apéndice A.

La última fase, ***encubrimiento de rastros***, es empleada para evitar ser detectado por el personal de seguridad de la institución o del equipo, busca eliminar toda evidencia que se genere al momento de realizar el ataque para anular acciones legales, algunos de los elementos que buscan eliminar o modificar en esta fase son las bitácoras, alarmas en IDS (Intrusion Detection System – sistema detector de intrusos), registros en firewalls, horario de ingreso a un sistema, cuentas de usuario y log de un sistema.

2.3.2. Ataques físicos

La seguridad física es el área más crítica de la seguridad en las tecnologías de la información, si una organización falla en la adecuada implementación de la seguridad física, entonces todos los otros mecanismos de seguridad implementados como firewall, VPN, cifrado, firmas digitales, entre otros, pueden ser evitados. Los ataques por medios físicos abarcan amenazas ocasionadas tanto por el hombre como por la naturaleza (incendios accidentales, tormentas, temblores, condiciones climatológicas e inundaciones), algunos ejemplos de ataques físicos provocados por el hombre contemplan el robo, corte de suministro eléctrico, amenazas ocasionadas involuntariamente, acciones hostiles, robo, fraude o sabotaje.

Es muy importante ser consciente que aunque la organización sea la más segura desde el punto de vista de ataques lógicos, la seguridad será nula si no se ha previsto combatir un daño físico, como lo es un incendio. La seguridad física es uno de los aspectos más olvidados al diseñar un sistema informático, esto puede derivar en que para un atacante sea más fácil perpetrar físicamente que lógicamente, algunos de los ataques físicos más comunes se muestran en la tabla 2.1 donde se relaciona la amenaza con el principio de la seguridad que busca vulnerar.

Tabla 2. 1 Amenazas Físicas.

Amenaza	Atenta contra
Terremoto	Disponibilidad
Fuego	Disponibilidad
Inundación	Disponibilidad
Fallas de alimentación	Disponibilidad
Tornado	Disponibilidad
Temperatura	Disponibilidad
Robo	Confidencialidad, disponibilidad
Modificación	Integridad

Para los ataques físicos realizados por el hombre la medida más empleada para combatirlos es el control de acceso, al implementar controles de acceso por medio de guardias, detectores de metales, utilización de sistemas biométricos y mecanismos de autenticación generales, en el caso de los ataques físicos de carácter natural, éstos no se pueden prever pero sí estudiar su posibilidad de aparición con base en un estudio de las características geográficas donde se encuentre la institución.

Tener controlado el ambiente y acceso físico permite disminuir siniestros, trabajar mejor manteniendo la sensación de seguridad, descartar falsas hipótesis si se producen incidentes, tener los medios para responder frente a un incidente.

Los ataque físicos son provocados de manera intencionada, siniestros, por desconocimientos de los usuarios y desastres naturales, los más comunes son:

- Falta de controles de acceso físico.
- Fallas eléctricas.
- Alteraciones del entorno como temperatura, niveles de humedad o presión.
- Inundaciones, incendios, terremotos.
- Salud física del administrador de los sistemas.

2.3.3. Ataques lógicos

Esta categoría se asigna a todos los ataques que explotan las debilidades de los protocolos empleados y el software en general, los protocolos de comunicación y el software carecen en su mayoría de seguridad o ésta ha sido implementada en forma de parche tiempo después de su creación. Debido a que la creación de protocolos y software nuevo es creación del hombre, tienden a tener errores en sus primeras versiones, algunos ejemplos de las debilidades lógicas más comunes son:

- Fallas en el diseño de las arquitecturas de hardware.
- Fallas de seguridad en los sistemas operativos.
- Fallas de seguridad en las aplicaciones.
- Errores en las configuraciones de los sistemas y dispositivos.
- Los protocolos de comunicación tienen debilidades.
- Los usuarios carecen de información respecto a la seguridad de la información.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un sistema informático, dentro de los ataques lógicos más comunes se encuentran: spam, virus, gusanos, pharming, phishing, robo de identidad, keyloggers, hombre en el medio, botnet, enumeración.[7]

Un paso importante que debe realizar una organización es el mapeo de cada amenaza contra qué pilar de la seguridad (integridad, confidencialidad y disponibilidad) atenta, algunas de éstas son mostradas en la tabla 2.2.

[7] Amenazas Lógicas - Tipos de Ataques, http://www.segu-info.com.ar/ataques/ataques.htm

Tabla 2. 2 Amenazas Lógicas.

Amenaza	Atenta contra
Denegación de Servicio	Disponibilidad
Código malicioso	Confidencialidad, disponibilidad e integridad
Acceso no autorizado	Confidencialidad
Phishing	Confidencialidad, disponibilidad e integridad
Errores humanos	Confidencialidad, disponibilidad e integridad
Errores de programación	Confidencialidad, disponibilidad e integridad
Errores de transmisión	Integridad, disponibilidad
Ingeniería social	Confidencialidad, disponibilidad e integridad

Las organizaciones no se pueden permitir el lujo de denunciar ataques contra sus sistemas, pues el nivel de confianza de los clientes bajaría enormemente, la mayor parte de éstos no se reportan. Se busca con frecuencia que los administradores tengan cada vez mayor conciencia respecto a la seguridad de sus sistemas, pero esto no es en todos los casos, actualmente existe diferentes fuentes de apoyo para implementar seguridad como nuevas herramientas de seguridad en el mercado, los *advisories* (documentos explicativos) sobre los agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT (Computer Emergency Response Team – Equipo de respuesta a incidentes de cómputo), securityfocus (organización dedicada para facilitar la discusión de temas relacionados con seguridad en cómputo), SANS Institute (organización líder en entrenamiento de seguridad en cómputo) entre otros, todo esto ha dado frutos e incrementado los niveles de seguridad.

La importancia de conocer los ataques que existen y la manera de operar de cada uno de ellos es una de las responsabilidades que recae en los profesionales de la seguridad de la información, por lo que es recomendable que se cuente con un panorama técnico de la manera de operar de los ataques, los ataques lógicos es una clasificación que se da a todos aquellos que se realizan por medios digitales, servidores, computadoras, teléfonos celulares, redes cableadas e inalámbricas. Los principales ataques lógicos se describen a continuación:

1. **Password cracking**[8]

Tomando en cuenta el uso de contraseña como el mecanismo de autenticación más utilizando, es muy común que personas ajenas intenten obtener dicha contraseña utilizando distintas técnicas. Password cracking consiste en romper o encontrar la clave de acceso de un sistema, al cual no se

[8] Para mayor detalle ver apéndice B

tiene autorización para ingresar, generalmente se utilizan técnicas como fuerza bruta, ataque de diccionario, estadísticos, determinado por medio de algoritmos definidos.

2. **Malware**[9]

Es el término que se le da al software malicioso, el cual tiene como objetivos principales, dañar, alterar o eludir un equipo de cómputo o funciones de red.

Este tipo de software pude ser móvil como aplicaciones applets de Java, controles ActiveX, troyanos, que además pueden propagarse por la red así como cambiar la funcionalidad de programas útiles, en general, cualquier tipo de software diseñado con la finalidad de dañar es considerado como malware.

3. **IP Spoofing**[10]

Suplantación de IP, es una técnica utilizada por los intrusos para sustituir la dirección IP origen de un paquete, esto se consigue con programas principalmente destinados para ello con la finalidad de reducir la oportunidad de ser detectado pero en realidad se está suplantado a un equipo verdadero, la suplantación de identidad implica una alteración de un paquete a nivel TCP.

En este tipo de ataque entran en juego tres máquinas: un atacante, una víctima, y un sistema suplantado que tiene cierta relación con la víctima; para que el intruso pueda conseguir su objetivo necesita por un lado establecer una comunicación falsa con su objetivo y por otro evitar que el equipo suplantado interfiera con el ataque.

4. **Fingerprinting**[11]

Se refiere a la obtención de huellas dactilares, es una variante del escaneo que permite de manera rápida y con un alto grado de certeza obtener el tipo de sistema operativo, versión de una aplicación o protocolo que un equipo está utilizando, entre otros, por medio de la información que se brinda al momento de hacer una comunicación entre equipos, esta información específica por lo regular el nombre y versión del servicio como FTP, e-mail, servidores web, esta técnica permite que el atacante encuentre las vulnerabilidades específicas de la versión del sistema operativo o software utilizado permitiéndole ver cuál es el camino más sencillo para obtener acceso al objetivo.

5. **DoS**[12]

El ataque DoS (Denial of Service - denegación de servicios) se enfoca a negar, alentar o saturar un servicio por varios motivos debido a demasiadas peticiones o envío de paquetes, saturación de red, memoria, procesador y espacio de almacenamiento.

[9] Para mayor detalle ver apéndice B
[10] Para mayor detalle ver apéndice B
[11] Para mayor detalle ver apéndice B
[12] Para mayor detalle ver apéndice B

El ataque DoS puede ser causado por inundación de peticiones, es decir, que el servidor atiende demasiadas conexiones simultáneas a tal grado que llega un momento en que no es posible atenderlas o saturar el tráfico en el segmento de red, se puede presentar el mismo caso cuando se transfieren grandes cantidades de archivos al disco duro de un sistema con el objetivo de agotar el espacio del disco duro, ejecutar una aplicación que consuma muchos recursos de su memoria RAM hasta llegar a su límite, una aplicación que consuma el poder de procesamiento de un equipo hasta bloquearlo.

6. Envenenamiento ARP[13]

El protocolo ARP es parte de la pila de protocolos TCP/IP y es el responsable de traducir la dirección hardware del nivel de enlace (MAC) a partir de la dirección IP. El ataque como su nombre lo indica, va dirigido a este protocolo, una máquina cuando intenta establecer una comunicación con otro equipo, envía una petición de la dirección MAC con base en la dirección IP del otro equipo si cuenta con su dirección MAC en la caché (tabla dinámica o estática en un equipo que mapea las direcciones IP con una dirección MAC correspondiente) no pregunta por ésta, en caso contrario, envía un broadcast solicitando la dirección MAC de la IP correspondiente, pero este proceso puede ser intervenido y con esto el tráfico realizado entre dos equipos pasa por un tercer equipo .

El ataque se basa en envenenar la caché *ARP* de los dos nodos cuya comunicación se desea intervenir con información falsa haciéndole creer al host origen que la MAC del destino es la MAC de la máquina atacante. De este modo, el tráfico generado entre ambas máquinas tiene como destino la máquina atacante y desde la cual los paquetes son reenviados al destino real, evitando así la detección del ataque, (figura 2.6).

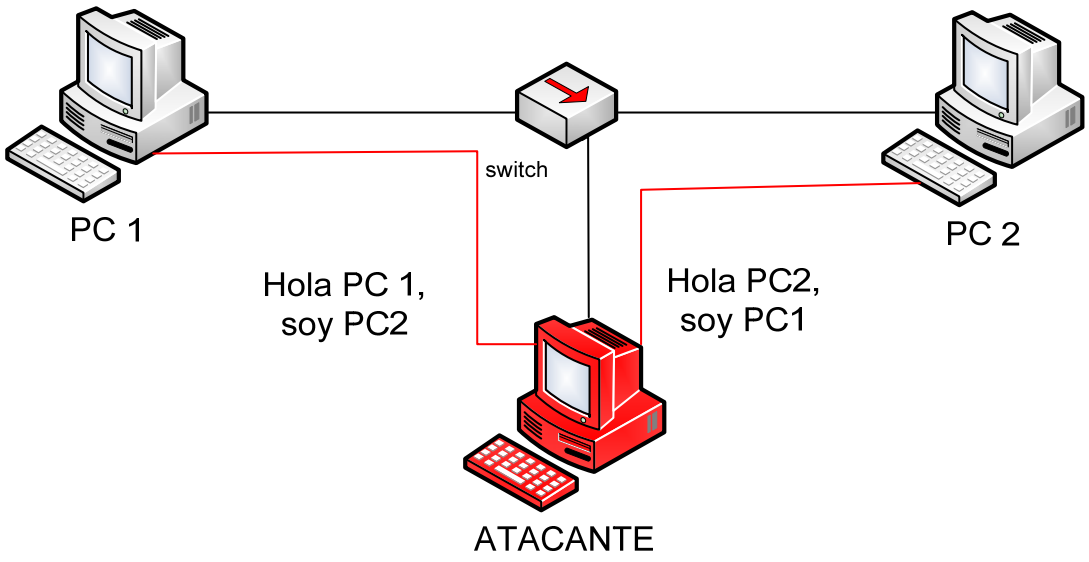


Figura 2. 6 Envenenamiento ARP.

[13] Para mayor detalle ver apéndice B

Pharming

Es la explotación de una vulnerabilidad en el software de los servidores DNS o en los equipos de los propios usuarios, dentro de los archivos que resuelven el protocolo DNS, permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta, de esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido accederá en su explorador de Internet a la página web que el atacante haya especificado para ese nombre de dominio.

La manera en que funciona dicha técnica es la siguiente, un intruso crea un sitio web, posteriormente envía un correo con contenido malicioso, el destinatario recibe y abre dicho correo, al ejecutarlo el código malicioso puede modificar los DNS con la finalidad de re direccionar al usuario a un sitio no seguro a través del cual puede obtener información (figura 2.7).

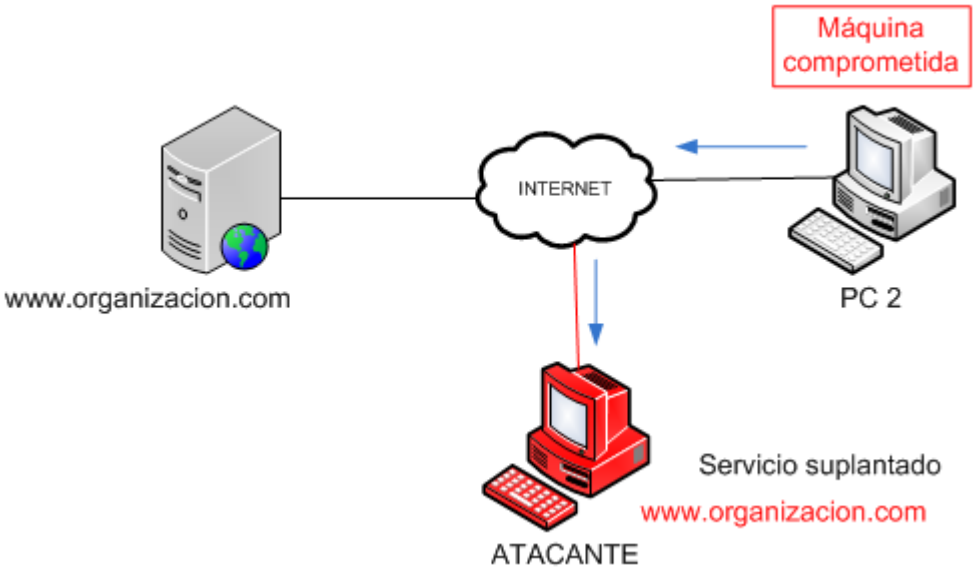


Figura 2. 7 Pharming.

7. Phishing[14]

El phishing es una modalidad de estafa diseñada con la finalidad de robar la identidad, consiste en obtener información de manera ilegal de un usuario, como lo son cuentas bancarias así como cualquier tipo de información que pueda ser de utilidad. Dado que los mensajes y los sitios Web que envían los atacantes parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

La forma de operar es a través de correos electrónicos o ventanas emergentes enviados a la víctima haciéndola creer que provienen de una organización legítima o captando su interés con información que permite engañarla al emplear ingeniería social combinada con la suplantación de identidad,

[14] Para mayor detalle ver apéndice B

haciendo que el usuario crea ingresar al servidor original debido a que accede a paginas idénticas a las que desea visitar (figura 2.8).

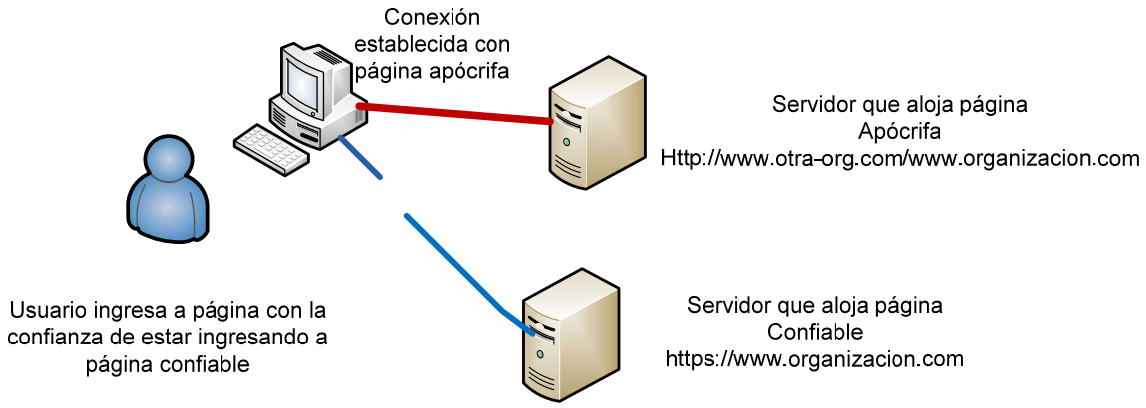


Figura 2. 8 Phishing.

8. Botnet[15]

Equipos comprometidos y controlados por un equipo maestro, son utilizados para aumentar la capacidad de cómputo, así como el poder de los ataques, se han buscado nuevas formas, para lograr reducir el tiempo de ataque y aumentar su efectividad, una botnet es una manera de aumentar el poder de cómputo y con ello la capacidad de realizar un ataque en menos tiempo.

Una botnet puede estar formada por algunos cuantos equipos o por millones de ellos, son difíciles de detectar, usualmente se propagan a través de archivos troyanos, virus, gusanos, incluso con el solo hecho de visitar una página, el usuario podría formar parte de una botnet y no estar enterado. Estas redes son tan famosas a tal grado que son compradas o rentadas por aquellos que deseen obtener algún tipo de beneficio (figura 2.9).

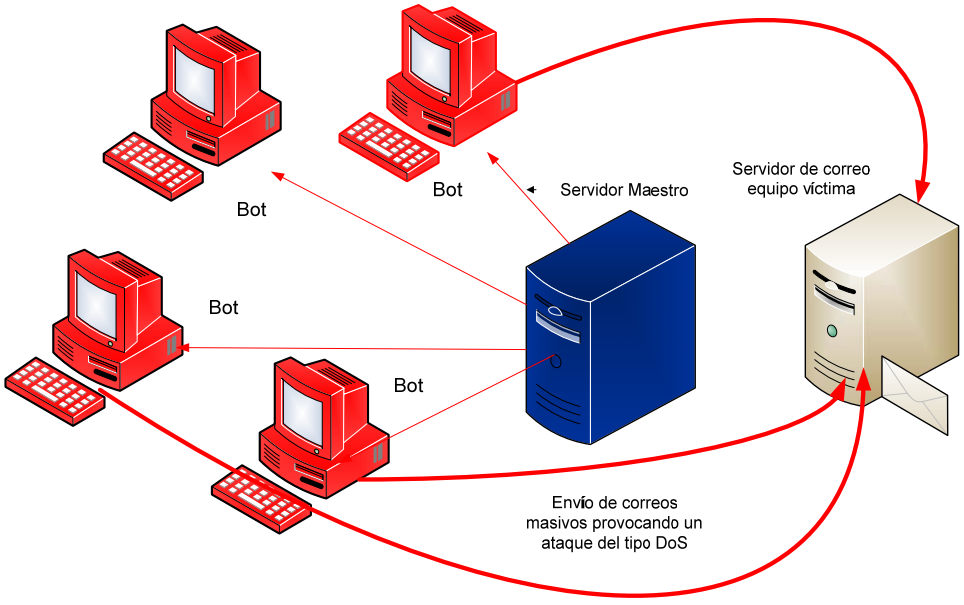


Figura 2. 9 Botnet.

[15] Para mayor detalle ver apéndice B

9. Man in the middle

Man in the middle significa hombre en el medio (MitM) es el término que se utiliza para describir un tipo de ataque, a través de esta técnica el intruso puede modificar a voluntad los mensajes o información que se está transmitiendo a través de la red entre dos entidades, es difícil que los usuarios se percaten de este tipo de ataque. En éste participan tres entidades, los dos usuarios que están intercambiando información y el atacante (figura 2.10).

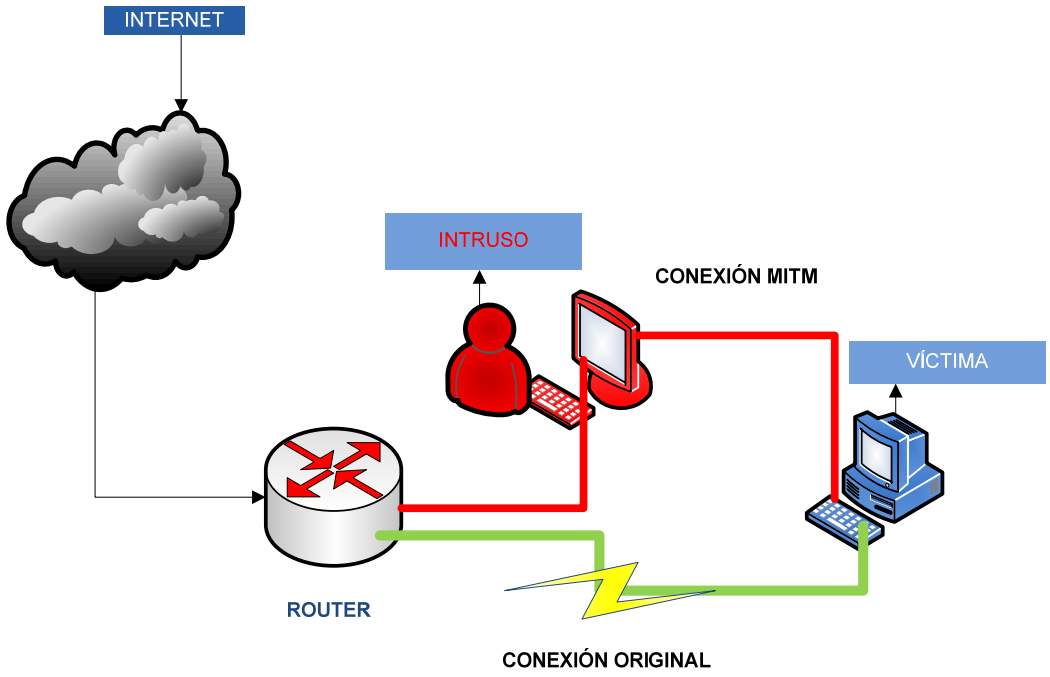


Figura 2. 10 Man in the middle.

Algunos ejemplos de ataques Man in the middle comunes son: ARP spoofing, DNS spoofing, DHCP spoofing. Existen en la red programas y basta información acerca de cómo protegerse de este tipo de ataques, algunos de ellos son: Ettercap, dsniff y fragrouter.

10. SQL injection[16]

SQL (*Structured Query Language - Lenguaje de Consulta Estructurado)*, es un estándar de ANSI para las consultas a bases de datos utilizado en manejadores como Oracle, SQL server, Postgres, MySQL, entre muchos otros más, éste lenguaje permite obtener información almacenada en las bases de datos, por ejemplo, obtener la lista de empleados de una institución, nóminas y en general cualquier tipo de información que se encuentre almacenada en una base y pueda ser de utilidad.

Sin embargo, los intrusos le han encontrado otra finalidad, por ejemplo, un usuario malicioso que intente entrar a un sitio en la red donde se necesite autenticar podría enviar una sentencia SQL en el campo del usuario o contraseña e inferir (obtener información confidencial a partir de datos no

[16] Para mayor detalle ver apéndice B

confidenciales) para intentar obtener información o entrar al sistema, por lo que estos ataques están dirigidos a los sitios web que hagan uso de bases de datos.

11. Backdoors[17]

Es una técnica utilizada por los intrusos para garantizar un futuro ingreso a un sistema con mayor facilidad, las puertas traseras se instalan una vez que el equipo ha sido comprometido, dejar una puerta trasera permite al usuario ingresar al equipo de manera más sencilla y sin que sea detectado.

Una de las características de las puertas traseras, es la capacidad que tienen para remover evidencias de su existencia, ya que no queda un registro en las bitácoras del sistema, pero una vez que el intruso hace uso de ella es posible detectarla.

12. Rootkits[18]

Los rootkits son un conjunto de herramientas que pueden ser utilizados para obtener el acceso a un sistema con privilegios de administrador y a los recursos de una computadora así como también esconder la presencia de los procesos que forman el rootkit en la máquina de la víctima.

Este tipo de técnica, es ejecutado después de haber comprometido un equipo por diferentes motivos como son, troyanos, ejecutar archivos adjuntos que vienen en un correo electrónico, conectar dispositivos con configuración de auto ejecución a un equipo, buffer overflow y otros ataques lógicos más que permitan acceso a los sistemas. Cada conjunto de herramientas (rootkits) es diseñado para una plataforma específica, tipo y versión, por ejemplo, los troyanos que oculten procesos al ejecutar comando como ps, netstat, puertos abiertos, puertas traseras (intetd), sniffers así como programas que eliminen bitácoras.

13. Footprinting[19]

Realizar un ataque implica distintas etapas ya mencionadas anteriormente, una de ellas es la recolección de información utilizando técnicas como la obtención del rastro de información a través Internet (footprinting), uno de los propósitos fundamentales de esta técnica es analizar los caminos para poder tener acceso a un equipo o sistema. La información obtenida permite al intruso conocer las vulnerabilidades del sistema y con ello las herramientas a utilizar contra dichas vulnerabilidades.

Dentro del proceso de esta técnica, no sólo consiste en conocer información acerca del sistema, también se incluye información como mapas de la red, localización física del equipo o persona, además de información del personal que ahí labore, la cual le podría ser de utilidad para aplicar ingeniería social.

[17] Para mayor detalle ver apéndice B

[18] Para mayor detalle ver apéndice B

[19] Para mayor detalle ver apéndice B

14. Escaneos[20]

El escaneo forma parte de la recopilación de información, ya que haciendo uso de ésta técnica, el intruso puede obtener mayor información que le facilite el acceso a una red o sistema, durante un escaneo se puede obtener información como la dirección IP, el tipo de servicios, así como aplicaciones instaladas con la finalidad de elegir el exploit adecuado para explotar alguna debilidad que presenten.

15. Enumeración

Después del escaneo, la etapa siguiente es la enumeración la cual consiste en organizar la información recopilada como lo es nombres de usuario, nombres de equipos, redes, puertos abiertos, sistema operativo utilizado, obtener este tipo de información requiere de una constate interacción entre el sistema y el intruso, razón por la cual puede ser identificado.

Uno de los principales objetivos de la enumeración es identificar cuentas de usuarios con suficientes privilegios, ya que el contar con una cuenta que tenga más privilegios permite escalar de manera más rápida a los siguientes niveles.

Muchas de las herramientas utilizadas están diseñadas para analizar redes IP que contienen información del NetBIOS (Network Basic Input/Output System -especificación de interfaz para acceso a servicios de red), nombre del equipo, usuarios conectados, así como la dirección MAC utilizados por los sistemas operativos de Microsoft.

Entre las herramientas que comúnmente son utilizadas se encuentran: DumpSec, SMB auditing, NetBIOS auditing.

2.3.4. Ingeniería social

La ingeniería social ha sido una amenaza para todo tipo de organizaciones desde mucho tiempo atrás, es una de las formas más comunes para tratar de conseguir información sensitiva de la organización, obtener acceso a un sistema o dificultar su disponibilidad, los objetivos en la ingeniería social son las personas situadas en ciertos roles, como administradores de sistemas que permitan utilizar la información que manejan de una manera maliciosa.

La ingeniería social no se considera un ataque lógico directo, pero sí como parte de un ataque lógico ya que es utilizado en combinación con la tecnología en algunos casos, juega un papel muy importante para los intrusos en la planeación de un ataque. Cuando se convierte en un ataque, éste consiste en aprovechar las habilidades de convencimiento y sacar provecho de la vulnerabilidad que el ser humano tiene, *la confianza*, para obtener información relevante que al intruso le podría servir para llevar a cabo algún otro ataque.

[20] Para mayor detalle ver apéndice B

Algunos métodos incluyen realizar una llamada telefónica para obtener datos personales, envío de correos electrónicos a nombre de otros, copias de correos electrónicos, documentos que desecha una institución, entrevistar a empleados de áreas especificas , contacto cara a cara, métodos técnicos como troyanos, backdoors, suplantación de identidad, phishing, pharming entre otros. La ingeniería social trata de obtener información de las personas como cuentas de usuario y contraseñas, secretos industriales, cuentas bancarias, listas de empleados, proveedores, clientes, información del sistema, información de la infraestructura, horarios de empleados, información de investigaciones, información que permita establecer conexiones remotas, en sí cualquier tipo de información que permita al atacante obtener el beneficio que busca.

El problema es tal que dentro del mundo de la seguridad, el ser humano es considerado el eslabón más débil de un esquema de seguridad, una forma de evitar en mayor medida este tipo de ataques, es a través de la educación de los usuarios, proporcionando información acerca de este tipo de ataques y la seguridad en general.

Para salvaguardar efectivamente una organización de la ingeniería social se combinan tres ángulos de defensa: conciencia, procesos/ procedimientos y gente.[21]

Los empleados debe tener *conciencia* del tipo de información que se considera sensitivo, con la finalidad de tener la discreción que se debe en el manejo ésta, solo después de la clasificación de la información se puede informar a los empleados de aquella que se considera sensitiva en cada departamento.

Los *procesos o procedimientos* que se realizan deben salvaguardarse por los responsables de cada área de acción, con la finalidad de que si se llegara a conocer alguno de estos no se pueda atacar, ya que se requiere el dato sensitivo de otro proceso para concretar un ataque.

La *gente* es el punto más débil, la manera de buscar minimizar los ataques de ingeniería social es a través de la educación.

2.4.Controles de seguridad

Generalmente los controles o mecanismos se refieren a medidas de seguridad que buscan reducir la posibilidad de que se presente un ataque, pueden ser clasificadas de las siguientes tres maneras:

a) **Física**, medidas físicas para prevenir el acceso no autorizado a sistemas incluyendo personal de seguridad, luces, circuitos cerrados, candados, alarmas, mecanismos de monitoreo, medidas de seguridad ambiental, tecnologías avanzadas de autenticación, medidas de seguridad para dispositivos de hardware, este punto también es reforzado con la implementación de políticas de seguridad que determinan el procedimiento que deben seguir los usuarios para garantizar la seguridad.

[21] Mike Horton, Hacknotes network security, McGraw-Hill, 2003, cap 8, pág 142,145.

b) ***Técnica,*** medidas de seguridad técnica como son firewalls, IDS, filtro de contenido, antivirus, actualizaciones de software y sistema operativo, Hardening–endurecimiento de sistemas, medidas de seguridad en software, medidas de seguridad en la comunicación, herramientas de seguridad adicionales que sean implementadas en sistemas remotos, redes y servidores. Muchas de las herramientas empleadas de este tipo son de software y algunas otras de hardware.

c) ***Operacional***, medidas de seguridad operacional, para analizar amenazas y el impacto que se tenga si se presenta un ataque, debe ser un proceso documentado en las políticas de seguridad de la organización, este tipo de herramienta es implementando de manera normativa.

Cualquiera de estas tres clasificaciones puede ser parte de un sistema de seguridad en cómputo, la elección de éstas depende meramente de las necesidades específicas y primordiales de cada organización.

En redes de datos existe una arquitectura de seguridad OSI definida en el ISO (International Standard Organization – Organización internacional para la estandarización) 7498-2, donde se define el servicio de seguridad como la característica que debe tener un sistema, para satisfacer una política de seguridad, a diferencia de un mecanismo de seguridad, ya que éste es un procedimiento concreto utilizado para implementar el servicio de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad (Sólo las entidades autorizadas podrán interpretar la información).
- Autenticación (Verifica la identidad de quien dice ser).
- Integridad (Se hace referencia al concepto integridad).
- Control de acceso (Define el acceso o negación a un recurso).
- No repudio (Se comprueba el origen de los datos).
- Disponibilidad (En todo momento el servicio o recurso estará disponible).

2.5.Análisis de riesgo

La administración de riesgos, es el proceso que permite a los administradores del negocio lograr un balance entre los costos operacionales y económicos, de las medidas de protección del negocio que soporta a la misión de la empresa, es una parte fundamental de la administración de la seguridad.

Entre los beneficios que genera:

- Identifica los puntos más débiles de la infraestructura de TI, que da soporte a los procesos críticos de la organización.
- Guía la selección de medidas de protección de costo adecuado.
- Determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio.

- Permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización.
- Es un elemento para la toma de decisiones estratégicas.

  En general los análisis de riesgos que se pueden llevar a cabo son de dos tipos, cualitativos y cuantitativos, la elección de éste depende de cómo se desea llevar a cabo el análisis.

a) *Cuantitativo*

- Enfocado a determinar valores numéricos (generalmente monetarios) para los componentes objeto del análisis, así como al nivel de posibles pérdidas.
- Los resultados son objetivos, basados en métricas generadas igualmente de forma objetiva, éstos se expresan en porcentajes, probabilidades de ocurrencia de amenazas, pesos, etcétera.
- Es sencillo mostrar el costo-beneficio en términos comprensibles para la alta dirección (no técnicos).
- Los cálculos pueden resultar complejos.
- El trabajo previo requiere tiempo y esfuerzos considerables.

b) *Cualitativo*

- No requiere determinar valores numéricos (generalmente monetarios) para los componentes objeto del análisis, así como al nivel de posibles pérdidas.
- No es necesario contar con la frecuencia de ocurrencia de las amenazas.
- Los resultados son subjetivos.
- No hay una base para demostrar el costo-beneficio.
- Los cálculos son sencillos.
- La calidad del análisis depende del equipo conformado.

Los componentes generales de un análisis de riesgo son:

1. ***Enunciar el alcance del análisis***; establece cuál es el activo informático a ser evaluado, Define cuál será el entregable (reporte, estrategia, mecanismo, etcétera.).

2. ***Conformar el equipo que sustentará el proceso de análisis de riesgos***; dueños de las funcionalidades, usuarios a todos los niveles, diseñadores y analistas de sistemas, desarrolladores de sistemas, administradores de BD, auditores, personal de seguridad física, telecomunicaciones, jurídico, administración de operaciones, sistemas operativos, seguridad información.

3. ***Identificar las amenazas***; es recomendable contar con una lista propuesta antes del análisis (tal vez basada en hechos que ya ocurrieron). Fomentar lluvias de ideas considerando lectura ilegal de información, negación de servicio, explotación de deficiencias en plataformas operativas, vandalismo en páginas web, falsificación de identidad, virus, caballos de Troya, gusanos, ingeniería social, se puede priorizar de acuerdo con integridad, confidencialidad y disponibilidad

4. ***Priorizar las amenazas y riesgos***; tabla para dar prioridades a las amenazas (por consenso), y para estimar el impacto a la organización.

5. ***Determinar la prioridad en función del impacto.***

6. ***Estimar el impacto total de la amenaza conforme al riesgo que representa.***

7. ***Identificar medidas de protección.***

8. ***Realizar un análisis costo/beneficio***; en este análisis se debe determinar cuáles son los controles que dan un máximo de protección a un menor costo (puede haber controles que sirvan para mitigar la ocurrencia de varias amenazas).

9. ***Ordenar las medidas de protección por prioridades***; debe ordenarse la selección para elegir el control adecuado.

    a) Cuántas amenazas puede mitigar un control.
    b) El impacto en la productividad al implantar un control.
    c) Controles que pueden desarrollarse en casa.
    d) Estimar un nivel de aceptación de riesgo.

10. ***Reportar el resultado del análisis***; el producto del análisis es un reporte donde se documentan los hallazgos, identificación de los controles, recomendación de controles puede en ocasiones llegar hasta esbozar un plan de implantación de los controles sugeridos, permite crear un histórico que permitirá apoyar las decisiones en análisis futuros.

11. ***Proponer soluciones estratégicas***[22]

Lo más complicado al momento de hacer un análisis de riesgo es determinar el valor de los activos, para esto se pueden utilizar varios métodos como lo son orden superior, política general, legislación, entrevistas con listas de verificación, cuestionarios, consenso (Delphi), valor en libros.

[22] Risk Management Guide for Information technology System, NIST SP800-30

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]

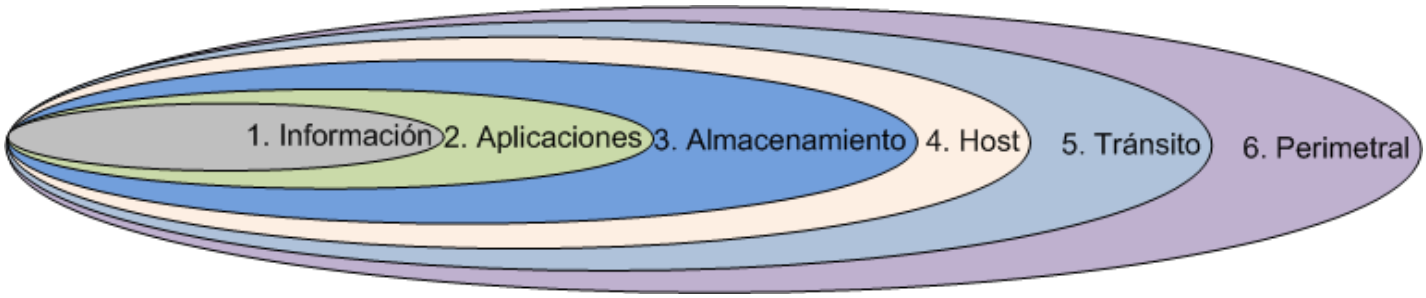


Figura 3. 1 Modelo de seguridad.

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.

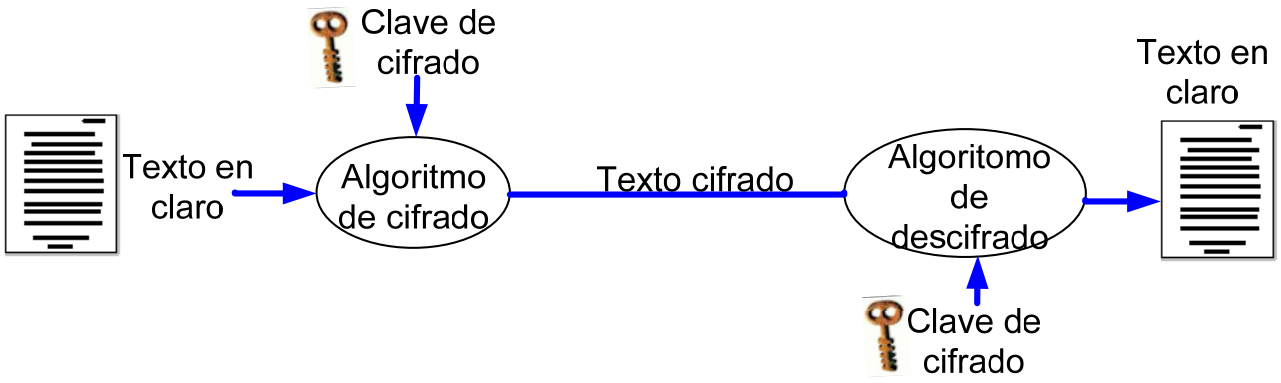


Figura 3. 2 Modelo simplificado de cifrado simétrico.

[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.

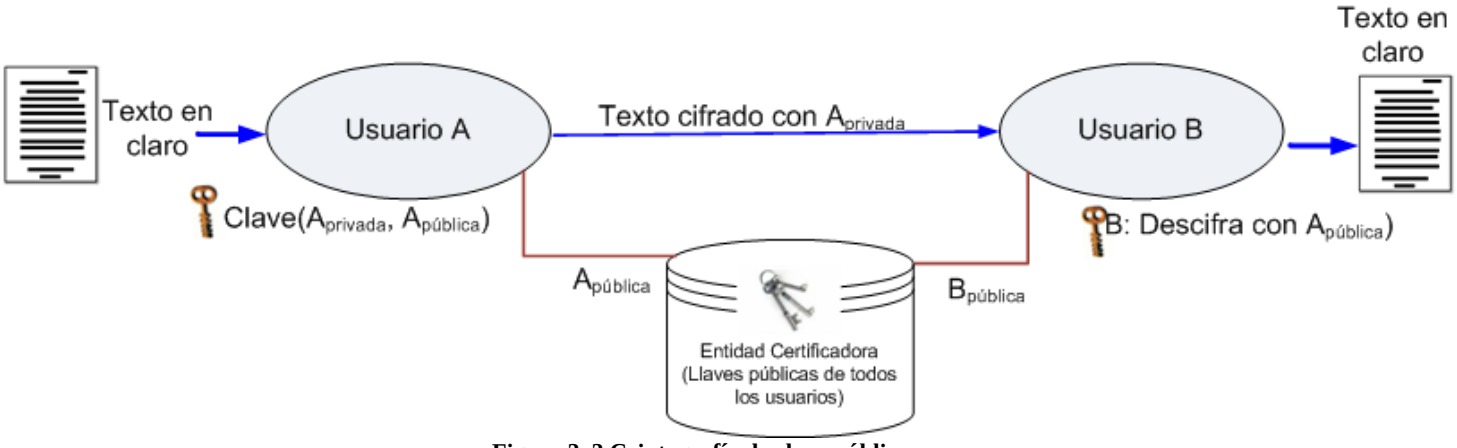


Figura 3. 3 Criptografía de clave pública.

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).

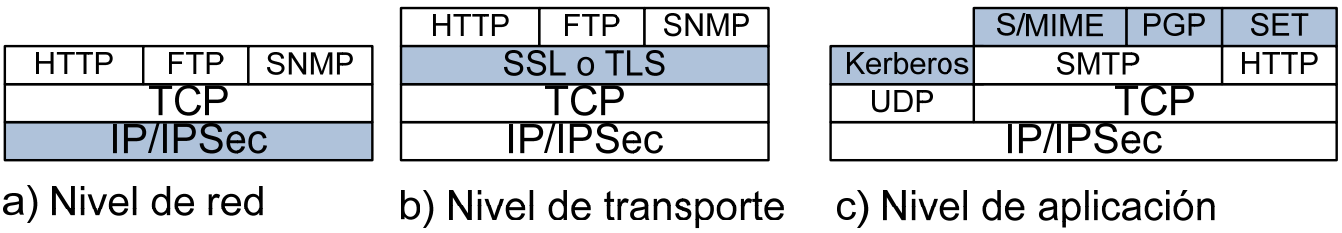


Figura 3. 4 Ubicación relativa de las herramientas de seguridad en la pila de protocolos TCP/IP.

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.

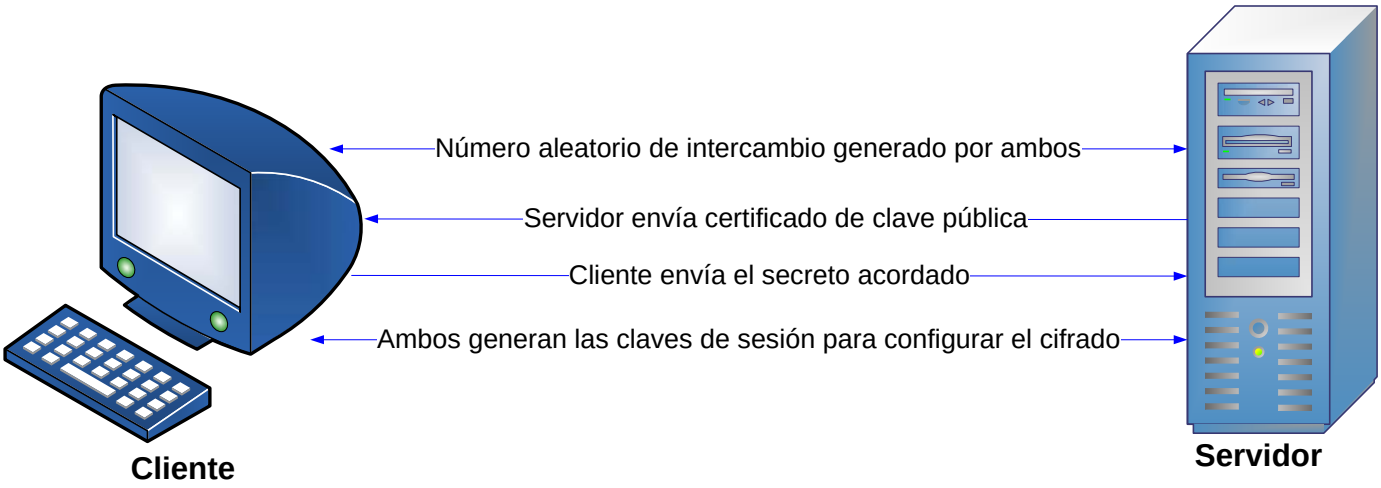


Figura 3. 6 Handshake de SSL.

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).

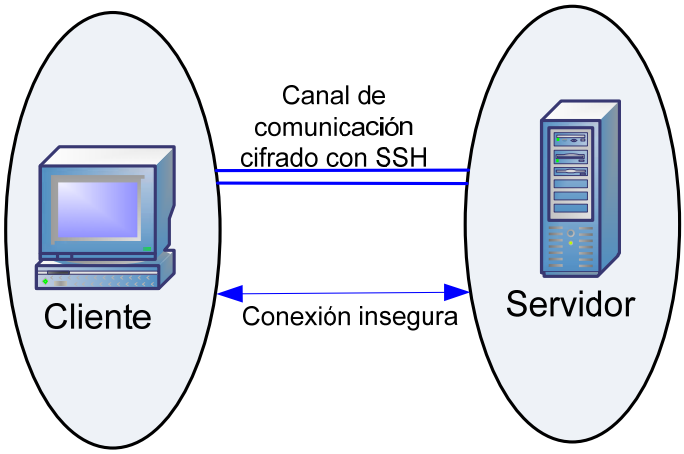


Figura 3. 7 SSH.

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).

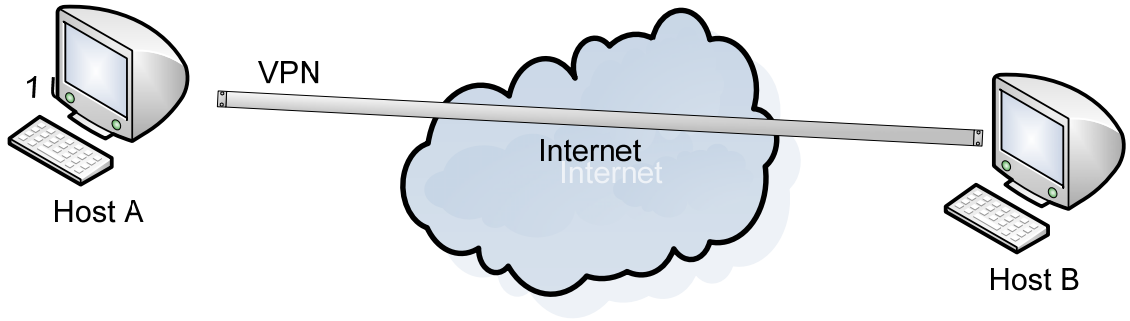


Figura 3. 8 VPN Host to Host

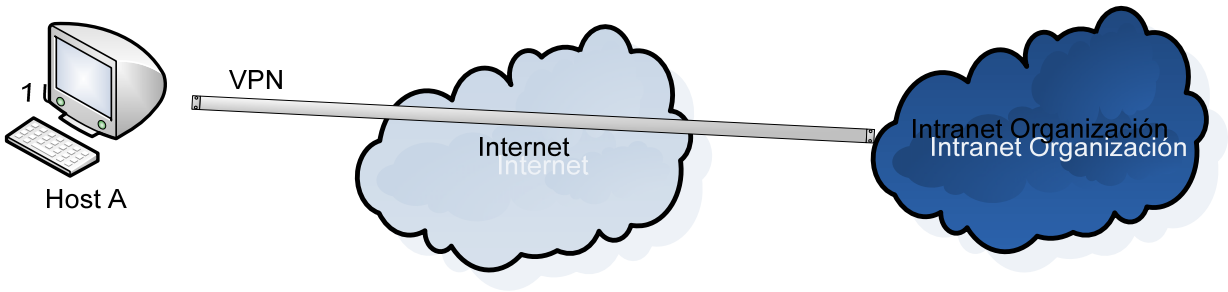


Figura 3. 9 VPN Host to Network

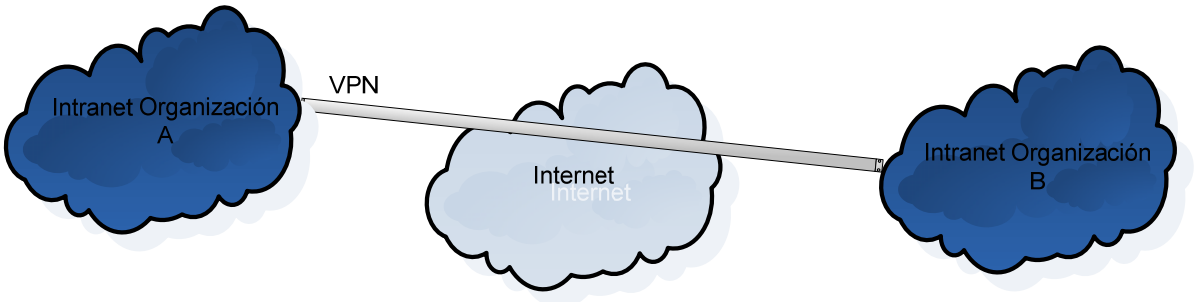


Figura 3. 10 VPN Network to Network.

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.

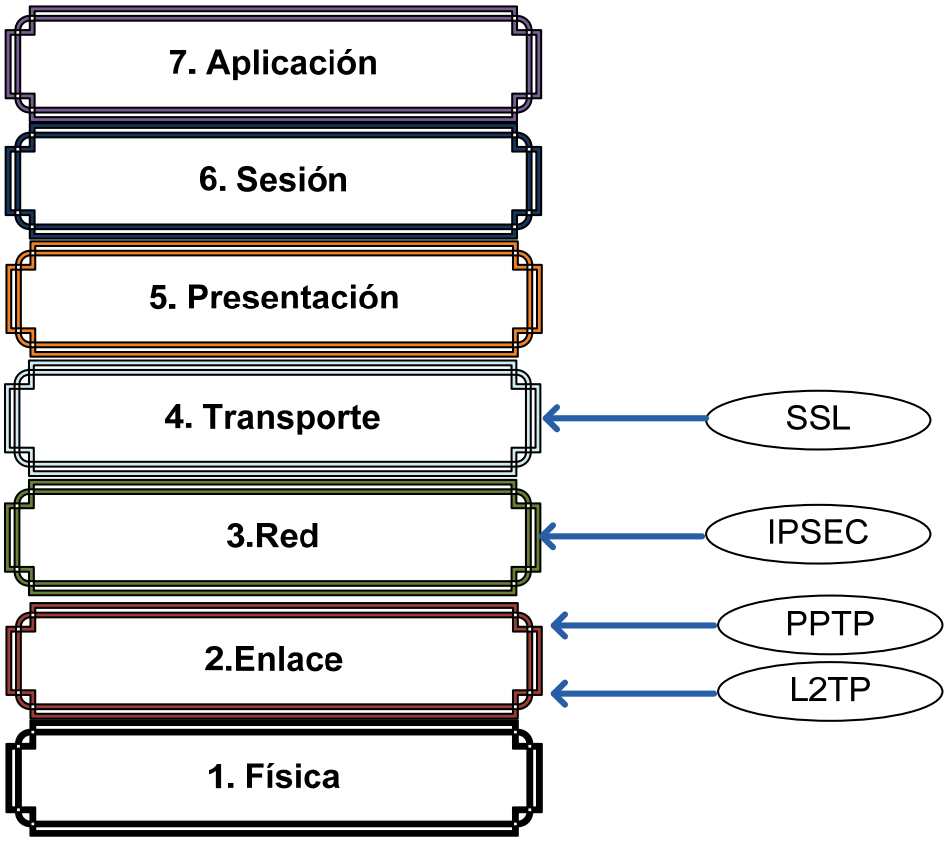


Figura 3. 11 Protocolos VPN en el modelo OSI.

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.

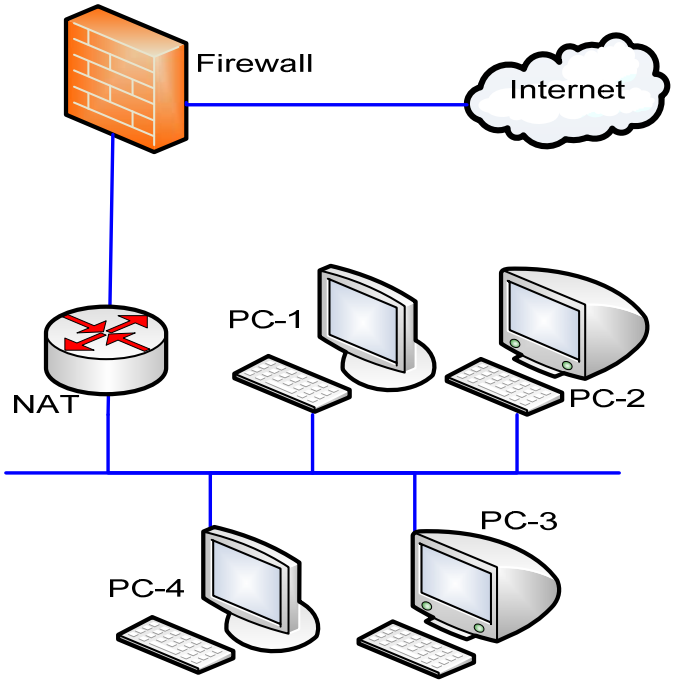


Figura 3. 12 Diagrama de funcionamiento de un NAT.

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).

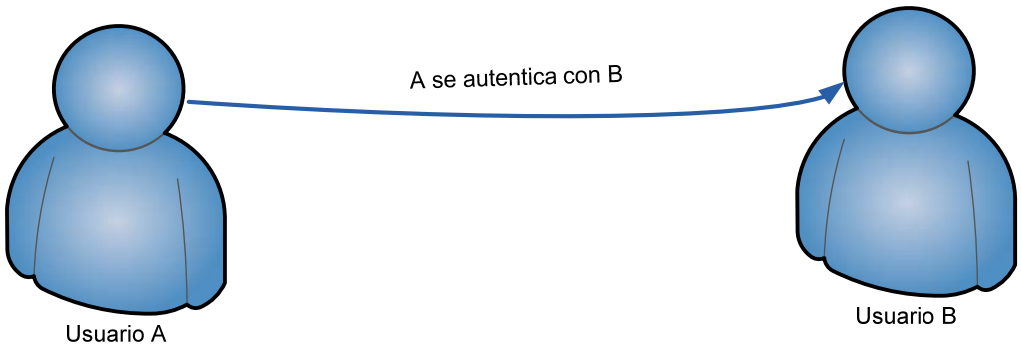


Figura 3. 14 Autenticación Unilateral.

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).

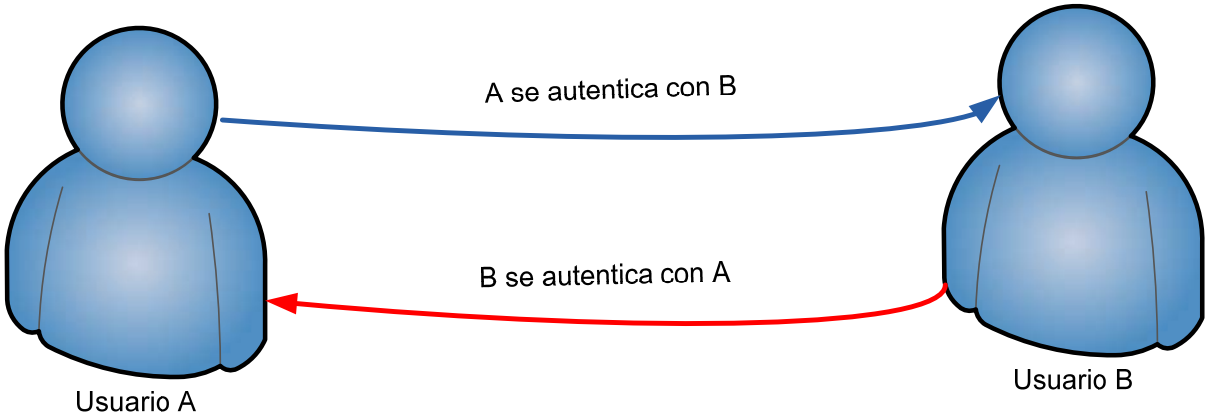


Figura 3. 15 Autenticación mutua.

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).

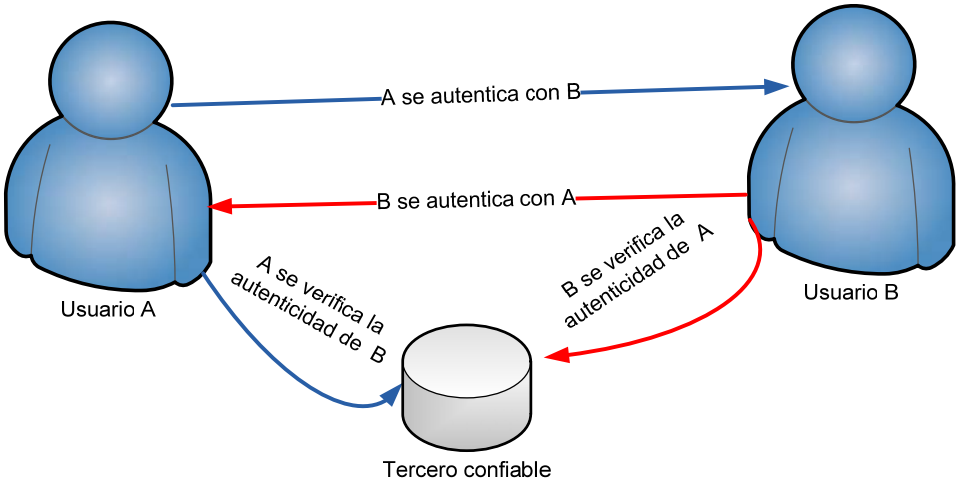


Figura 3. 16 Autenticación por medio de un tercero confiable.

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.

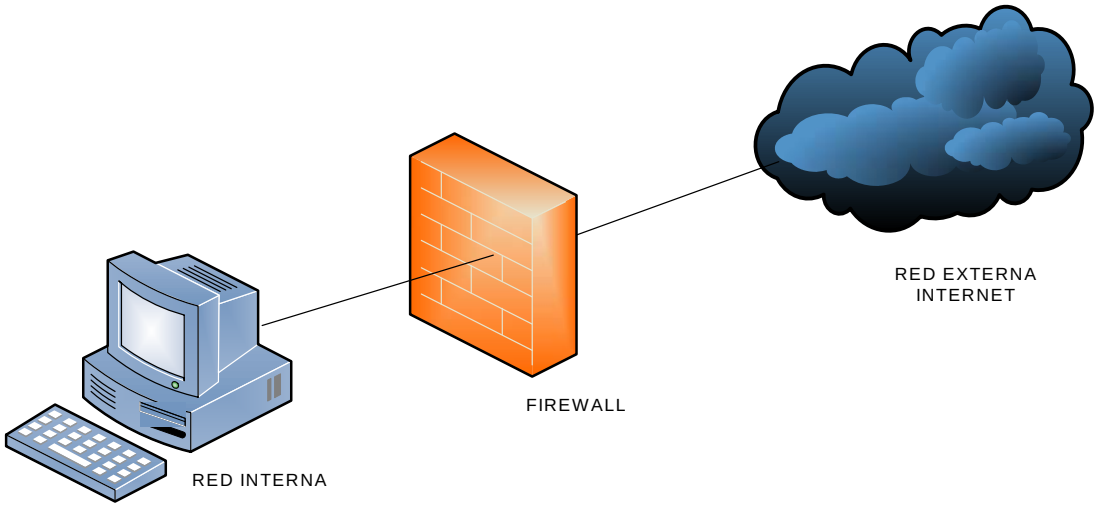


Figura 3. 17 Firewall.

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.

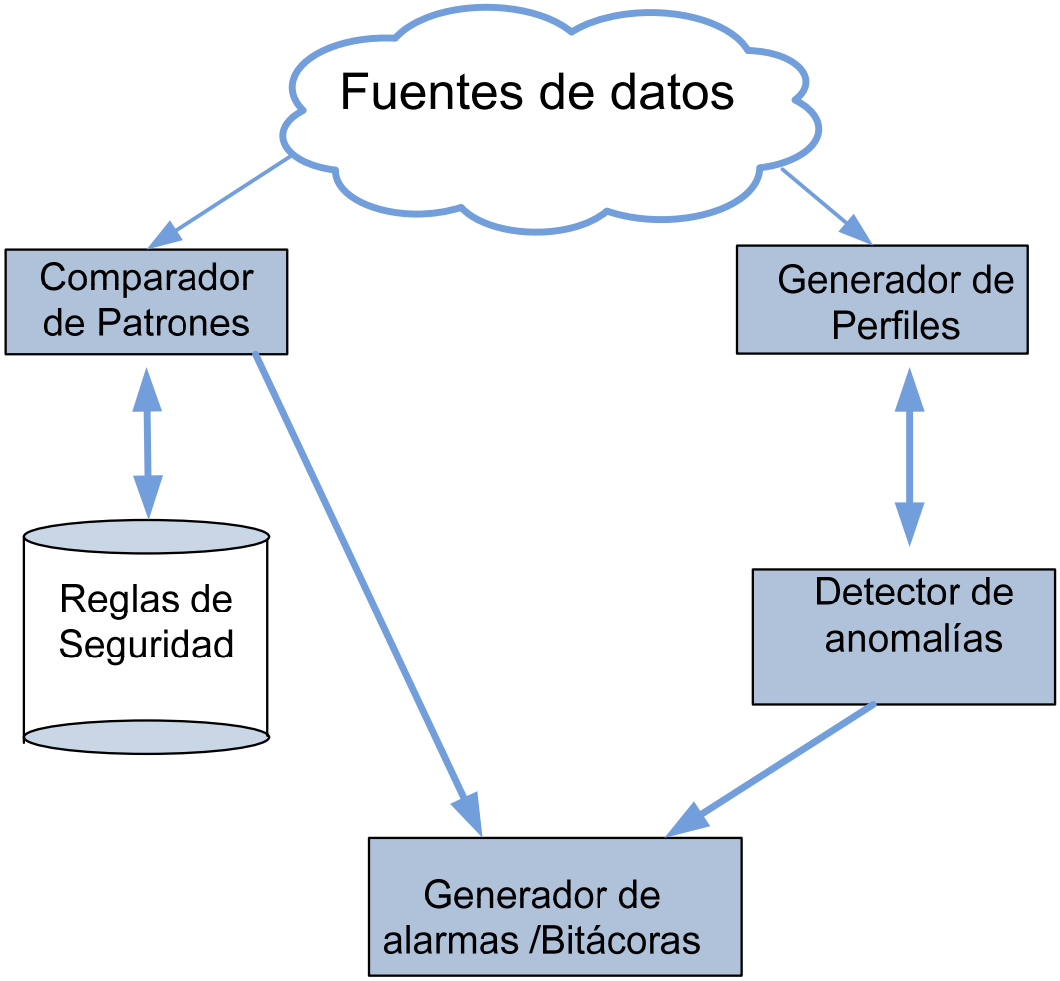


Figura 3. 18 Esquema general de un Sistema Detector de Intrusos.

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).

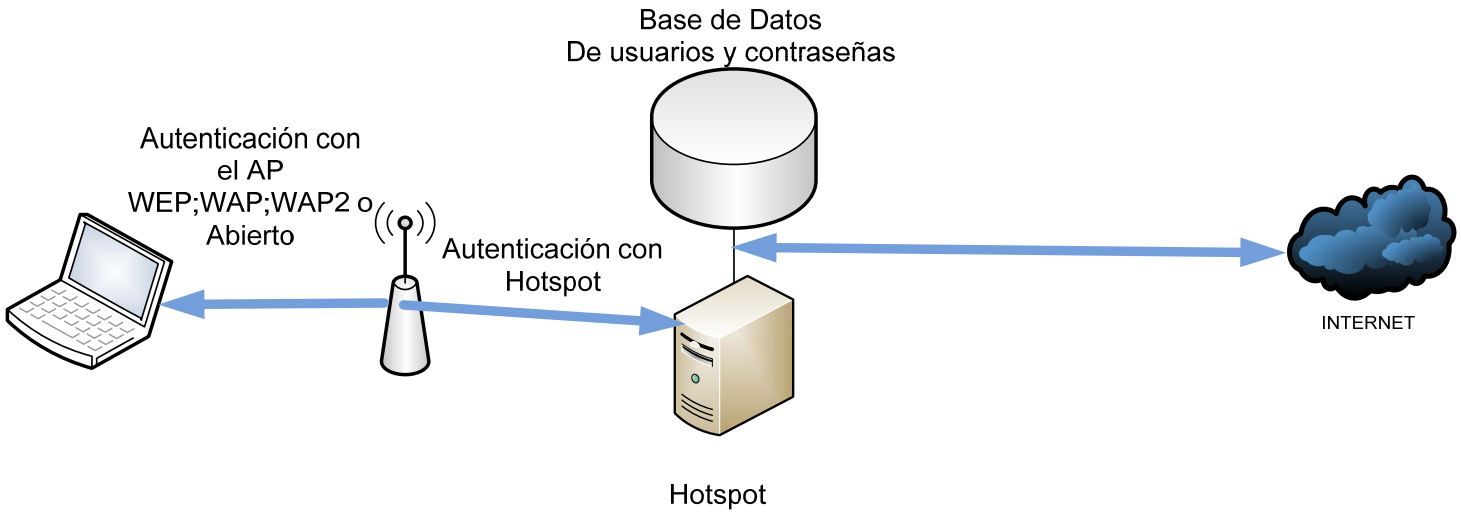


Figura 3. 19 Hotspot.

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.

CAPÍTULO 4
Buenas Prácticas de Seguridad

“El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en un caja fuerte de titanio, encerrado en un bunker de concreto, rodeado por gas venenoso y cuidado por guardias muy bien armados y pagados. Aun así, no apostaría mi vida por él”. [Eugene Spafford].

4.1. Justificar por qué invertir en seguridad

Tal vez uno de los puntos más importantes al momento de tratar de implementar una solución de seguridad es demostrar la necesidad de invertir en este rubro, debido a que es complicado cuantificar el daño que representa la afectación de un principio de seguridad en un bien, algunos de los mecanismos para esto son los siguientes:

- Retorno de inversión, se logra demostrar en términos financieros que la inversión en seguridad será rentable para la compañía y que sus beneficios van más allá del ámbito de seguridad.

- Desarrollar una demostración presencial de qué tan sencillo resulta comprometer un sistema con la finalidad de mostrar la gravedad del problema.

- Regulaciones, las compañías invierten en seguridad para cumplir con alguna regulación a la cual están sujetas, dependiendo el tamaño de éstas.

- Clasificar la escala de gravedad de un incidente, para catalogar los hechos de seguridad en función del impacto sobre el sistema de información, se trata en algunos casos de medir una pérdida económica, y en otros, comparecer ante un tribunal. Por tal motivo es fundamental comprender que esta medición de la gravedad de un incidente debe realizarse tras una gestión de los riesgos (tabla 4.1).

Tabla 4. 1 Escala de gravedad de un incidente.

Categoría	Nivel	Gravedad	Criterio
Parada	5	Inaceptable	El hecho cuestiona la supervivencia de la empresa.
	4	Muy importante	El hecho presenta un riesgo muy importante y necesita medidas de urgencia inmediatas.
Degradación	3	Importante	El hecho no ocasiona riesgo importante alguno, pero se toca una parte significativa del sistema.
	2	Media	El hecho tiene una consecuencia sobre el funcionamiento normal y debe generar una reacción inmediata.
Perturbación	1	Leve	El hecho no tiene consecuencias notables pero debe tratarse para restablecer el funcionamiento normal
Funcionamiento normal	0	Ninguna importancia desde el punto de vista de la seguridad	Funcionamiento normal

- Apegarse a estándares internacionales con la finalidad de brindarle prestigio a la institución, requieren de mayores recursos económicos.
- Demostrar que lo que se ha gastado en seguridad es lo correcto con respecto, al valor de la información a proteger.
- Demostrar el impacto que se produce si se compromete cierta información, o se deja de brindar un servicio por algún tiempo.

4.2. Buenas prácticas en la administración de la seguridad con base en estándares

Los estándares internacionales son una muy buena guía que proporcionan un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. [37]

Entre los puntos importantes a considerar con relación a los estándares internacionales, enfocándose en el ISO 27001 se encuentran:

1. Adoptan algún modelo para aplicarse a los procesos de SGSI, como lo es el modelo Planear-Hacer-Checar-Actuar (PDCA – Plan-Do-Check-Act), Figura 4.1. La adaptación del modelo PDCA también refleja los principios tal como se establecen en los lineamientos OECD (2002).[38]

    a) ***Planear (establecer el SGSI):*** Establecer políticas, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

    b) ***Hacer (implementar y operar el SGSI):*** Implementar y operar la política, controles, procesos y procedimientos SGSI.

    c) ***Checar (Monitorear y revisar el SGSI):*** Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.

    d) ***Actuar (mantener y mejorar el SGSI):*** Tomar acciones correctivas y preventivas, basados en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante para lograr el mejoramiento continuo SGSI.

[37] Estándar Internacional ISO/IEC 27001, Primera edición, Referencia ISO/IEC 27001:2005

[38] Guias de la OCDE para la seguridad de los sistemas de información y redes, http://www.anacom.pt/streaming/1946922.pdf?categoryId=45842&contentId=132698&field=ATTACHED_FILE

Figura 4. 1 modelo PDCA.

2. Un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de varios estándares.

La organización por su parte debe hacer lo siguiente:

1. Permiten definir el alcance y los limites de SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología, incluyendo los detalles de la justificación de cualquier exclusión del alcance.

2. La creación de una política de SGSI en términos de las características del negocio, la organización, activos y tecnología.

3. Permite definir las líneas a seguir para realizar el análisis de riesgo, que contempla:
    b) Identificar los activos dentro del alcance del SGSI y los propietarios de estos activos.
    c) Identificar las amenazas para aquellos activos.
    d) Identificar las vulnerabilidades que podrán ser aprovechadas por las amenazas.
    e) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.
    f) Calcular la probabilidad realista de que ocurra dicha falla.
    g) Determinar si el riesgo es aceptable o requiere tratamiento.
    h) Identificar y evaluar las opciones para el tratamiento de los riesgos, las acciones posibles incluyen:

        - Aplicar los controles apropiados.
        - Aceptar los riesgos conscientes y objetivamente siempre que se satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización.
        - Transferir los riesgos comerciales asociados a otras entidades, por ejemplo: aseguradores, proveedores.

4. Seleccionar objetivos de control y controles para el tratamiento de riesgo, esta selección debe tomar en cuenta el criterio para aceptar los riesgos, así como los requerimientos legales, reguladores y contractuales.

5. Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

6. Obtener la autorización de la gerencia para implementar y operar el SGSI.

7. Implementar los procedimientos y otros controles capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

8. Implementar los programas de capacitación y conocimiento.

9. Ejecutar procedimientos de monitoreo y revisión y otros controles para :

    a) Identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos
    b) Permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante alguna tecnología se están realizado como se esperaba.
    c) Realizar revisiones regulares de la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
    d) Actualizar los planes de seguridad para tomar en cuenta las actividades de monitoreo y revisión.
    e) Registrar las acciones o eventos que podrían tener un impacto sobre la efectividad.

10. Realizar auditorías internas a intervalos planeados, contemplando:

    a) Que se cumplan los requerimientos del estándar.
    b) Cumple con los requerimientos de seguridad.
    c) Se implementa y mantiene de manera efectiva.
    d) La selección de los auditores y la realización de las auditorías debe asegurar la objetividad e imparcialidad del proceso de auditoría.
    e) Los auditores no pueden auditar su propio trabajo.
    f) Las responsabilidades y requerimientos para la planeación y realización de las auditorías y para el reporte de los resultados y mantenimiento de registros se debe definir en un proceso documentado.
    g) La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no conformidades detectadas.

11. Actualizar los planes de seguridad para tomar en cuenta las actividades de monitoreo y revisión.

12. Implementar las mejoras identificadas en el SGSI.

13. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones.

14. Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle de acuerdo con las circunstancias.

15. Asegurar que las mejoras logren su objetivo señalado.

La documentación del SGSI debe incluir lo siguiente:

1. Enunciados documentados de la política y los objetivos.
2. El alcance del SGSI.
3. Procedimientos y controles del SGSI.
4. Una descripción de la metodología de evaluación de riesgos.
5. Reporte de la evaluación de riesgos.
6. Plan de tratamiento del riesgo.
7. Los procedimientos necesarios por la organización se establecen, documentan, implementan y mantienen para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles.
8. Revisar y actualizar los documentos conforme sea necesario y re aprobar los documentos.
9. Asegurar que se identifiquen los cambios y el estado de la revisión actual de los documentos.
10. Los documentos pueden estar en cualquier forma o medio.
11. Se debe establecer un proceso documentado para definir las acciones gerenciales para:
    a) Aprobar la idoneidad de los documentos antes de su emisión.
    b) Revisar y actualizar los documentos conforme sea necesario.
    c) Asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso.
    d) Asegurar que los documentos se mantengan legibles y fácilmente identificables.
    e) Asegurar que se controle la distribución de los documentos.
    f) Evitar el uso indebido de documentos obsoletos.

12. Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva, deben protegerse y controlarse.

13. Se debe mantener registro del desempeño de los procesos y de todas las ocurrencias de incidentes de seguridad significativos.

14. La gerencia debe establecer compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora.

a) Establecer una política SGSI.
b) Asegurar que se establezcan objetivos y planes SGSI.
c) Establecer roles y responsabilidades para la seguridad de la información.
d) Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de una mejora continua.

15. Propiciar la capacitación o realizar otras acciones (por ejemplo emplear al personal competente) para satisfacer estas necesidades.

De manera resumida éstos son algunos puntos principales en los cuales se puede apoyar para definir un esquema de seguridad de la información, ya que permite llevar el proceso de forma ordenada y efectiva.

4.3. Buenas prácticas de seguridad en redes

En la actualidad la aplicación de buenas prácticas en los esquemas de seguridad de las organizaciones, permite responder de una mejor manera frete a los incidentes, ya que se contemplan las mejores experiencias para cada caso. En el presente tema se pretende destacar la importancia de las buenas prácticas de seguridad en redes, a continuación se muestra una lista de las cuestiones que se deben tomar en cuenta para garantizar un nivel de seguridad adecuado en las redes de datos:

- Contar con políticas de seguridad basados en modelos como COBIT y estándares como ISO 27001.
- Realizar planes de contingencia en caso de incidentes BRP (Business Recovery Plan- Plan de recuperación del negocio), BCP (Business Continuity Plan – Plan de continuidad del negocio).
- Dar a conocer la importancia de la seguridad a todos los que trabajan en la institución o empresa a través de carteles, cursos, campañas u otros medios.
- Ejecutar frecuentes auto-evaluaciones de seguridad de la información.
- Consultar guías de configuración de sitios como NSA, NIST, SANS, ISO, security focus, insecure, entre otros.
- Contar con un equipo de personas dirigidos a la administración y seguridad de la organización.
- Manejar Canales seguros de comunicación.
- Cifrar comunicaciones y datos durante el transporte y almacenamiento.
- Hacer un uso adecuado de contraseñas.
- Realizar respaldos de información.

- Establecer planes de contingencia ante un incidente de seguridad.
- Contar con un inventario detallado de los equipos que integran la red incluyendo localización geográfica.
- Identificar los servicios que se ofrecen y eliminar aquellos que no son necesarios.
- Establecer esquemas de seguridad en profundidad.
- Proteger las redes a través de diferentes mecanismos.
- Delimitar tanto el acceso lógico como físico a los sistemas.
- Utilizar firewalls, sistemas detectores de intrusos, antivirus.
- Controlar y regular las cuentas de usuarios tanto de administradores como otros usuarios.
- Evitar utilizar la misma contraseña para todos los dispositivos o sistemas.
- Evaluar los impactos que se tendrían si se pierde algún activo.
- Asegurar física y lógicamente los equipos que integran la red.
- Evitar utilizar servicios como Telnet o donde la información viaje en claro.
- Instalar monitores de red que permitan analizar el comportamiento de la red.
- Auditar firewalls, sistemas y cualquier dispositivo que se considere necesario.
- Implementar controles de autenticación robusta para administradores o para el acceso a una intranet, se recomienda emplear mínimo dos controles.
- Minimizar el número de cuentas de usuarios que operen sistemas críticos.
- Utilizar contraseñas robustas para administradores y usuarios.
- Llevar un control de la asignación de direcciones IP.
- Contar con mapas de red.
- Establecer responsables por área.
- Identificar equipos críticos.
- Deberán implementarse políticas de uso de la red.
- Realizar pruebas de estrés a la red.
- Realizar pruebas de penetración.
- Realizar continuamente auditorías.

En el listado anterior se da un panorama general de las buenas prácticas que se deben seguir, sin embargo, será necesario tomar en cuenta otras recomendaciones que se crean necesarias con base en los objetivos y prioridades de cada organización.

4.4. Respaldo de información

Dentro de las políticas de seguridad o como parte de un plan de seguridad se debe contemplar y recalcar la importancia de realizar respaldos de la información, la razón es simple y sencilla, cualquier sistema puede incurrir en un fallo y con ello pérdida o daño de la información, lo que puede representar una pérdida económica, en tiempo o continuidad de operaciones.

Toda información por mínima que ésta sea, deberá respaldarse y clasificarse de acuerdo con la sensibilidad de la misma, a continuación se muestra un listado del tipo de información que debería considerarse para respaldar.

- En caso de maquinas virtuales, una copia idéntica de los archivos que la conforman
- Bases de datos.
  - Estructura e información.
- Documentos.
  - Texto.
  - Audio.
  - Video.
  - Archivos de configuración.
  - Bitácoras.
  - Políticas de seguridad.
  - Inventarios de equipos.
- Cuentas de usuarios.
  - Archivos.
- Cualquier otro tipo de información que se considere importante.
  - Guías de configuración.
  - Facturas.
  - Informes de trabajo.
  - Proyectos, por mencionar solo algunos.

Los respaldos deberán estar almacenados en distintos medios como cintas magnéticas, equipos alternos, dispositivos de almacenamientos masivos, además de que éstos deberán estar seguros de manera física y en caso extremo, cifrados.

El acceso a dicha información deberá estar restringido y sólo personal autorizado tendrá los privilegios para realizar dichos respaldos para evitar fuga de información, pérdida, o alteración de la misma.

Otros puntos importantes que se deberán considerar para un respaldo adecuado de la información son:

- Evitar contar con respaldos excesivos ya que esto puede complicar la administración de los mismos por lo que se deberán establecer fechas y tiempos de respaldo, esto dependerá de la importancia de la información.

- Los respaldos de la información no sólo son responsabilidad del administrador de un equipo, los usuarios deberán de contemplar que son responsables de su propia información y con ello implica que son responsables de lo que pueda acontecer con la misma. Esto deberá estar detallado en las políticas de seguridad.

- También deberán contar con una bitácora donde se contemple fecha, tamaño del archivo que se haya respaldado, responsable e incluso tipo de archivo y versión del software utilizado, en algunos casos requerirá mayor detalle.

4.5. Seguridad en aplicaciones

En la actualidad el desarrollo de aplicaciones seguras ha cobrado mayor importancia, esto debido a que los programas constituyen la mayor parte de los sistemas de cómputo como lo son los sistemas operativos, drivers, programas de infraestructura de red, administradores de bases de datos entre otras aplicaciones, debido a que los programas integran un gran porcentaje de los sistemas de cómputo, es importante tener especial cuidado con el manejo de ellos tanto en la implementación, como en el desarrollo de los mismos.

En el desarrollo de sistemas generalmente implica la integración de distintas tecnologías por lo que será necesario realizar un análisis profundo de las tecnologías a utilizar para determinar su factibilidad, éste debe incluir un análisis de seguridad, costo y beneficios que implica el uso de una u otra tecnología. La seguridad en aplicaciones deberá cubrir los aspectos tratados durante el desarrollo del presente trabajo: disponibilidad, confidencialidad e integridad.

Entre los puntos más importantes a considerar durante la implementación de aplicaciones se encuentran:

- Distribución libre o comercial.
- Tipo de tecnología utilizada.
- Compatibilidad.
- Soporte.

Durante el desarrollo de algún sistema se deberán tomar en cuenta los diferentes tipos de ataques en los que se podría verse implicado el software desarrollado, como por ejemplo el ataque buffer overflow y todas sus variantes que han sido muy aprovechadas por los intrusos atentando contra la disponibilidad, SQL injection, Cross-Site Scripting(XXS).

Algunos puntos importantes a considerar durante el desarrollo de software se encuentran:

- Basar los códigos de programación en estándares sobre todo si se maneja algún lenguaje de programación como C o C++.
- Verificar código haciendo uso de herramientas de auditoría.
- Evitar utilizar rutinas de C que impliquen el uso de rutinas que interactúen con la memoria.
- Utilizar herramientas de compilación que permitan detectar posibles vulnerabilidades.
- Tomar en cuenta la seguridad durante el desarrollo de aplicaciones.
- Tomar en cuenta estándares como ISO 2700x así como publicaciones de NIST 800-64 y 800-27.
- Establecer un modelo de desarrollo de código seguro.
- Utilizar herramientas que permitan detectar defectos de seguridad.
- Contar con un modelo de amenazas.
- Contar con una lista de verificación de implementación.
- Realizar pruebas de penetración.

En la tabla 4.2 se muestra una lista de herramientas útiles para el análisis de vulnerabilidades[39].

Tabla 4. 2 Herramientas de análisis de vulnerabilidades.

Nombre	Lenguaje
FXCop	.NET
SPLINT	C
Flawfinder	C/C++
ITS4	C/C++
Bugscan	C/C++ binaries
CodeAssure	C/C++, Java
Prexis	C/C++, Java
RATS	C/C++, Python, Perl, PHP

Otras herramientas para el análisis de vulnerabilidades

- NESUS
- NIKTO
- WebInspect
- GFILANguard

4.6. Seguridad en sistemas operativos

Entre las buenas prácticas de seguridad se recomienda asegurar los distintos sistemas operativos, así como los distintos elementos que lo integran, programas y servicios. Deberán existir políticas de configuración de los distintos equipos que integran una red, esto con la finalidad de disminuir el riesgo.

[39] Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001

A continuación se describen algunas características que deberán tomarse en cuenta para los sistemas operativos Linux, Windows y aunque no se consideren otros sistemas, de igual forma deberán tomarse en cuenta, desde luego esto dependerá de la infraestructura con la que cuente cada institución.

4.6.1. Hardening en plataformas Microsoft

Hardening es el proceso que se realiza para aumentar el grado de confianza de un sistema, acción compuesta por un conjunto de actividades para reforzar al máximo la seguridad. Al referirnos a Hardening en plataformas Microsoft se dan recomendaciones para aumentar el nivel de confianza de los sistemas operativos fabricados por Microsoft, tanto en sus versiones de estación de trabajo como de servidor.

El sistema operativo Windows es uno de los sistemas operativos más utilizados a nivel mundial, lo que implica un especial cuidado en el manejo del mismo, pues el hecho de que éste sea uno de los sistemas más populares también implica que éste sea un objetivo común de los atacantes.

A continuación se muestran algunas prácticas para asegurar la familia de los sistemas operativos Windows.

- La instalación deberá realizarse utilizando el sistema de archivos NTFS.
- Ubicar los equipos en algún lugar seguro físicamente.
- Colocar contraseña al BIOS.
- Las instalaciones eléctricas deberán ser las adecuadas, así como las condiciones físicas.
- Mantener un control adecuado de usuarios.
- Establecer contraseñas robustas para el administrador y usuarios limitados.
- Deshabilitar cuentas innecesarias como "invitado" y aquellas que no se utilicen.
- Renombrar la contraseña de administrador y no dejar la que el sistema operativo crea. por default, así como asignarle una contraseña robusta.
- Forzar a los usuarios para que cambien su contraseña periódicamente.
- Instalar antivirus y mantenerlo actualizado.
- Mantener actualizado el sistema operativo.
- Mantener activado el firewall local.
- Contar con la última actualización para cada sistema operativo.
- Evitar instalar programas innecesarios.
- Deshabilitar, en caso de que esté habilitado, el servicio de escritorio remoto.
- Algunos servicios deberán de activarse sólo cuando se requieran.
- Evitar instalar todos los servicios en un mismo equipo.
- Deshabilitar la reproducción automática de dispositivos como USB, disco o cualquier dispositivo extraíble.
- Establecer políticas locales o de grupo del sistema de acuerdo con las necesidades o actividades que desempeñan los usuarios.

- Restringir el uso de ciertos programas.
- Si el equipo se administra de manera remota, deberá realizarse a través de un canal seguro de comunicación.
- Analizar bitácoras del sistema operativo a través del visor de eventos de Windows u otras herramientas.
- Utilizar herramientas para el análisis de vulnerabilidades y actualizaciones de Microsoft como Microsoft Baseline Security Analyzer (MBSA).
- Utilizar herramientas para escanear puertos y ver qué servicios están haciendo uso de ellos.
- Utilizar herramientas que permitan escanear puertos para determinar las aplicaciones o servicios que los están utilizando.
- Deshabilitar NetBios, así como SMB si no es necesario que éste se encuentren habilitados.
- Activar el protector de pantallas después de cierto tiempo de inactividad.
- No permitir la enumeración de cuentas y recursos compartidos.
- Cifrar carpetas o archivos utilizando herramientas externas o las que ofrece el propio sistema operativo.

4.6.2. Hardening en Unix y Linux.

Los ataques no sólo van dirigidos hacia el sistema operativo Windows, en realidad no importa el tipo de sistema operativo, cualquiera que éste sea, es vulnerable, algunos con mayor frecuencia que otros pero todos están en riesgo, por ello sin importar el nombre del sistema o versión deberá de asegurarse.

El sistema operativo Linux que deriva directamente del sistema operativo UNIX ha ganado aceptación por los usuarios, además de que ha tenido un crecimiento muy rápido por toda la comunidad de desarrolladores que se encuentran detrás de éste.

Como se mencionó aunque es un sistema operativo menos utilizado, no está exento de incurrir en algún problema de seguridad, a continuación se describen algunos aspectos que se deben considerar para asegurar un sistema con ambiente Linux:

- Sin importar la distribución, ésta deberá personalizarse de acuerdo con las necesidades.
- Prevenir el cambio de configuración del BIOS.
- Analizar la posibilidad de no instalar el modo gráfico.
- Planear la instalación para asignar y crear las particiones necesarias.
- Determinar los servicios que se ofrecerán.
- Evitar instalar servicios innecesarios.
- Crear sólo las cuentas de usuario necesarias.
- Monitorear constantemente las cuentas de usuarios.
- Limitar el número de procesos que un usuario puede ejecutar.

- Verificar que los usuarios utilicen contraseñas robustas.
- Verificar integridad de archivos importantes como /etc/passwd y /etc/shadow y los binarios.
- Configurar los archivos de etc/group.
- Configurar el archivo que inicia servicios al arrancar el sistema etc/intetd.conf.
- Utilizar software que permita determinar vulnerabilidades.
- Mantener actualizado los programas que se instalen.
- Analizar constantemente bitácoras de los servicios instalados.
- Establecer cuotas a los usuarios.
- Cifrar archivos.
- Verificar integridad de archivos.
- Establecer permisos, lectura, ejecución, escritura y borrado.
- Si no es necesario ejecutar el modo gráfico, editar los niveles de ejecución.
- Asegurar cada uno de los servicios instalados como ssh, bases de datos, web, correo etcétera.
- Utilizar software que permita realizar auditorías para determinar fallas en la configuración.
- Escanear periódicamente los puertos abiertos TCP y UDP.
- Realizar pruebas de penetración.

4.7. Buenas prácticas de seguridad en servidores

En las infraestructuras de redes, los servidores juegan un papel muy importante, esto debido a que la información que manejan la mayoría de las veces es sensible, las recomendaciones que se hacen recaen en los siguientes puntos:

- Tratar de utilizar versiones de software lo más estable posible.
- Deshabilitar el booteo a partir de otros dispositivos diferentes al disco duro, como CD-ROM, USB, red, floppy, etcétera.
- Tener todo el sistema operativo dentro de una aplicación de cifrado.
- Saber reconocer los procesos que están corriendo en el equipo.
- Eliminar componentes de software extraños.
- Implementar un adecuado control de usuarios y privilegios.
- Forzar al uso de contraseñas robustas cuando se utilicen como métodos de autenticación.
- Habilitar la auditoría en el servidor.
- Verificar la aplicación de los parches de seguridad.
- Realizar auditorías de[40]:
    - Intentos de obtener acceso a través de cuentas existentes
    - Acceso y permiso a los archivos y directorios.
    - Cambios no autorizados a usuarios, grupos y servicios.
    - Sistemas más vulnerables a ataques.
    - Tráfico de red sospechoso o no autorizado.

[40] Chris Brenton,Top 5 Essential Log Reports version 1, SANS, http://www.sans.org/security-resources/top5_logreports.pdf

- Identificar los puertos válidos con base en los servicios que debe ofrecer cada equipo.
- Utilizar software de reconocimiento de rootkits.
- Renombrar las cuentas de administrador o root, según sea el caso.
- No tener habilitados en usuarios remotos root o administrador, utilizar un usuario sin privilegios para el logueo y elevar privilegios de ser necesario.
- Cambiar las contraseñas de root o administrador cada cierto tiempo, recomendación con cambio cada tres meses como mínimo y un registro de cada acceso de esta cuenta al servidor.
- Deshabilitar cuentas de usuarios invitados.
- Eliminar cuentas de usuario sin uso.
- En servidores Windows, uso de alguna herramienta que le permita utilizar un segundo factor, como método de autenticación, el cual debe ser introducido en el sistema cada vez que se desee iniciar sesión.
- Uso de particiones NTFS en el caso de servidores Windows por sus beneficios de cuotas, compresión y cifrado.

Es un hecho que no todos los puntos pueden ser cubiertos, aunque sería lo más recomendable, pero con base en las necesidades de cada caso particular, tener los elementos para dar la solución adecuada es una buena práctica.

4.8. Seguridad en dispositivos removibles y verificaciones regulares al sistema

Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB (memorias, cámaras digitales, cámaras de video, teléfono celular, etcétera), constituyen otro de los mayores focos de infección y propagación de malware, el extravío de estos dispositivos permite filtrado de información, así como medio para la extracción de información debido al avance tecnológico que permite actualmente guardar grandes cantidades de información en espacios muy pequeños.

Por lo tanto, es necesario tener presente algunas de las siguientes medidas que ayudan a mantener el entorno de información con un nivel adecuado de seguridad, ya sea en entornos corporativos como en casa:

- Establecer políticas que definan el uso correcto de dispositivos de almacenamiento removibles, esto ayuda a tener claro las implicaciones de seguridad que conlleva el uso de estos dispositivos.
- Deshabilitar el autoarranque de estos dispositivos en los sistemas operativos de Microsoft Windows en los equipos de la institución.
- De ser necesario, registrar el uso de los mismos.
- Deshabilitar o bloquear dispositivos removibles en equipos sensibles de la institución con la finalidad de evitar sustracción de información.
- Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla, de esta forma en caso de robo o extravío, la información no podrá ser vista por terceros.

- Es recomendable verificar con antivirus cualquier dispositivo que se conecte a la computadora para controlar cada posible infección.

Desde el punto de vista técnico, se podría contar con la más alta tecnología e infraestructura para garantizar un nivel de seguridad aceptable, sin embargo, si estos sistemas no son monitoreados de manera constante no será posible detectar fallas y mucho menos garantizar el servicio que se ofrece.

La verificación o revisión del sistema deberá de realizarse de manera periódica para tener la certeza de que todo funciona de manera adecuada o esperada para determinar anomalías y corregirlas.

La verificación del sistema implica análisis de bitácoras - logs de los distintos servicios que se ofrecen como web, correo, bases de datos IDS, RADIUS, switches, ruteadores, firewalls, e incluso cualquier sistema debería contar con una bitácora que permita analizar procesos, fallas, tiempo de activación del servicio, última actualización y todos los procesos que generen error.

Además del análisis de bitácoras, también es conveniente analizar procesos en tiempo real, lo cual permitirá medir el desempeño del equipo o sistema de cómputo.

Ventajas:

- Recuperación ante incidentes de seguridad.
- Detección ante un comportamiento inusual.
- Evidencia legal.
- Información para resolver problemas.
- Son de utilidad para un análisis forense.

4.9 Concientizar a los usuarios finales

El usuario final es uno de los pilares más débiles en la cadena de los controles empleados para la seguridad, tanto los usuarios como las organizaciones son cada vez más dependientes de Internet, por esta razón se dan recomendaciones que tiene que ser consideradas por el usuario final con el fin de que reduzca la posibilidad de caer en alguno engaño. En consecuencia, se presenta una serie de medidas preventivas:

- Dar curso de Ingeniería Social al personal con la finalidad de anular su impacto.
- No confiar en correos SPAM con archivos adjuntos y explorar el archivo antes de ejecutarlo, esto asegura que no se ejecutará malware.
- Cuando se reciben archivos adjuntos, prestar especial atención a las extensiones de los mismos.
- Evitar publicar la dirección de correo en sitios web de dudosa reputación como sitios de foros, chat, pornográficos, entre otros.

- Emplear filtros anti-spam.

- Evitar responder correo spam.
- Utilizar claves seguras y cambiar la contraseña con periodicidad.
- Eliminar o deshabilitar programas innecesarios.
- Proteger la dirección de correo utilizando una cuenta alternativa.
- Tener en cuenta que las entidades bancarias no solicitan información por correo electrónico.
- Tratar de no acceder a VPN, cuentas bancarias, cuentas de correo desde lugares públicos.
- Tratar de no publicar información sensible y confidencial, debido a que personas extrañas pueden aprovechar esa información con fines maliciosos.
- Evitar el almacenamiento de información confidencial y sensible en computadoras que comparten archivos.
- Es recomendado, dependiendo el grado de confidencialidad que se desea, cifrar todo el sistema operativo.
- Evitar aceptar contactos desconocidos en la mensajería instantánea.

4.10. Controles críticos de seguridad

El SANS (SysAdmin, Audit, Network, Security Institute – Administración de sistemas, auditoría, Red, Instituto de Seguridad) la fuente más confiable y más completa sobre información de seguridad informática, publicó una serie de controles que con base en estudios realizados, son los 20 controles de seguridad más críticos de seguridad de hoy en día:

- Inventario de los dispositivos autorizados y no autorizados.
- Inventario de software autorizado y no autorizado.
- Configuraciones seguras y que cumplan con políticas para servidores, estaciones de trabajo, laptops, etcétera.
- Configuraciones seguras de dispositivos de red.
- Defensa perimetral.
- Mantenimiento y análisis de log; mediante el análisis de las alertas emitidas en cada sistema se realiza una revisión las cuales permiten dar mantenimiento y mejorar el funcionamiento del mismo.
- Seguridad en el software de aplicación, el software que funcione en la red debe ser seguro.
- Uso controlado de los derechos de administrador.
- Acceso controlado de acuerdo con funciones, definir quiénes tienen derecho a qué.

- Mantenimiento y remedio continúo a las vulnerabilidades.
- Control y monitoreo de cuentas, políticas de contraseñas en general.
- Defensa contra malware.
- Limitación y control de puertos de red, protocolos y servicios.
- Control de dispositivos inalámbricos.
- Prevención de pérdida de datos, planes de contingencia, respaldos, control de salida de información.
- Ingeniería de seguridad en redes, es decir, planear una red con la seguridad en mente.
- Pruebas de penetración, tener un plan de evaluación de su red, saber dónde es vulnerable.
- Capacidad de respuesta a incidentes, hay que considerar factores internos como sabotaje o fallas de suministro y factores externos como ataques y fenómenos naturales.
- Capacidad de recuperación de datos, respaldos, una política correcta de respaldos e incluso contar con servidores espejo.
- Capacitación en seguridad, debe haber responsables de la seguridad y contar con capacitación constante.

Así mismo SANS publica una lista con las 20 vulnerabilidades mayormente comprometidas, el propósito de crear esta lista fue ayudar a los administradores a comenzar a asegurar sus equipos contra las más comunes amenazas.[41]

- Vulnerabilidades del lado del cliente.
  - Navegadores Web.
  - Software de oficina.
  - Clientes de correo.
  - Reproductores multimedia.

- Vulnerabilidades en servidores.
  - Aplicaciones web.
  - Servicios de Windows.
  - Servicios de Unix y Mac.
  - Software de respaldo.
  - Software antivirus.
  - Administración de servidores.
  - Software de bases de datos.

[41] The Top Cyber Security Risk, SANS, http://www.sans.org/top20/

- Políticas de seguridad y personal.
  - Derechos de usuario excesivos y dispositivos no autorizados.
  - Phishing.
  - Laptops sin cifrado y dispositivos removibles.

- Abuso de aplicaciones.
  - Mensajería instantánea.
  - Programas punto a punto (Peer-to-Peer).

- Dispositivos de red.
  - Servidores y teléfonos de VoIP.

- Ataques de día cero; todos aquellos nuevos ataques que explotan vulnerabilidades aun no detectadas, que por su característica no existe a la fecha procedimiento de solución.

Algunos años atrás la seguridad de los servidores y servicios fue la principal tarea para la seguridad de una organización, hoy es igual de importante, quizás inclusive más importante es prevenir a los usuarios finales para que no comprometan sus máquinas por medio de páginas web con código malicioso u otros objetivos en el cliente.

4.11. Pruebas de penetración

Una vez implementado todo un esquema de seguridad con todos los mecanismos necesarios para implementar la seguridad, éstos deberán ser sometidos a pruebas de intrusión o penetración haciendo uso de las mismas herramientas que cualquier intruso utilizaría para intentar burlar la seguridad con la finalidad de hallar vulnerabilidades o encontrar algunas cuestiones que no se hayan tomado en cuenta y poder corregirlas antes de que algún intruso lo haga.

No deberá confundirse una prueba de penetración con un ataque real, puesto que un ataque pone en riesgo información, mientras que una prueba será con la finalidad de reforzar, crear o modificar los mecanismos de seguridad.

Para realizar un proceso de penetración deberá especificarse el ámbito donde se aplicará la prueba y puede incluirse una lista específica de las pruebas a realizar o incluso se puede proporcionar una descripción amplia de los procedimientos a realizar.

También es importante establecer límites, ya que en algunas ocasiones existe información con un alto grado de sensibilidad la cual por ningún motivo deberá darse a conocer.

Se debe establecer un tiempo exacto para realizar la prueba, esto con la finalidad de evitar confusiones con las personas encargadas de la seguridad.

Una vez concluidas las pruebas se deberá realizar un reporte ejecutivo con los resultados de las pruebas realizadas, además de un reporte técnico donde se incluyan de manera detallada:

- Los resultados ordenados por prioridad.
- Riesgos a los que está expuesta la organización.
- Requerimientos para disminuir las amenazas.
- Recomendaciones y acciones a realizar.

Una vez generado el reporte, uno de los pasos finales es evaluar los resultados para mejorar las políticas de seguridad de la organización, lo ideal es realizar las pruebas de penetración antes de que las políticas estén completamente terminadas.

Algunas consideraciones importantes a tomar durante las pruebas de penetración, es comprender las razones o motivos por las que un atacante decidiría irrumpir la seguridad, actuar como si se tratase del propio atacante, pensar como un atacante.

Como se mencionó, la importancia de las pruebas de penetración permite revelar vulnerabilidades que pueden ser solucionadas de diferentes maneras:

- Actualizar el sistema afectado.
- Reconfigurar el firewall u otros dispositivos de seguridad.
- Modificar los controles de acceso de aplicaciones y sistemas operativos.

Aunque se realicen pruebas de penetración para determinar fallas técnicas, también es necesario verificar cuestiones de seguridad física, además de realizar un análisis de las políticas establecidas para determinar si éstas son suficientes para garantizar la seguridad.

4.12. Implementar un Plan de Continuidad y Recuperación de Desastres (DRP)

Desde hace tiempo muchas organizaciones, frente a un evento catastrófico, formulan un conjunto de procedimientos que detallen acciones para ser tomadas de manera anticipada frente a una catástrofe, este procedimiento deberá ser diseñado como si el evento catastrófico fuera inevitable, este tipo de planes se conoce como DRP. Es importante recordar que uno de los elementos claves de la seguridad de la información es la *disponibilidad*, la planeación correcta es necesaria para asegurar la disponibilidad de sistemas de misión crítica.

Los requerimientos para un plan de recuperación de desastres varía para cada organización, sin embargo, para la mayoría los objetivos mínimos de plan de recuperación de desastres es brindar la información y procedimientos necesarios para hacer lo siguiente[42]:

- Plan de respuesta a emergencias de cómputo.

[42] Robert Comella, Computer Disaster Recovery Plan Policity, SANS, http://www.sans.org/security-resources/policies/disaster_recovery2.pdf

    - Creación de equipo de recuperación de desastres.
  - Contar con un directorio de las personas que forman el equipo de respuesta.
  - Quién debe ser contactado, cuándo y cómo.
  - Qué acciones inmediatas deben tomarse cuando se presente un evento.

- Sucesión del plan.

  - Notificar al personal necesario para responder al evento.
  - Describe el flujo de responsabilidades cuando un staff normal no está disponible para ejecutar sus obligaciones.

- Estudio de datos.

  - Detalla los datos almacenados en los sistemas, críticos y confidenciales.

- Lista de servicios críticos.

  - Lista todos los servicios brindados y su orden de importancia.

- Plan de restauración y respaldo de datos.

  - Detalla qué datos son respaldados.
  - Los medios de almacenamiento.
  - Lugar de almacenamiento.
  - Tiempos de ejecución de los respaldos.
  - Qué datos deben ser almacenados.

- Plan de reemplazo de equipo.

  - Describe qué equipo es requerido para comenzar a brindar servicio.
  - Lista el orden en que esto es necesario.
  - Nota dónde comprar el equipo.

- El plan debe de ser puesto en acción.

  - Después de crear los planes, es importante practicarlo y extender sus alcances.
  - Durante las pruebas puede causar que el plan falle, lo que permite corregirlo en un entorno de pocas consecuencias.

- El plan debe ser actualizado.

- Revisar los planes por lo menos una vez al año, que permitan incorporar los nuevos procesos en la organización.

- Tener en un lugar estratégico las guías de configuración y bitácoras que muestren el procedimiento a seguir en caso de un evento.

- Contar con sitios alternos que permitan brindar servicios desde sitios físicos diferentes.
- Respuesta a los procesos tan rápidamente como sea posible para asegurar la mínima ruptura en las operaciones de la organización.
- Cumplir con algunos requerimientos regulatorios que dicten la existencia de un plan de recuperación de desastres para la organización.
- Responder a la existencia de un desastre.

Uno de los factores clave en el éxito de un plan de recuperación de desastres, es la planificación apropiada de un grupo que administre las tecnologías de la información. La mayoría de las organizaciones en estos días tiene mucha confianza en el uso de equipos de cómputo, redes de datos, telecomunicaciones y tecnologías de la información en general, como resultado, las TI juegan un papel clave en el plan de recuperación de desastres de las organizaciones.

El plan de recuperación de desastres es una decisión que debe ser considerada como decisión del negocio, el costo de la recuperación debió haber sido comparado contra las pérdidas generadas como resultado de la intervención del servicio.

CAPÍTULO 5
Propuesta de implementación, caso práctico

5.1. Obtención de información de los activos y la infraestructura

La Dirección General del Colegio de Ciencias y Humanidades es la entidad encarga de dirigir correctamente los procesos educativos, académicos, administrativos y técnicos de los 5 planteles de nivel bachillerato, como entidad central de control se maneja una variedad de activos que deberá ser protegida, este capítulo se centra en el análisis de riesgo de la institución, enfocado en los procesos electrónicos y servicios que brinda la institución. La Dirección General del Colegio de Ciencias y Humanidades contemplan el siguiente organigrama, para desempeñar sus funciones (figura 5.1).

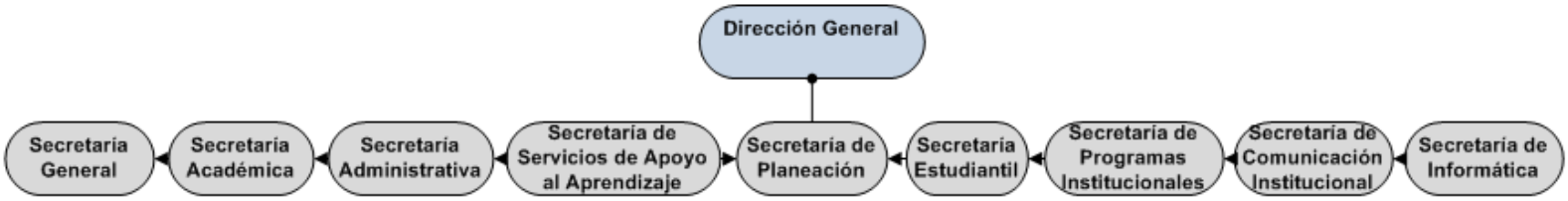


Figura 5. 1 Organigrama Dirección General Colegio de Ciencias y Humanidades.

Una de las Secretarías que conforman el organigrama es la Secretaría de Informática, encargada entre algunas de sus actividades de:

- Evaluar y establecer políticas generales del Colegio de Ciencias y Humanidades en materia de cómputo y telecomunicaciones que apoyen a la Dirección General y a los 5 planteles del colegio, para una toma de decisiones que repercutan en el mejor aprovechamiento de la infraestructura actual.
- Supervisar el uso adecuado de los equipos y redes de cómputo, así como los programas que usan en el colegio.
- Establecer los procesos de capacitación necesarios para el óptimo aprovechamiento de la infraestructura de cómputo y telecomunicaciones.

Estos puntos mencionados, son parte de las actividades que realiza la Secretaría de Informática, tareas relacionadas con este trabajo, que como objetivo plantea "La implementación de un esquema de seguridad perimetral", por lo que la administración, aprobación y mejoras en procesos serán evaluados por la Secretaría de informática.

La fase de la recopilación de información se llevó a cabo empleando:

- Entrevistas y cuestionarios a los responsables de la administración de telecomunicaciones, servidores y sistemas.
- Cuestionarios a los usuarios finales.
- Visitas a sites.
- Recorrido por las instalaciones de la organización.
- Escaneos del segmento de red.

Todo el proceso de identificación de información cae dentro de uno de los pasos de análisis de riesgos, para este caso, el análisis de riesgos está basado en los documentos emitidos por el NIST 800-30 y 800-53, debido a que se utilizan otros documentos de la misma serie SP 800, dedicada a la seguridad de la información y que presenta los mismos beneficios de emplear el análisis de riesgos con base en alguna otra metodología como BS 7799 parte 3, MARGERIT, OCTAVE, COBIT, ISO 27005, entre otros. A continuación se muestra el diagrama del análisis de riesgos basado en la metodología recomendada por NIST 800-30 (figura 5.2).

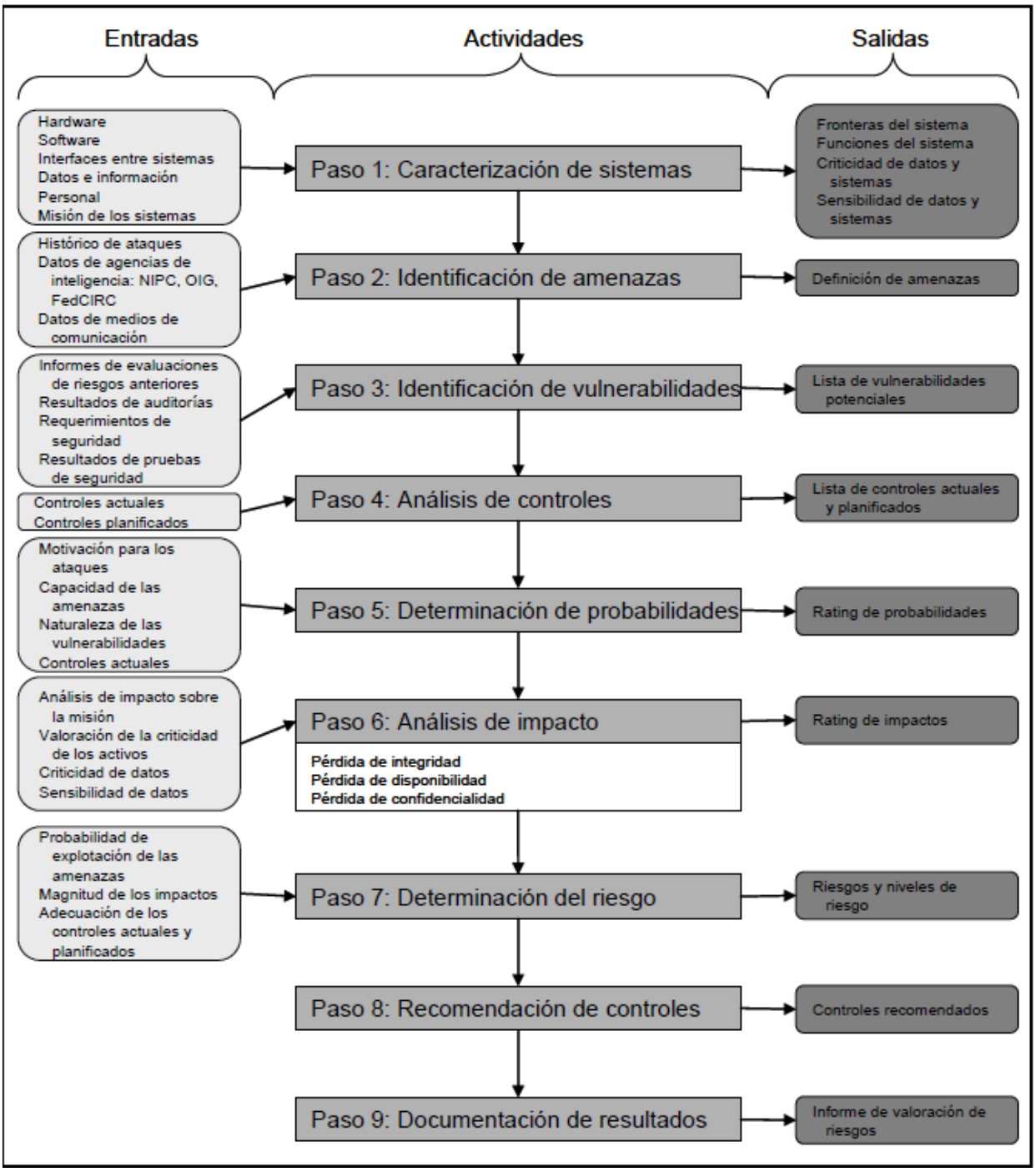


Figura 5. 2 Análisis de Riesgos NIST 800-30.

El análisis de riesgo se centrará en servidores, instalaciones, sistemas y equipos de telecomunicaciones, ya que los controles que se implementarán para gestionar los riesgos serán administrados por la Secretaría de Informática, en caso de que se detecten vulnerabilidades que no puedan ser gestionados por la Secretaría mencionada, sólo se realizará la recomendación pertinente. La obtención de información es uno de los procesos más largos que se realiza al momento de tratar una implementación de seguridad, debido a que muestra el total de activos físicos a proteger. Durante una primera etapa se buscó información a través de documentos, herramientas de escaneo, cuestionarios, entrevistas en sitio a los responsables de servidores e infraestructura por parte de la Secretaría de Informática, solicitando el acceso a la siguiente lista de documentos, políticas y guías de configuración, lo cual corresponde a la documentación técnica de la institución (tabla 5.1).

Tabla 5. 1 Lista de documentos solicitados para revisión .

Documento	Encontrado	Parcialmente	No encontrado
Relación de responsables de activos (Hardware)	X		
Inventario de software utilizado y relación de licencias			X
Inventario de equipos de cómputo	X		
Inventario de la asignación de direcciones IP		X	
Relación de servidores y responsables		X	
Respaldos de servidores			X
Memorias técnicas de la configuración de los servidores			X
Memorias técnicas de la configuración de equipos activos			X
Respaldo de la configuración de equipos activos			X
Informe de seguridad de TI			X
Diagramas de red		X	
Control de modificaciones en configuraciones			X
Memorias técnicas de los sites			X
DRP			X
Guías de hardening para servidores			X
Memorias técnicas de aplicaciones			X
Análisis de riesgo			X
Políticas de instalación para equipos portátiles, servidores y estaciones de trabajo			X
Políticas de monitoreo			X
Políticas de uso de red			X
Política de respaldo			X
Memorias técnicas de cableado estructurado		X	

Es importante aclarar que la lista anterior fueron los puntos solicitados a los responsables, en algunos casos no existe documento que contenga los datos, por lo tanto se contemplan como recomendaciones la elaboración de los mismos, los cuales se justifica su elaboración, con base en el análisis de riesgos.

Continuando con el inventario de activos se listan los componentes que forman parte de la infraestructura tecnológica de la organización (tabla 5.2).

Tabla 5. 2 Resumen de infraestructura.

Activos informáticos	Tipo	Cantidad
Servidores físicos (Hardware)	Servicio	14
Servidores físicos (Software)	Servicio	6
Servidores virtuales (ESX)	Servicio	7
Máquinas virtuales (software)	Servicio	12
Dominios	Servicio	12
Nodos de red	Servicio	270 aproximadamente en uso
Antena WiBox estacionamiento	Servicio	1
Equipos Windows XP	Servicio	171
Equipos Windows vista	Servicio	140
Equipos Windows 7	Servicio	15
Equipos de cómputo UNIX	Servicio	16
Portátiles	Servicio	23
Router	Comunicaciones	2
Switch	Comunicaciones	8
Puntos de acceso	Comunicaciones	3
Cámaras vigilancia IP	Comunicaciones	0
Firewall	Comunicaciones	0
Printserver	Comunicaciones	6
IDS	Comunicaciones	0
Sensores de red	Comunicaciones	1
UPS	Comunicaciones	1
Reguladores	Comunicaciones	40
Sites	Comunicaciones	3
Closet	Comunicaciones	2
Servidores NAT	Comunicaciones	2
Segmentos de red	Comunicaciones	3
Aire acondicionado en sites	Comunicaciones	3
Página web de la institución	Servicio interno y externo	1
Servidores Web otros	Servicio interno y externo	6
Servidores de correo	Servicio interno y externo	1
Antivirus de servidor correo	Servicio interno y externo	1
Antispam en servidor de correo	Servicio interno y externo	1
Servidores de bases de datos	Servicio interno y externo	9
Servidores hotspot	Servicio interno	0
Conexiones a internet	Servicio externo	1
Servidores NAS/SAN	Servicio interno	2
VPN hacia la red interna	Comunicaciones	0
VPN hacia otras entidades	Comunicaciones	2
Servidores de terceros para procesos de la organización.	Servicio externo	1
Cámaras de vigilancia	Monitoreo	8
Personal de seguridad	Vigilancia perimetral	6
Cifrado en medios de almacenamiento	Equipos personales críticos	0
Recursos humanos	Personal	15

De todo el hardware mencionado en la tabla anterior, algunos tienen mayor importancia para la actividad de la institución, los equipos que forman parte de esta categoría se mencionan en la tabla 5.3.

Tabla 5. 3 Relación de equipos críticos para la institución.

Activo	Ubicación	Memoria Técnica
Sw Core FastIron SuperX P 108E-36FO	Site Telecomunicaciones	NO
Sw ServerIron XL P 16E +2FO	Site Servidores	NO
Sw FastIron Edge X424 P 24E + 4FO	Site Servidores	NO
Router Cisco 2800 series P 6E	Site telecomunicaciones	NO
3com 3C16470 P 16E	Soporte	NO APLICA
3com 3C16471 P 24E	Secretaría Administrativa	NO APLICA
Allied AT-8000S P 24E	Closet Salas	NO
Allied AT-8000S P 24E	Control de publicaciones	NO
3com switch 2250 Plus P 50E	Secretaría General	NO
3com 4400 3C172204 P 50E	Medios Digitales	NO
Punto de Acceso Belair	Pasillo Principal	NO
Intel SR2400 Firewall	Site Servidores	NO
Dell PowerEdge 1950 Servidor ESX	Site servidores	NO
Dell PowerEdge 1950 Servidor ESX	Site Servidores	NO
EMC AX150	Site servidores	NO
Silkworm E_200	Site servidores	NO
Dell PowerEdge 1950 centOS vServer	Site servidores	NO
PinetiOn Centro de video vigilancia	Site Telecomunicaciones	----------
IBM System x3550 Servidor Correo	Site Servidores	NO
IBM System x3550 ESX Prueba	Site Servidores	NO
IBM System x3550 Servidor ESX	Site Servidores	NO
Dell PowerEdge 1950 ESX 4	Site Servidores	NO
Dell PowerEdge 1950 ESX 4	Site Servidores	NO
Antena WiBox	Estacionamiento	NO
HP- CPU Cacti	Site Servidores	NO
HP - Pavilion A6100a	Site servidores	NO
HP dx2400	Control presupuestal	NO
HP Proliant ML370	Secretaría General	NO
Aire acondicionado	Site telecomunicaciones	NO APLICA
Aire acondicionado	Site servidores	NO APLICA
Aire acondicionado	Site servidores	NO APLICA
UPS Tripp lite SU6000RT4U 4200W	Site servidores	NO APLICA
UPS ISB 800	Site telecomunicaciones	NO APLICA
UPS Tripp lite omni900lcd 475W	Secretaría de Planeación	NO APLICA

Realizando un análisis de costos en la infraestructura principal de red y servidores, se tiene una inversión en hardware de $2,209,785.69, sin contemplar el costo que representa la información contenida en los diferentes equipos, información que representa la razón de ser de la institución (tabla 5.4).

Tabla 5. 4 Relación de costos de infraestructura crítica.

Equipo	Características	Costo
SERVIDOR	HP PROLIANT	51,173.85
SERVIDOR	INTEL	65,866.84
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	IBM 41U	86,250.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,194.99
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
SERVIDOR	DELL	96,195.00
STORAGE	EMC2	253,000.00
SWITCH	SILKWORM	74,951.01
SWITCH	3COM	7,348.50
SWITCH	3COM	7,348.50
SWITCH	ALLIED	7,348.50
SWITCH	ALLIED	7,348.50
SWITCH	FOUNDRY,FESX424	54,339.80
SWITCH	FOUNDRY,FCSLB16	113,999.99
SWITCH	3COM	10,062.50
SWITCH	FOUNDRY F1-8X1	465,000.00
ROUTER	CISCO 2821	40,825.00
ROUTER	CISCO 2821	40,825.00
ROUTER	CISCO 2801	40,825.00
PUNTO DE ACCESO	BELAIR	52,750.00
UPS	TRIPP LITE	46,000.00
ACONDICIONADOR DE AIRE	CARRIER	16,617.50
ACONDICIONADOR DE AIRE	MITSUBISHI	22,655.00
ACONDICIONADOR DE AIRE	MITSUBISHI	22,655.00
KVM	17FP	5,480.00

La siguiente relación muestra el total de activos lógicos importantes para la institución, administrados por 9 personas, esta tarea contemplando todos los servicios brindados hacia la comunidad, que incluyen servicio web, bases de datos, correo, sensores de red y servidores virtuales, con un total de 31 servicios (tabla 5.5).

Tabla 5. 5 Servicios críticos para la institución.

Servicio	URL
1) Registros Intra CCH	academia.cch.unam.mx/intracch
2) Página web institucional	www.cch.unam.mx
3) Correo institucional	correo.cch.unam.mx
4) Web moodle academia	academia.cch.unam.mx
5) Web moodle Inglés	idiomas.portalacademico.cch.unam.mx/moodle/login/index.php
6) Web moodle Portal Académico	portalacademico.cch.unam.mx
7) Web formación de profesores	132.248.122.4/tacur/
8) Web Control de datos personal Académico	dcdpa.cch.unam.mx
9) Web programa de seguimiento integral	psi.cch.unam.mx
10) Web página Secretaría de Planeación	seplan.cch.unam.mx
11) VMware ESX server 4.0	----------
12) VMWare ESX server 4.0	----------
13) VMware ESX server 4.0	----------
14) VMware ESX server 4.0	----------
15) VMware ESX server 4.0	----------
16) Router Cisco	----------
17) AccessCar	----------
18) ViCenter - Vmware	----------
19) VMware vServer	----------
20) Base de datos portal académico	portalacademico.cch.unam.mx
21) Base de datos PSI	psi.cch.unam.mx
22) Base de datos intraCCH	academia.cch.unam.mx/intracch
23) Base de datos spac-e	spac-e.cch.unam.mx
24) Base de datos portal DGCCH	www.cch.unam.mx
25) Base de datos academia en línea	academia.cch.unam.mx
26) Base de datos DCDPA	dcdpa.cch.unam.mx
27) Base de datos AccessCar	----------
28) Base de datos control presupuestal	----------
29) Base de datos planeación	seplan.cch.unam.mx
30) Enlace internet Red UNAM	----------
31) Cacti - monitor de red	----------
32) Servidor web Secretaría de Planeación	seplan.cch.unam.mx
33) Servidor web spac-e	----------

Cuando se evaluó el estado de la red, contemplando su distribución física, se observó que no existía ningún dispositivo de seguridad implementado, a continuación se muestra el diagrama de red, que se tenía en la institución antes de la implementación del esquema de seguridad propuesto (figura 5.3).

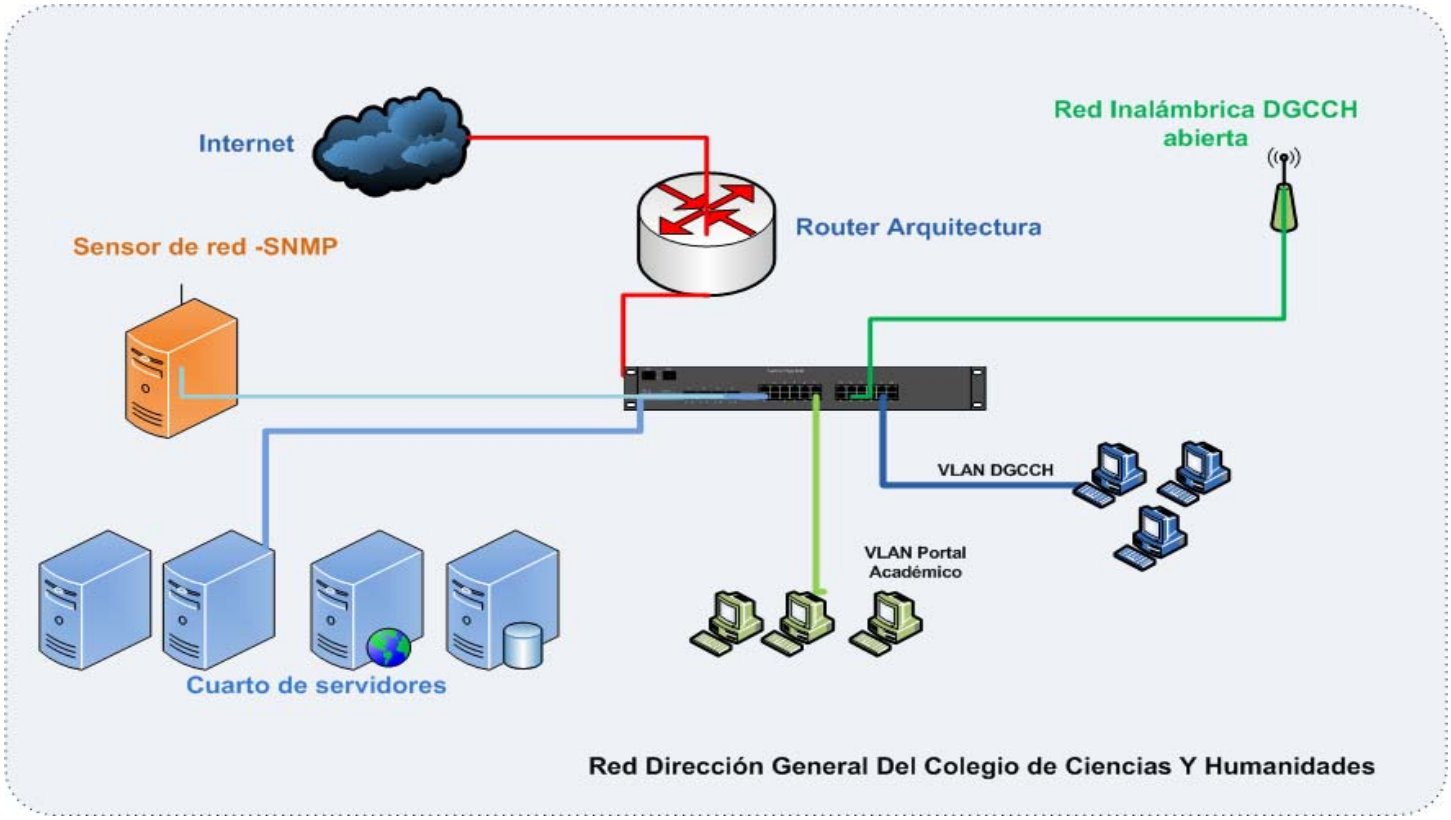


Figura 5. 3 Diagrama de red, antes de la implementación del esquema de seguridad.

Para la mayoría de los servidores y dispositivos activos se planea la elaboración de memorias técnicas, documentos que ayudarán a identificar configuraciones actuales, puertos abiertos, distribución de sistema operativo, características de hardware, conexión física y protocolos que emplean para su administración.

5.2. Análisis de riesgo de la situación actual

La información recabada como parte del análisis de riesgos fue útil para determinar la relación de las posibles amenazas a las que están expuestos los activos, desde los niveles directivos hasta los niveles técnicos. Con base en los activos reportados anteriormente e históricos de actividades arrojados en las entrevistas, escaneo de puertos, se determinaron las amenazas, definidas en el Paso 2 “Identificación de amenazas”, que en conjunto con los resultados de prueba de seguridad y entrevistas en sitio, se encontraron las vulnerabilidades definidas en el Paso 3 definido en NIST 800-30, "Identificación de vulnerabilidades” (tabla 5.6).

Tabla 5. 6 Identificación de vulnerabilidades.

Amenaza	Vulnerabilidad
▪ Usuarios internos ▪ Usuarios malintencionados ▪ Usuarios poco capacitados ▪ Usuarios deshonestos ▪ Usuarios negligentes	1. Inexistencia o falta de : • Identificación con credencial del personal que ingresa a la institución. • Controles de acceso físicos a oficinas. • Bitácoras para visitantes en los departamentos. • Controles de acceso a aplicaciones. • Controles de acceso a servidores y equipos activos. • Control de acceso a computadoras. • Control de asignación de direcciones IP's en el segmento de la institución. • Control de tráfico de red. • Control de acceso en la red inalámbrica. • Mecanismos de control perimetral de la red. • Personal que atienda un incidente de seguridad. • Políticas de confidencialidad. • Políticas de uso de la red. • Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Conocimientos de empleados en temas de seguridad. • Actualización de firmware en equipos de red. • Actualizaciones en los sistemas operativos y aplicaciones. • Actualización en antivirus. • Mantenimiento en servidores y equipo de telecomunicación. • Mantenimiento preventivo en equipos de cómputo. • Mantenimiento a equipos de aire acondicionado. • Mantenimiento a estaciones eléctricas. • Corriente eléctrica regulada. • Cifrado en discos duros. • Respaldos de información. • Respaldos de configuración de equipos activos • UPS con capacidad suficiente. • Fuente de corriente eléctrica alterna. • Capacitación. • Separación de funciones de los empleados. • Información en temas de seguridad. • Sites alternos 2. Tableros eléctricos expuestos. 3. Fallas eléctricas. 4. Fallas en equipos de cómputo. 5. Límites de uso de memoria y procesador en servidor. 6. Cableado de red expuesto a los usuarios.

	7. Respaldos en USB sin cifrado. 8. Respaldos en mismo disco duro. 9. Parámetros de configuración por default en equipos activos, servidores y Printserver. 10. Acceso a todas las terminales de administración. 11. Acceso a todos los recursos de red. 12. Acceso total a todos los recursos de Internet. 13. Tiempo de vida útil de un equipo. 14. Uso de la misma contraseña por periodos largos de tiempo. 15. Uso de una contraseña única en varios equipos. 16. Uso de contraseñas no robustas. 17. Uso de protocolos de administración inseguros. 18. Descuidos del personal que labora en la institución. 19. Confianza en otras personas. 20. Uso de IP homologadas para usuarios en general. 21. Fallas por parte del proveedor del servicio de internet. 22. Fallas por parte del proveedor suministro eléctrico.
Usuarios externos ▪ Delincuencia ▪ Hacker ▪ Crackers ▪ Ex empleados ▪ Otras instituciones ▪ Etcétera.	1) Falta de : • Identificación con credencial del personal que ingresa a la institución. • Controles de acceso físicos a oficinas. • Bitácoras para visitantes en los departamentos. • Controles de acceso a aplicaciones. • Controles de acceso a servidores y equipos activos. • Control de acceso a computadoras. • Control de asignación de direcciones IP's en el segmento de la institución. • Control de tráfico de red. • Control de acceso en la red inalámbrica. • Mecanismos de control perimetral de la red. • Personal que atienda un incidente de seguridad. • Políticas de confidencialidad. • Políticas de uso de la red. • Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Conocimientos de empleados en temas de seguridad. • Actualización de firmware en equipos de red. • Actualizaciones en los sistemas operativos y aplicaciones. • Actualización en antivirus. • Mantenimiento en servidores y equipo de telecomunicación. • Mantenimiento preventivo en equipos de cómputo. • Mantenimiento a estaciones eléctricas. • Corriente eléctrica regulada.

	• Cifrado en discos duros. • Respaldos de información. • Respaldos de configuración de equipos activos • UPS con capacidad suficiente. • Fuente de corriente eléctrica alterna. • Capacitación. • Información en temas de seguridad. • Separación de funciones de los empleados. • Sites alternos 2) Tableros eléctricos expuestos. 3) Limites de uso de memoria y procesador en servidor. 4) Cableado de red expuesto a los usuarios. 5) Respaldos en USB sin cifrado. 6) Respaldos en mismo disco duro. 7) Parámetros de configuración por default en equipos activos, servidores y Printserver. 8) Acceso a todas las terminales de administración. 9) Acceso a todos los recursos de red. 10) Acceso total a todos los recursos de Internet. 11) Uso de la misma contraseña por periodos largos de tiempo. 12) Uso de una contraseña única en varios equipos. 13) Uso de contraseñas no robustas. 14) Uso de protocolos de administración inseguros. 15) Descuidos del personal que labora en la institución. 16) Confianza en otras personas. 17) Uso de IP homologadas para usuarios en general. 18) Fallas por parte del proveedor del servicio de internet. 19) Fallas por parte del proveedor suministro eléctrico.
Desastres Naturales	1) Falta de: • Planeación relacionada con la infraestructura de la organización. • Impermeabilizado. • Tuberías aisladas. • Mantenimiento en cableado eléctrico. • Controles de humedad. • Controles de temperatura. 2) Fallas en diseño construcción de los Sites. 3) Tableros eléctricos expuestos. 4) Instalación de red expuesta. 5) Equipos de telecomunicaciones expuestos.
Amenazas Lógicas ▪ Virus ▪ Gusanos ▪ Troyanos ▪ Botnet ▪ Malware ▪ Spyware	1) Falta de : • Dispositivos de seguridad perimetral. • Actualización en software. • Actualización en sistemas operativos. • Actualización en firmware de dispositivos. • Políticas de confidencialidad. • Políticas de uso de la red.

▪ Etcétera.	• Políticas sobre el manejo de información. • Políticas de seguridad en sistemas operativos. • Políticas de seguridad en servidores Windows /Linux. • Políticas de seguridad en dispositivos activos. • Políticas de contraseñas. • Políticas de desarrollo de software seguro. 2) URL con software malicioso. 3) Descarga de ejecutables desde sitios no confiables. 4) Instalación de software pirata. 5) Instalación de software crackeado. 6) Descarga de software de recursos peer to peer (P2P). 7) Configuración por default. 8) Auto arranque de dispositivos extraíbles en terminales y servidores. 9) Debilidades en los protocolos de comunicación. 10) Errores de configuración de los sistemas. 11) Mecanismos de administración remota vulnerables. 12) Contraseñas basadas en palabras de diccionario. 13) Vulnerabilidades de las versiones empleadas en los servidores. 14) Ataques conocidos a sistemas operativos. 15) Puertos abiertos sin utilización. 16) Falta de conocimiento en temas de seguridad.

A continuación se cita una serie de observaciones críticas, relacionado con la infraestructura actual que se tiene:

- Es importante mencionar que la mayoría de los equipos de telecomunicación, comparten una misma contraseña, no recomendables, ya que debilita la seguridad, además de utilizar protocolos de administración inseguros, lo que en conjunto crea un punto crítico de seguridad.
- Se realizaron escaneos desde el exterior de la red institucional, que mostraron acceso a puertos innecesarios en los servidores críticos de la institución, así como acceso a printserver, switch y router, en si todo aquello que tenga un puerto abierto.
- Algunos de los equipos tienen configuraciones por default, permitiendo tener acceso a la configuración, con solo conocer las cuentas preestablecidas por el fabricante.
- No se cuenta con respaldo de la configuración actual que tienen los equipos activos como switch, router y puntos de acceso.
- Por la fecha de adquisición de los equipos, actualmente ninguno de éstos cuenta con garantía, lo que ocasiona que en el momento de fallas de hardware se pierda disponibilidad en los servicios soportados por el hardware dañado, que en puntos críticos puede ocasionar pérdida de servicio o información.
- La red inalámbrica en funcionamiento, no cuenta con algún mecanismo de autenticación y cifrado, lo que permite a cualquier persona hacer uso de los recursos sin ninguna restricción y seguimiento de sus actividades.
- El cableado de red de la institución no se ha actualizado en varios años, se han improvisado conexiones que se quedaron de manera permanente, se recomienda considerar una instalación de cableado estructurado en todo el edificio, para salvaguardar el acceso físico a los medios de transmisión de datos.

- En cuestión al monitoreo y seguridad, se tiene actualmente sólo un sensor que permite verificar el estado de los dispositivos, no se cuenta con un esquema de seguridad perimetral lo que permite a los atacantes tener acceso a todos los puntos de conexión de la institución, servidores y equipos activos. Se recomienda establecer un esquema de seguridad perimetral que permita monitorear el uso de la red con mayor detalle y establecer políticas de acceso sólo a aquellos recursos que deben estar visibles para los usuarios finales.

- Actualmente el equipo UPS ubicado en el site principal, no soportan la carga de corriente requerida, estando por debajo del 50% del total de consumo actual, el UPS actual tiene un soporte de 4200[W], teniendo un consumo de 13000 [W], lo que ocasiona que en fallas eléctricas no se cuente con la protección eléctrica adecuada.
  - 1 Storage EMC AX-150, con una fuente de 315 VA (300 Watts)
  - 1 Switch de fibra Brocade Silkworm 200e de 45 Watts a 60 Watts
  - 1 Switch Foundry X424 de con una fuente de 220 Watts
  - 1 Switch Foundry ServerIron con una fuente de 550 Watts
  - 5 Servers Dell PowerEdge 1950 con dos fuentes, cada una de 670 Watts (6700 Watts en total)
  - 4 Servers IBM X3550 con dos fuentes, cada una de 670 Watts (5360 Watts en total)
  - 1 Server Intel con una fuente de 550 Watts
  - 1 Switch KVM Dell de 40 Watts
  - 1 Consola de administración Dell, entre los 40 y 50 Watts.

  Total en watts 13.820 KW

- La instalación de los equipos de cómputo de los usuarios finales, se realiza siguiendo un procedimiento específico, que limite al usuario final para sólo tener acceso a ciertos recursos del equipo, dicho procedimiento deberá ser revisado para garantizar su óptimo funcionamiento.

- Cuando se presentan incidentes de seguridad reportados por DGTIC, la solución parcial en atención al incidente, es notificar a soporte para su corrección, el tiempo que soporte tome para resolver el incidente, permanecerá en operación la actividad maliciosa del equipo comprometido.

El siguiente punto considerado en la metodología es paso 4: "*análisis de los controles"*, mostrando una lista de controles con los que se cuenta actualmente y aquellos que se planifican a futuro, para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad (Ver apéndice D).

Para obtener la *probabilidad de ocurrencia y el análisis de impacto*, paso 5 y 6 respectivamente, se determinaron con base en las entrevistas, revisión de instalaciones, visitas en sitio, cuestionarios realizados y decisiones gerenciales. Con base en los siguientes criterios se determinó la prioridad de atención de los riesgos. Al momento de determinar el impacto, la estimación se realizó del tipo cualitativo, se considero un activo importante con base en el tipo de información que maneja, debido a que tratar de estimar su valor económico es muy complicado y variado, pero el hecho de pérdida de disponibilidad, confidencialidad o integridad del activo afecta significativamente el funcionamiento de la institución (tabla 5.7).

Tabla 5. 7 Matriz de nivel de atención de riesgos.

		Probabilidad/ Likelihood		
		Alto(1.0)	Medio (0.5)	Bajo (0.1)
Impacto Impact	Alto(100)	Alto (100x1)	Medio (100x0.5)	Bajo (100x0.1)
	Medio (50)	Medio (50x1)	Medio (50x0.5)	Bajo (50x0.1)
	Bajo (10)	Medio (10x1)	Bajo (0.16)	Bajo(0.08)

Alto (>50 a 100); Medio (>10 a 50); Bajo (1 a 10)

- ***Alto;*** se requiere fuertemente la necesidad de tomar acciones correctivas.
- ***Medio;*** acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar estas acciones en un periodo de tiempo.
- ***Bajo;*** se observó un bajo riesgo y se deberá determinar si se tomarán acciones correctivas o decidir aceptar el riesgo.

Una vez realizado el levantamiento de activos, amenazas, vulnerabilidades, probabilidad de ocurrencia e impacto, se realiza una evaluación de los riesgos para priorizar los niveles de atención, las opciones de los riesgos son:

- ***Mitigación del riesgo;*** implementando controles que reduzcan la probabilidad de ocurrencia.
- ***Transferir el riesgo;*** con base en el análisis de riesgo contemplar la posibilidad de que algunos controles sean realizados por terceros (outsourcing), en algunas veces reduce costos.
- ***Aceptar el riesgo;*** tener conocimiento de los riesgos a los que se está expuesto, aceptando la posibilidad de que se presenten.
- ***Evitar el riesgo;*** las acciones están orientadas a cambiar las actividades o la manera de desempeñar una actividad en particular
- ***Riesgo residual;*** después de implantar los controles necesarios para el tratamiento de los riesgos, por lo general se encuentran remanentes. Lo que se conoce como riesgo residual.

En la tabla 5.8 se muestra la determinación del riesgo, basado en la matriz de nivel de atención de riesgos (tabla 5.7), la cual muestra la probabilidad de explotación de las vulnerabilidades por parte de las diversas amenazas.

Tabla 5. 8 Probabilidad de impacto y ocurrencia.

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Red inalámbrica abierta	Alta	Alto	Confidencialidad	**Alto**
Inexistencia de controles sobre el uso de la red inalámbrica	Alta	Alto	Disponibilidad	**Alto**
Poco control en la administración de direcciones IP	Alta	Alto	Disponibilidad	**Alto**
Inexistencia de control en la información descargada a través de la red de la institución	Alta	Alto	Integridad	**Alto**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Falta de cuidado del equipo de cómputo	Alta	Alto	Disponibilidad	**Alto**
Limitantes de potencia en UPS	Alta	Alto	Disponibilidad	**Alto**
Falta de mecanismos de control perimetral de la red	Alta	Alto	CIA	**Alto**
Uso de protocolos de administración inseguros	Alta	Alto	CIA	**Alto**
Inexistencia de políticas de uso de red	Alta	Alto	CIA	**Alto**
Inexistencia de políticas para servidores	Alta	Alto	CIA	**Alto**
Inexistencia de respaldos en equipos activos	Alta	Alto	Integridad	**Alto**
Acceso a todos los recursos de red institucional	Alta	Alto	CIA	**Alto**
Uso de una misma contraseña por periodos largos de tiempo	Alta	Alto	CIA	**Alto**
Uso de una contraseña única en varios equipos	Alta	Alto	CIA	**Alto**
Uso de contraseñas no robustas	Alta	Alto	CIA	**Alto**
Confianza en otras personas	Alta	Alto	Confidencialidad	**Alto**
Uso de IP's homologadas para usuarios en general	Alta	Alto	Confidencialidad	**Alto**
Fallas por parte del proveedor del suministro eléctrico	Alta	Alto	Disponibilidad	**Alto**
Puertos abiertos sin uso en estación de trabajo	Alta	Alto	CIA	**Alto**
Inexistencia de respaldos en las diferentes Secretarías	Media	Alto	Confidencialidad	**Medio**
Tableros eléctricos expuestos	Alta	Medio	Disponibilidad	**Medio**
Controles de acceso inseguros para administración de servidores	Media	Alto	Integridad	**Medio**
Vulnerabilidades inherentes del protocolo TCP/IP	Media	Alto	Confidencialidad	**Medio**
Daño en hardware por fallas eléctricas	Media	Alto	Disponibilidad	**Medio**
Inexistencia de control en el tráfico de red generado por la institución	Alta	Medio	Disponibilidad	**Medio**
Fuga de información	Media	Mediano	Confidencialidad	**Medio**
Daño físico a la infraestructura de red	Media	Alto	Disponibilidad	**Medio**
Puertos abiertos sin motivo en servidores críticos	Media	Alto	Confidencialidad	**Medio**
Inexistencia de controles de seguridad en portátiles	Alta	Medio	Confidencialidad	**Medio**
Inexistencia de monitoreo de uso de la red	Alta	Medio	Disponibilidad	**Medio**
Fallas en sistemas de aire acondicionado	Media	Alto	Disponibilidad	**Medio**
Control de acceso débil en aplicaciones	Media	Alto	Confidencialidad	**Medio**
Personal poco capacitado en temas de seguridad	Media	Alto	CIA	**Medio**
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red	Media	Alto	CIA	**Medio**
Falta de mantenimiento preventivo en servidores y equipos activos	Alta	Medio	Disponibilidad	**Medio**
Falta de mantenimiento de estaciones eléctricas	Media	Alto	Disponibilidad	**Medio**
Falta de corriente eléctrica regulada	Alta	Medio	Disponibilidad	**Medio**
Inexistencia de fuente de corriente eléctrica alterna	Alta	Medio	Disponibilidad	**Medio**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Inexistencia de planes de capacitación	Alta	Medio	CIA	**Medio**
Inexistencia de Sites alternos	Alta	Medio	Disponibilidad	**Medio**
Cableado de red expuesto	Alta	Medio	Disponibilidad	**Medio**
Respaldos en mismo disco duro	Alta	Medio	Disponibilidad	**Medio**
Parámetros por default en equipos activos	Media	Alto	CIA	**Medio**
Acceso a todas las terminales de administración	Media	Alto	Integridad	**Medio**
Acceso a todos los recursos de internet	Alta	Medio	CIA	**Medio**
Uso de protocolos de comunicación inseguros	Media	Alto	CIA	**Medio**
Falta de mantenimiento en cableado eléctrico	Media	Alto	Disponibilidad	**Medio**
Inexistencia de controles de humedad	Alta	Medio	Disponibilidad	**Medio**
Inexistencia de controles de temperatura	Alta	Medio	Disponibilidad	**Medio**
Consultas de sitios con software malicioso	Alta	Medio	CIA	**Medio**
Descarga de ejecutables de sitios no confiables	Alta	Medio	CIA	**Medio**
Inexistencia de políticas sobre el uso del equipo de cómputo	Alta	Medio	CIA	**Medio**
Autoarranque de dispositivos extraíbles	Alta	Medio	CIA	**Medio**
Falta de políticas de desarrollo de software seguro	Alta	Medio	CIA	**Medio**
Inexistencia de controles de integridad en equipos activos	Alta	Medio	Integridad	**Medio**
Firmas antivirus deficientes	Media	Medio	Confidencialidad	**Medio**
Inexistencia de políticas de uso de software	Media	Medio	Disponibilidad	**Medio**
Poco control sobre los respaldos	Media	Medio	Confidencialidad	**Medio**
Filtrado de agua a sites	Media	Medio	Disponibilidad	**Medio**
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda	Media	Medio	Disponibilidad	**Medio**
Falta de procedimientos de creación de cuentas	Media	Medio	Disponibilidad	**Medio**
Vulnerabilidades inherentes a las aplicaciones	Media	Medio	Disponibilidad	**Medio**
Tiempo de vida útil de los equipos	Media	Medio	Disponibilidad	**Medio**
Tuberías expuestas	Media	Medio	Disponibilidad	**Medio**
Uso de versiones viejas en aplicaciones	Media	Medio	CIA	**Medio**
Vulnerabilidades conocidas en sistemas operativos	Media	Medio	CIA	**Medio**
Empleo de software sin actualizaciones	Media	Medio	CIA	**Medio**
Inexistencia de auditorías	Alta	Bajo	CIA	**Bajo**
Limitantes de espacio en disco duro en servidores	Baja	Alto	Disponibilidad	**Bajo**
Fallas eléctricas	Baja	Alto	Disponibilidad	**Bajo**
Inexistencia de cultura de seguridad en usuarios finales	Baja	Alto	Integridad	**Bajo**
Inexistencia de control perimetral de los puertos permitidos	Alta	Bajo	Disponibilidad	**Bajo**
Inexistencia de procedimientos de cambios en sistemas	Alta	Bajo	Integridad	**Bajo**
Inexistencia de políticas en sistemas operativos	Alta	Bajo	CIA	**Bajo**

Vulnerabilidad	Probabilidad de ocurrencia	Impacto	Principio de seguridad afectado	Nivel de atención del Riesgo
Inexistencia de cifrado en discos duros	Alta	Bajo	Confidencialidad	**Bajo**
Poca separación de funciones criticas	Baja	Alto	CIA	**Bajo**
USB sin cifrado	Alta	Bajo	Confidencialidad	**Bajo**
Fallas por parte del proveedor de servicios de internet	Baja	Alto	Disponibilidad	**Bajo**
Daños en la configuración de los equipos por poco mantenimiento	Baja	Medio	Integridad	**Bajo**
Descuido en el manejo del hardware	Baja	Medio	Disponibilidad	**Bajo**
Errores de cambios en la configuración de equipos activos y servidores	Baja	Medio	Integridad	**Bajo**
Inexistencia de control a servicios de servidores	Media	Bajo	Confidencialidad	**Bajo**
Inexistencia de políticas de confidencialidad	Baja	Medio	Confidencialidad	**Bajo**
Inexistencia de monitoreo de las aplicaciones	Baja	Medio	Disponibilidad	**Bajo**
Poca educación sobre temas de seguridad a usuarios finales	Baja	Medio	Integridad	**Bajo**
Errores humanos	Baja	Medio	Disponibilidad	**Bajo**
Aprovechamiento de vulnerabilidades de controles físicos	Baja	Medio	Disponibilidad	**Bajo**
Falta de gestión de garantías	Baja	Medio	Disponibilidad	**Bajo**
Interferencias magnéticas	Baja	Bajo	Disponibilidad	**Bajo**
Desastres naturales en la institución	Baja	Bajo	Disponibilidad	**Bajo**

5.3. Alcance y requerimientos de la propuesta

Los controles que pueden mitigar o eliminar los riesgos identificados son señalados para su implementación o planeación, el objetivo de la recomendación de los siguientes controles es reducir el nivel de riesgo, a un nivel aceptable por la dirección.

Después de evaluar el riesgo de cada vulnerabilidad, se determinó con aprobación de la gerencia si el riesgo se mitiga, transfiere o acepta. Como resultado se tiene la propuesta de controles para elaborar una estrategia de seguridad. A la hora de tomar acciones correctivas se encontró que no todos los controles se pueden implementar, el proyecto presentó una serie de restricciones, no necesariamente técnicas que establecen un marco al que debe limitarse, éste contempla decisiones gerenciales y/o mecánicas de trabajo, por ejemplo:

- La cantidad de recursos asignados.
- La forma de planificar el gasto y de ejecutar el presupuesto. En este punto se aprovecharon los recursos con los que cuenta la institución, contemplado gastos mínimos.
- La cultura o forma interna de trabajo puede ser incompatible con ciertos controles.
- Rechazo de controles, por el personal de la institución.

A continuación se realiza un listado de las vulnerabilidades detectadas, con base en el nivel de atención del riesgo, a las cuales se sugiere uno o varios controles que permitan reducir la posibilidad de ocurrencia de los riesgos (tabla 5.9).

Tabla 5. 9 Controles recomendados, con base en el análisis de riesgo.

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Red inalámbrica abierta	Alto	Hotspot, servidor RADIUS, cifrado
Inexistencia de controles sobre el uso de la red inalámbrica	Alto	Hotspot, servidor RADIUS, cifrado
Poco control en la administración de direcciones IP	Alto	Inventario de gestión de direcciones IP
Inexistencia de control en la información descargada a través de la red de la institución	Alto	Firewall, filtrado de contenido
Falta de cuidado del equipo de cómputo	Alto	Concientización en temas de seguridad
Limitantes de potencia en UPS	Alto	Evaluación y adquisición de un UPS
Falta de mecanismos de control perimetral de la red	Alto	Firewall, IDS, gestor de uso de red
Uso de protocolos de administración inseguros	Alto	Políticas de configuración de equipos activos
Inexistencia de políticas de uso de red	Alto	Elaboración de políticas de uso de red
Inexistencia de políticas para servidores	Alto	Elaboración de políticas para servidores
Inexistencia de respaldos en equipos activos	Alto	Elaboración de políticas de respaldo
Acceso a todos los recursos de red institucional	Alto	Firewall perimetral, firewall site de servidores, vlan's, NAT's
Uso de una misma contraseña por periodos largos de tiempo	Alto	Políticas de contraseñas
Uso de una contraseña única en varios equipos	Alto	Políticas de contraseñas, concientización en temas de seguridad
Uso de contraseñas no robustas	Alto	Políticas de contraseñas, concientización en temas de seguridad
Confianza en otras personas	Alto	Concientización en temas de seguridad
Uso de IP's homologadas para usuarios en general	Alto	Vlan, NAT
Fallas por parte del proveedor del suministro eléctrico	Alto	Emitir recomendaciones a la Secretaría Administrativa
Puertos abiertos sin uso en estación de trabajo	Alto	Políticas de hardening en estaciones de trabajo
Inexistencia de respaldos en las diferentes secretarías	Medio	Políticas de respaldo
Tableros eléctricos expuestos	Medio	Informar de la observación a la Secretaría Administrativa
Controles de acceso físicos, inseguros para administración de servidores	Medio	Implementar controles biométricos en los sites
Vulnerabilidades inherentes del protocolo TCP/IP	Medio	Políticas de monitoreo
Daño en hardware por fallas eléctricas	Medio	UPS
Inexistencia de control en el tráfico de red generado por la institución	Medio	Gestor de uso de red, balanceadores de carga

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Fuga de información	Medio	Políticas de confidencialidad
Daño físico a la infraestructura de red	Medio	Cableado estructurado
Puertos abiertos sin motivo en servidores críticos	Medio	Políticas de hardening en servidores
Inexistencia de controles de seguridad en portátiles	Medio	RFID, bandas magnéticas, cintas de seguridad para portátiles
Inexistencia de monitoreo de uso de la red	Medio	Políticas de monitoreo
Fallas en sistemas de aire acondicionado	Medio	Mantenimiento preventivo
Control de acceso débil en aplicaciones	Medio	Políticas desarrollo de software seguro
Personal poco capacitado en temas de seguridad	Medio	Capacitación del personal
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red	Medio	Políticas de hardening en estaciones de trabajo y Políticas de hardening en servidores
Falta de mantenimiento preventivo en servidores y equipos activos	Medio	Mantenimiento preventivo en servidores y equipo activo
Falta de mantenimiento de estaciones eléctricas	Medio	Mantenimiento preventivo en estaciones eléctricas
Falta de corriente eléctrica regulada	Medio	Implementar reguladores en la mayoría de los equipos
Inexistencia de fuente de corriente eléctrica alterna	Medio	Planta eléctrica
Inexistencia de planes de capacitación	Medio	Capacitación del personal
Inexistencia de sites alternos	Medio	Contratos con compañías o acuerdos con otras instituciones
Cableado de red expuesto	Medio	Cableado estructurado
Respaldos en mismo disco duro	Medio	Políticas de respaldo
Parámetros por default en equipos activos	Medio	Políticas de configuración de equipos activos
Acceso a todas las terminales de administración	Medio	Firewall perimetral, firewall Site servidores, listas de control de acceso
Acceso a todos los recursos de internet	Medio	Firewall, gestor de contenido
Uso de protocolos de comunicación inseguros	Medio	Implementación de comunicaciones cifradas
Falta de mantenimiento en cableado eléctrico	Medio	Mantenimiento preventivo en la institución
Inexistencia de controles de humedad	Medio	Sensor de humedad
Inexistencia de controles de temperatura	Medio	Sensor de temperatura
Consultas de sitios con software malicioso	Medio	Gestor de contenido, capacitación al usuario
Descarga de ejecutables de sitios no confiables	Medio	Gestor de contenido, capacitación al usuario
Inexistencia de políticas sobre el uso del equipo de cómputo	Medio	Políticas sobre el uso del equipo de cómputo

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Autoarranque de dispositivos extraíbles	Medio	Políticas de hardening en estaciones de trabajo
Falta de políticas de desarrollo de software seguro	Medio	Políticas de desarrollo de software seguro
Inexistencia de controles de integridad en equipos activos	Medio	Memorias técnicas y respaldos de configuración
Firmas antivirus deficientes	Medio	Evaluación y adquisición de un antivirus
Inexistencia de políticas de uso de software	Medio	Políticas de hardening en estaciones de trabajo
Poco control sobre los respaldos	Medio	Políticas de control de cambios y políticas de respaldo
Filtrado de agua a Sites	Medio	Mantenimiento preventivo
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda	Medio	Políticas de hardening en servidores
Falta de procedimientos de creación de cuentas	Medio	Políticas de contraseñas
Vulnerabilidades inherentes a las aplicaciones	Medio	Actualizaciones
Tiempo de vida útil de los equipos	Medio	Mantenimiento preventivo, renovación de hardware
Tuberías expuestas	Medio	Restructuración de instalación eléctrica, mantenimiento
Uso de versiones viejas en aplicaciones	Medio	Actualizaciones
Vulnerabilidades conocidas en sistemas operativos	Medio	Actualizaciones
Empleo de software sin actualizaciones	Medio	Actualizaciones
Inexistencia de auditorías	Bajo	Planificación de auditorias
Limitantes de espacio en disco duro en servidores	Bajo	Evaluación y adquisición de medios de almacenamiento masivo
Fallas eléctricas	Bajo	Mantenimiento general a la red Eléctrica
Inexistencia de cultura de seguridad en usuarios finales	Bajo	Capacitación del personal
Inexistencia de control perimetral de los puertos permitidos	Bajo	Firewall perimetral, IDS
Inexistencia de procedimientos de cambios en sistemas	Bajo	Políticas de control de cambios
Inexistencia de políticas en sistemas operativos	Bajo	Políticas de hardening en estaciones de trabajo
Inexistencia de cifrado en discos duros	Bajo	Cifrado
Poca separación de funciones críticas	Bajo	Definir responsabilidades, separación de funciones
Dispositivos extraíbles sin cifrado	Bajo	Cifrado
Fallas por parte del proveedor de servicios de internet	Bajo	Enlaces redundantes , acuerdos de LSA
Daños en la configuración de los equipos por poco mantenimiento	Bajo	Mantenimiento preventivo

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Descuido en el manejo del hardware	Bajo	Capacitación del personal
Errores de cambios en la configuración de equipos activos y servidores	Bajo	Capacitación del personal
Inexistencia de control a servicios de servidores	Bajo	Políticas de hardening en servidores
Inexistencia de políticas de confidencialidad	Bajo	Políticas de confidencialidad
Inexistencia de monitoreo de las aplicaciones	Bajo	Políticas de monitoreo, implementación de herramientas de monitoreo
Poca educación sobre seguridad a usuarios finales	Bajo	Capacitación del personal
Errores humanos	Bajo	Capacitación del personal
Aprovechamiento de vulnerabilidades de controles físicos	Bajo	Implementación de controles de acceso de 2 o más factores
Falta de gestión de garantías	Bajo	Adquisición de periodos de garantía más largos
Interferencias magnéticas	Bajo	----------
Desastres naturales en la institución	Bajo	Prevención

En cuestión a los controles propuestos para la organización, se aprobó el siguiente plan de seguridad, que contempla la siguiente arquitectura de red (figura 5.4).

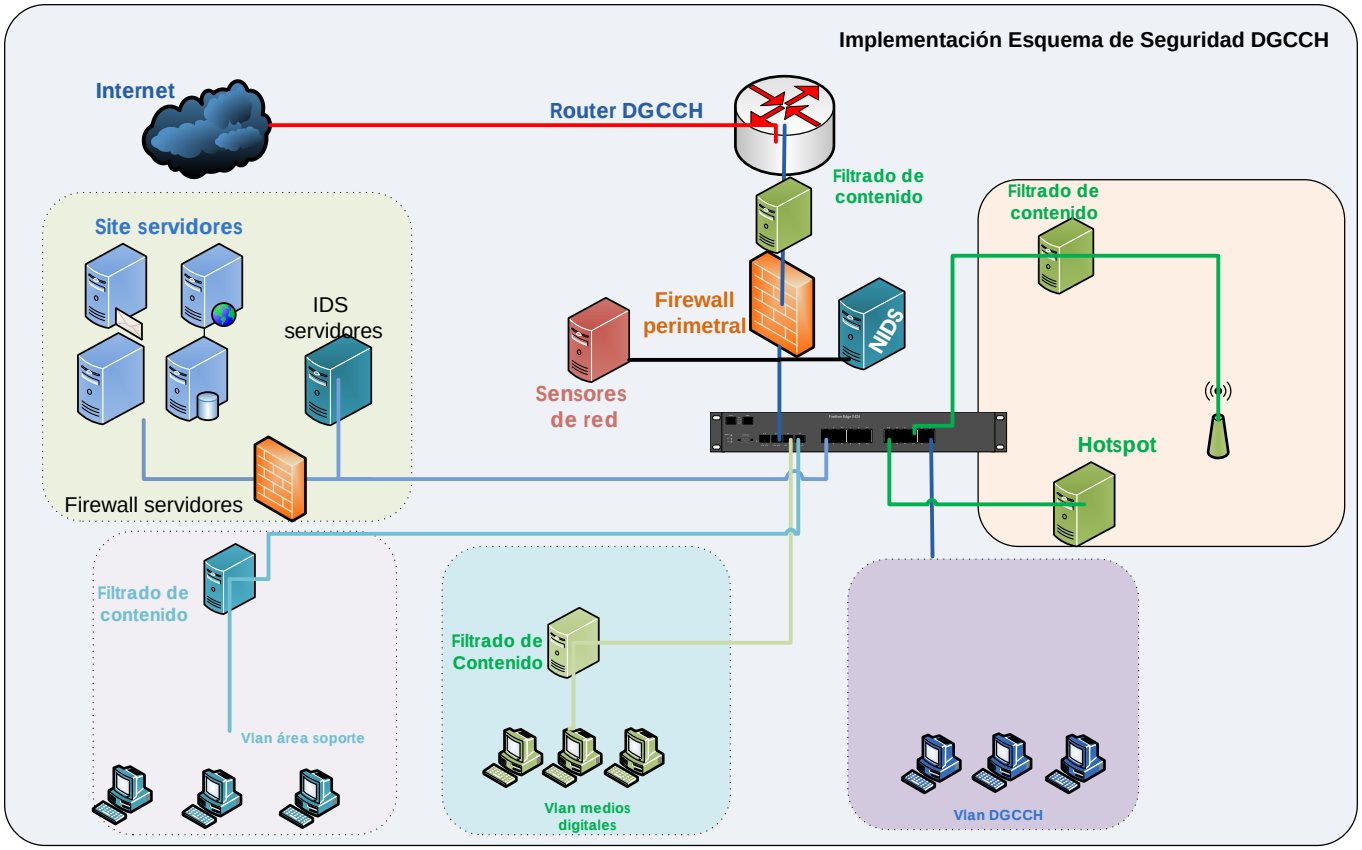


Figura 5. 4 Propuesta de esquema de seguridad para la red.

El esquema de protección planteado, consta de los siguientes mecanismos apoyado de políticas, procedimientos y documentos de respaldo que fortalecen el esquema de seguridad.

a. Esquema de seguridad perimetral

- 2 Firewall (Perimetral y Site de servidores); estableciendo reglas de filtrado apegadas sólo a los requerimientos de servicio.
    - A la fecha de entrega del proyecto, solo se ha configurado el equipo perimetral, por falta de recursos.
- 2 IDS (Perimetral y Site de servidores).
    - A la fecha de entrega del proyecto, solo se ha configurado el equipo perimetral, por falta de recursos.
- 1 Sensor de uso de la red, por tipo de tráfico, host y servicio, (Perimetrales).
- Monitoreo de enlace, por parte del proveedor de servicio "NOC UNAM".
- Zonas de seguridad por secretaría, 3 Segmentos de red por medio de NAT's, y segmento homologado.
- 1 Filtro de contenido perimetral.
- 3 Filtros de contenido independientes.
- Implementación de controles de autenticación y cifrado de los servicios de red inalámbrica.

b. Políticas

- Políticas de seguridad para la red de la organización.
- Políticas de seguridad para sistemas operativos Windows / UNIX.
- Políticas de monitoreo.
- Políticas de respaldo para servidores.

c. Procedimientos

- Establecer responsables de la seguridad lógica de la institución.
- Realización de análisis de riesgos de manera periódica.
- Aplicación para el inventario y asignación de direcciones IP.
- Definición de funciones específicas para cada puesto.
- Procedimiento de actualización de memorias técnicas.
- Procedimiento de instalación y configuración de firewall.
- Procedimientos dé instalación de IDS.
- Procedimiento de instalación de Hotspot.
- Procedimiento de configuración de equipos activos.
- Procedimiento de instalación de sensor de red.
- Procedimiento de configuración de zonas para SAN.
- Procedimiento de instalación servidores ESX.
- Políticas de cambio de contraseñas.
- Hardening en equipos activos.
- Hardening en servidores.
- Procedimiento de instalación sistemas operativos de los usuarios.
- Capacitación al personal de soporte y encargados de la red de la institución.
- Capacitación a los usuarios finales.

- Documentar los procesos y verificarlos periódicamente.

d. Seguridad Física

- Cámaras de circuito cerrado y políticas de monitoreo.
- Empleo de cerraduras físicas, biométricas o electrónicas en sites.
- Planta eléctrica redundante, para site de servidores.
- Instalación de cableado estructurado.
- Monitoreo de condiciones ambientales en sites.

e. Documentos

- Diagramas de red de la institución.
- Memorias técnicas de cableado estructurado.
- Memorias técnicas de los equipos activos (Switch, Router, A.P.).
- Memorias técnicas de servidores.
- Respaldo de la configuración de los equipos activos que lo permitan.
- Respaldo de servidores.

- **Hardware**
  - Contemplar la compra de un SAN para la realización de respaldos de servidores.
  - Configuración de NAS, para respaldos de los datos de los usuarios, cuando requieran mantenimiento los equipos.
  - Implementar un esquema de alta disponibilidad en servidores.
  - Configuración de Firewall con opción de configuración para alta disponibilidad.
  - Redundancia en mecanismos de alimentación eléctrica para site de servidores.
  - Considerar site alternos.

Existen dispositivos que ayudarían a garantizar de mejor manera la continuidad de operación de los servicios brindados, los cuales representan un gasto considerable para la organización. En cuestión de políticas, procedimientos, diagramas y guías de configuración todos contemplan la siguiente información como mínima indispensable:

- Nombre del documento.
- Persona que elaboró.
- Persona que aprobó.
- Fecha de publicación.
- Objetivo del documento.
- Alcance.
- Definiciones.
- Control de Cambios.

5.4. Desarrollo de la implementación

El esquema de seguridad que se implementó no representó un costo considerable a la institución, ya que se aprovecharon todos aquellos recursos de los cuales podrían hacer uso, dentro de éstos se lista el material utilizado para cada control, pero es importante aclarar que muchos de los controles propuestos son procedimientos, los cuales requieren documentación, personal humano y tiempo para su elaboración. El tipo de dispositivos que se propone anteriormente tiene diversidad en costos, fabricantes y prestaciones que brinda, las propuestas de seguridad que se realizaron no representaron un costo adicional hasta el momento de su implementación, pero cabe aclarar que no contempló la totalidad de mecanismos mencionados en la propuesta.

a. ***Firewall perimetral;*** Primer dispositivo contemplando en la implementación, por solicitud de la jefatura se pide contemplar la implantación de este control como una primer barrera de protección derivada de ataques externos.
    - Servidor Intel.
    - 2 interfaces de red de fibra óptica.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

b. ***IDS perimetral;*** Segundo dispositivo instalado, brinda apoyo en la detección de ataques que no pueden ser detectados por el firewall, permite establecer reglas personalizadas.
    - Servidor Dell, independiente subutilizado.
    - Máquina virtual colocada en servidor ESX-A.
    - Se configura mirror en switch core.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

c. ***Sensor de red;*** dispositivo instalado al mismo tiempo que el IDS, capaz de monitorear el comportamiento de protocolos como TCP/UDP/ICMP, y ya dentro de éstos, agruparlos por FTP,HTTP,DNS,telnet,SNMP,POP3 y por host.
    - Servidor Dell, independiente subutilizado.
    - Máquina virtual colocada en servidor ESX-A.
    - Personal encargado de la instalación y monitoreo de dichas tareas.
    - Elaboración de procedimiento de instalación.
    - Solución con software libre.

d. ***Servidores NAT;*** Segmentación de redes virtuales, en áreas que así lo permitan.
    - Configuración de NAT en equipos cisco.
    - Configuración de NAT, empleando software libre.
    - Elaboración de procedimiento de instalación.
    - Personal encargado de la instalación y monitoreo de dichas tareas.

e. ***Filtrado de contenido;*** Empleado como un control en los destinos de búsqueda, de los clientes, permitiendo elegir categorías de bloqueo como pornografía, p2p, proxy, películas, chat, drogas, redes sociales, etcétera.
    - Cuenta creada en OpenDNS para aplicar filtrado de contenido en cada uno de los segmentos de red generados, la herramienta de suscripción anual con todas sus funciones. En este caso sólo se utiliza en la versión libre.
    - Personal encargado de dichas tareas.

f. ***Hotspot***; Control de acceso y confidencialidad de la red inalámbrica.
- Servidor Dell, independiente subutilizado.
- 1 Tarjeta de red PCI express con 2 interfaces ethernet 10/100/1000.
- Configuración de Hotspot en servidor ESX-B.
- Solución con software libre.
- Personal encargado de la instalación y soporte al servicio.
- Elaboración de procedimiento de instalación.

g. Actualización del inventario de las asignaciones de IP y dominios.
- Desarrollo de sistema para el control de asignaciones IP.
  - URL: https://132.248.122.122/ips/inicio.aspx
- Documentación del desarrollo.
- Personal encargado de la supervisión en las asignaciones.

h. Elaboración de memorias técnicas.
- Contempla las memorias técnicas de todos los equipos de comunicación.
- Centralización de contraseñas empleando un gestor de contraseñas.
- Personal humano encargado de dichas tareas.

i. Elaboración de procedimientos para el área de servidores administrados por la Secretaría de Informática.
- Personal humano encargado de dichas tareas.

j. *Elaboración de respaldos*.
- Personal humano encargado de dichas tareas.
- Unidad de almacenamiento externo, NAS y SAN.

k. *Etiquetar medios de transmisión primarios*.
- Personal humano encargado de dichas tareas.

Los controles que se colocaron se complementan con aquéllos que había antes de la implementación, estos mecanismos existentes antes de la implementación son:

- Seguridad física de la red y su entorno.
- Procedimiento en la instalación de sistemas operativos para las máquinas de los usuarios.
- Procedimientos propios de seguridad de cada administrador.

Los controles garantizan un nivel de seguridad, sin embargo, deberán complementarse a través de documentos, guías de configuración, políticas, buenas prácticas que permitan una adecuada gestión de la seguridad.

5.5. Limitantes de la implementación

Cuando se trata de implementar un esquema de seguridad surgen como resultado del análisis de riesgo un sin fin número de mejoras posibles, lo ideal sería que todos los controles plateados se lograran implementar, los principales obstáculos a los que se enfrentan las instituciones al implementar un plan de seguridad eficaz son:

- Falta de presupuesto dirigido meramente a la seguridad de la institución.
- Falta de personal dedicado a la seguridad lógica de la institución.
- Tener definido claramente, las funciones de cada puesto.
- Falta de personal calificado en el área de seguridad.
- Falta de conciencia de los usuarios para utilizar los servicios de cómputo de manera adecuada.
- Cambios tecnológicos constantes.
- Costumbres y formas de trabajo en determinadas áreas.
- Conciencia de los Directivos sobre la importancia de proteger la red de la institución.

Actualmente muchas instituciones cuentan con conexión a Internet, pero pocas se han preocupado por proteger su infraestructura, información y procesos. El hecho de no contar con un área de seguridad en cómputo dentro del organigrama provoca que el administrador de red y el personal asignado al área de sistemas, además de sus tareas diarias, deba lidiar con problemas de seguridad.

En el proyecto realizado actualmente se tiene pendiente la implementación y el desarrollo de algunos controles, el motivo principal de este retraso son los recursos económicos y de personal, que afectan directamente en la adquisición de hardware faltante, el personal dedicado para esta tarea, seguido por las costumbres de trabajo en algunas áreas.

Las actividades que se planea realizar en un futuro, que repercuten en temas de seguridad son:

- Cableado estructurado para toda la institución, con un costo de $452,779.32, el cual incluye el recableado de la totalidad de la instalación en cobre categoría 6E.
- UPS de 10KW en potencia, con un costo aproximado de $97,044.81.
- Cámara de vigilancia IP, sensor de temperatura y humedad $22,096.84.
- Interfaces de red ethernet y de fibra para servidores $13,000.
- La adquisición de un equipo de almacenamiento alternativo NAS, que resguarde una copia de las máquinas virtuales en producción y brinde un soporte de crecimiento en almacenamiento.
- En el caso del IDS por ser una solución de software libre sin licencia se tiene un retardo en las actualizaciones de las firmas de ataque, aproximado a un mes. En caso de que se deseen tener las reglas de filtrado completamente actualizadas se debe pagar una licencia de $30 US anual para un sensor, de 1-5 sensores $499/número de sensores y de más de 6 sensores $399/número de sensores.
- Capacitación.

En la tabla 5.10 se citan todos aquellos riesgos residuales que no fueron atendidos por los recursos relacionados a los mismos, pero que se planean llevar a cabo en un futuro cercano.

Tabla 5. 10 Riesgos residuales.

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Falta de cuidado del equipo de cómputo	Alto	Concientización en temas de seguridad
Confianza en otras personas	Alto	Concientización en temas de seguridad
Fallas por parte del proveedor del suministro eléctrico	Alto	Acuerdos de niveles de servicio
Tableros eléctricos expuestos	Medio	Informar de la vulnerabilidad detectada a la Secretaría Administrativa
Controles de acceso inseguros para administración de servidores	Medio	Implementar controles biométricos en los Sites
Fuga de información	Medio	Políticas de confidencialidad
Daño físico a la infraestructura de red	Medio	Cableado estructurado
Inexistencia de controles de seguridad en portátiles	Medio	RFID, bandas magnéticas y cintas de seguridad
Control de acceso débil en aplicaciones	Medio	Políticas desarrollo de software seguro
Falta de corriente eléctrica regulada	Medio	Implementar reguladores en la mayoría de los equipos
Inexistencia de fuente de corriente eléctrica alterna	Medio	Planta eléctrica
Inexistencia de planes de capacitación	Medio	Capacitación del personal
Inexistencia de sites alternos	Medio	Contratos con compañías, acuerdos con otras instituciones
Cableado de red expuesto	Medio	Cableado estructurado
Uso de protocolos de comunicación inseguros	Medio	Implementación de comunicaciones cifradas
Tuberías expuestas	Medio	Restructuración de instalación eléctrica, mantenimiento
Empleo de software sin actualizaciones	Medio	Actualizaciones
Inexistencia de auditorias	Bajo	Planificación de auditorias
Limitantes de espacio en disco duro en servidores	Bajo	Evaluación y Adquisición de medios de almacenamiento masivo
Inexistencia de cultura de seguridad en usuarios finales	Bajo	Capacitación del personal
Inexistencia de cifrado en discos duros	Bajo	Cifrado
Poca separación de funciones criticas	Bajo	Definir responsabilidades, Separación de funciones
USB sin cifrado	Bajo	Cifrado
Fallas por parte del proveedor de servicios de internet	Bajo	Enlaces redundantes , acuerdos de LSA
Descuido en el manejo del hardware	Bajo	Capacitación del personal
Errores de cambios en la configuración de equipos activos y servidores	Bajo	Capacitación del personal
Inexistencia de políticas de confidencialidad	Bajo	Políticas de confidencialidad
Poca educación sobre temas de seguridad a usuarios finales	Bajo	Capacitación del personal

Vulnerabilidad	Nivel de atención de riesgo	Control sugerido
Errores humanos	Bajo	Capacitación del personal
Aprovechamiento de vulnerabilidades de controles físicos	Bajo	Implementación de controles de acceso de 2 o más factores
Falta de gestión de garantías	Bajo	Adquisición de periodos de garantía más largos
Interferencias magnéticas	Bajo	----------
Desastres naturales en la institución	Bajo	Prevención

5.6. Posibilidades de crecimiento

Cuando se implementa un esquema de seguridad que va ligado con un análisis de riesgo, muestra claramente aquellos riesgos residuales que se generan con la implementación de los controles seleccionados, lo que permite contemplar mejoras a mediano y largo plazo. Dentro de las posibilidades de crecimiento que se contemplan para llevar a cabo, se sugiere:

De manera inicial se recomienda contemplar los puntos mencionados en las limitantes de la implementación, como mejoras inmediatas, ya que algunas de ellas su nivel de riesgo es elevado, pero por cuestiones de recursos económicos no fue posible su implementación.

1. Elaboración de análisis de riesgo de manera periódica, basándose en estudios realizados anteriormente, generando un histórico de esquemas de seguridad, que permita observar los puntos de mejora y críticos a la fecha.
2. Revisión y actualización de las políticas de seguridad.
3. Asignar a una persona como responsable de la seguridad de la institución.
4. Aumento de la seguridad física en los sites, implementado controles de acceso de 2 factores.
5. Realizar separación de funciones en todas las actividades críticas de la institución.
6. Establecer un help desk para la atención de incidentes, dentro de la institución.
7. Desarrollar procedimientos de manejo de incidentes, entre ellos de contención de código malicioso.
8. Implementación de plantas de energía eléctricas alternativas y UPS en los sites.
9. Realizar una instalación de cableado estructurado.
10. Segmentación de la red en la totalidad de sus secretarías.
11. Elaboración de un sistema de gestión y respuesta de incidentes de seguridad.
12. Capacitación continúa en cuestiones de seguridad al personal de la institución.
13. Guía de respaldo para base de datos.
14. Actualización de los equipos de telecomunicaciones a equipos administrables.
15. Aplicar un plan de gestión de la seguridad PDCA (Plan - Do - Check - Act).
16. Dar a conocer las políticas de uso de equipos, red y seguridad en red de la institución.
17. Normativa para la publicación de sitios web.
18. Realizar auditorías periódicamente con la finalidad de detectar nuevas vulnerabilidades.

19. Legalizar el uso de software que se tiene de manera ilegal.
20. Revisión de Acuerdos de Niveles de Servicio (LSA) con proveedores de servicio de red y suministro eléctrico.
21. Realizar informes detallados, para sustentar las decisiones derivadas de las iniciativas de seguridad.
22. Migración de todos los servidores a los Sites donde se cuenta con condiciones adecuadas para su funcionamiento y resguardo.
23. Implementar esquema de seguridad para los planteles que integran el Colegio de Ciencias y Humanidades.
    - Aprobación de las políticas de red propuestas desde esta entidad central hacia los planteles que la conforman.
    - Separación de funciones, determinando roles específicos para cada persona.
    - Cifrado de información en equipos portátiles con base en su grado de importancia.
    - Elaboración de planes de contingencia.
    - Capacitación a los encargados de sistemas, en temas relacionados a la seguridad de sistemas operativos Windows y Linux.
    - Capacitar al usuario final en cuestiones de seguridad básicos, ya que él forma el eslabón más débil en la cadena que conforma la seguridad de la información.
24. Gestión, monitoreo y elaboración de estadísticas del uso de la red.

Conclusiones

Haber implementado el esquema de seguridad dentro del Colegio de Ciencias y Humanidades, representó una experiencia enriquecedora en nuestro desarrollo profesional, después de haber realizado un análisis de las necesidades del Colegio en cuanto a seguridad de la información. El enfoque de protección que se plantea, con base en los objetivos, se centra en el diseño e implementación de un esquema de seguridad perimetral, punto que fue cubierto. Es importante destacar que gracias a este trabajo fue posible implementar el primer esquema de seguridad de red perimetral para la institución, esperando que las perspectivas de seguridad plasmadas en este documento presente al lector la importancia de la seguridad de la información, procedimientos, buenas prácticas y mecanismos que permitan llevar a cabo un ciclo de mejora continua.

El trabajo realizado en conclusión cumplió con los objetivos propuestos, considerando riesgos residuales aceptados por la dirección, a los cuales en un futuro se recomienda dar su adecuado tratamiento, mencionados en el tema 4.1. Dentro de los beneficios generados con este trabajo, considerando etapas de análisis, desarrollo del esquema e implementación, se listan las siguientes aportaciones:

- Un primer análisis de riesgos con base en el NIST 800-30, a través de los cuales se determinaron activos, amenazas, riesgos, así como controles para reducir la posibilidad de presentarse un incidente de seguridad, permite ser un punto inicial para futuros análisis de riesgos.
- Seguimiento de incidentes, para futuros análisis de riesgos.
- Listado centralizado de los servicios y administradores de la institución.
- Políticas de uso de red para la institución, que respaldan y apoyan los controles implementados, con un diseño que permite su fácil actualización y control de cambios.
- Documentación completa de la topología de la red.
- Memorias Técnicas de los equipos de telecomunicaciones.
- Respaldos de la configuración actual de los equipos de telecomunicaciones.
- Procedimientos de respaldos de los equipos de telecomunicaciones.
- Configuración de manera segura en los equipos de telecomunicaciones.
- Procedimientos de configuración de servidores, servicios y equipos activos.
- Acceso sólo a servicios necesarios para administradores y usuarios, cuando se intenta acceder a los recursos del segmento, por medio del firewall implementado y hardening en servidores.
- Bitácoras de acceso no autorizado en el perímetro de red.
- Análisis de tráfico en tiempo real.
- Permitir a los usuarios internos sólo acceso a servicios válidos, limitando la posibilidad de que un ataque se lleve desde la organización.
- Reducir el ancho de banda generado por malware desde el interior de la organización, intencional o no, que pueda afectar a otras redes.

- Bitácoras del tráfico que pasa por el perímetro de red.
- Contemplando los puertos válidos por el firewall, apoya la tarea de monitoreo un IDS sobre los servicios permitidos hacia la institución y sus ataques conocidos a éstos, permitiendo tomar medidas sobre dichos comportamiento.
- Creación de reglas específicas que permitan detectar algún tipo de tráfico en particular.
- Gráficas de ancho de banda utilizado por protocolo.
- Gráficas de ancho de banda utilizado por servicio.
- Gráficas de ancho de banda utilizado por host.
- Gráficas de uso de ancho de banda, por parte del proveedor de servicios DGTIC y su mesa de ayuda "www.noc.unam.mx".
- Contribuir a evitar el uso indebido de ancho de banda por medio de gestores de contenido.
- Adecuar el contenido no deseado de internet de acuerdo con las políticas de uso válido.
- Reducir riesgos legales por la descarga y compartir software.
- Informes de los 100 sitios más solicitados donde se emplee filtrado de contenido.
- Informes de los 100 sitios menos solicitados donde se emplee filtrado de contenido.
- Políticas de filtrado web que permitan emplear los recursos de una manera productiva y positiva.
- Reportes de uso de la red inalámbrica.
- Monitoreo de uso de la red inalámbrica por día, cuenta de usuario o MAC address.
- Capacidad para la elaboración de manera periódica de informes.
- Soporte en hardware y respaldo eléctrico para nuevos servicios.
- Aumento en la capacidad de almacenamiento de respaldos.

Para garantizar la seguridad de la información dentro de la institución, no sólo se requiere de la implementación de los diferentes mecanismos de control, ya que no serán suficientes si no se cuenta con el personal adecuado que garantice su operación. Como responsables de seguridad siempre debemos considerar la capacitación constante, que nos permita responder a futuros incidentes.

Cuando se busca establecer un esquema de seguridad, uno de los principales problemas es la forma de trabajo y el desinterés por temas relacionados con la seguridad, para la mayoría de los usuarios, los temas de seguridad de la información representan limitantes para el desarrollo de sus actividades o incluso molestias. Remarcar la importancia de la seguridad de la información para usuarios finales es una de las tareas que la Secretaría de Informática tiene que reforzar, para transmitir la importancia que tiene la seguridad apoyada con las políticas establecidas que permita ver a la seguridad, no como una limitante que dificulte su trabajo, sino como procedimientos y mecanismos de apoyo, que auxilien el correcto desempeño de sus actividades.

En general, el proyecto se logró concluir de manera satisfactoria, se utilizaron los recursos existentes, la mayoría de los controles implementados no representaron costos significativos, lo que implicó un ahorro para la institución.

No podemos decir que los controles, procedimientos, políticas y recursos humanos empleados, garantizan el 100% de la seguridad de la institución, ya que como nos dimos cuenta, existen riesgos residuales, que por las características propias de cada institución no son atendidos de manera inmediata. El trabajo desarrollado permite llevar a la institución a un proceso de mejora continua, que ayude a responder de mejor manera ante un incidente.

A la fecha los planteles que integran el Colegio de Ciencias y Humanidades no cuentan con un esquema de seguridad, por lo que se encuentran expuestos en su totalidad, una meta a corto plazo es unir esfuerzos para lograr la implementación en los diferentes planteles, para que con ello se pueda llegar a desarrollar un esquema de seguridad de acuerdo con sus necesidades, razón por la cual se torna importante invertir en capacitación, tecnología y los recursos humanos necesarios.

Apéndice A
Clasificación de atacantes

En general los ataques son producidos por diversas entidades físicas y lógicas, dentro de las físicas se encuentran las personas que buscan realizar algún daño, a éstas se les conoce como atacantes o perpetradores en términos generales, de manera particular se realiza una clasificación con base en el nivel de conocimiento de la persona y su finalidad, recibiendo así nombres diversos.

Los hackers pueden ser divididos en 3 grupos: White hats –sobrero blanco, Black hats - sombrero negro y Gray hats- sombrero gris, *los Ethical hackers –Hackers éticos, por lo regular caen en la clasificación de White hats pero algunas veces ellos también forman parte de los gray hats, los cuales son profesionales en seguridad y utilizan sus habilidades de una manera ética, en ocasiones también son auditores en pruebas de penetración.* [43]

Los ***White hats*** son los chicos buenos, los hackers éticos quienes utilizan su habilidades de hackeo para propósitos de defensa, usualmente son profesionales de seguridad con conocimiento de hackeo y herramientas, quienes utilizan su conocimiento para localizar vulnerabilidades e implementar contramedidas.

Black hats, son los chicos malos, los hacker maliciosos o crackers quienes usan sus habilidades para propósitos maliciosos o ilegales, violar la integridad de los sistemas, obtener acceso no autorizado a máquinas remotas, destruir datos vitales, denegar servicio a usuarios legítimos y básicamente causar problemas para sus objetivos.

Gray hats, muchos de los profesionales de seguridad son capaces de realizar ataques, pero su comportamiento se declina por la moral, son hackers los cuales pueden actuar de manera defensiva u ofensiva, dependiendo de la situación, esta es la delgada línea entre el hacker y el cracker.

Adicional a este grupo de personas existen otros grupos como lo son los lammers (personas con poco conocimiento informático que normalmente utilizan herramientas fáciles de usar para atacar ordenadores), script kiddies (cracker inexperto que usa programas, scripts, exploits, troyanos, creados por terceros para romper la seguridad de un sistema, suele presumir de hacker o cracker cuando en realidad no posee un grado relevante de conocimientos), phreakers (son los crackers de líneas telefónicas, ya sea para dañarlos o hacer llamadas gratuitas), Insiders (son los crackers corporativos, empleados de la empresa que atacan desde adentro, movidos usualmente por la venganza), espías corporativos(son muy raros porque son extremadamente costosos y legalmente riesgoso, se emplean estos medios contra compañías competencia).

43 *Kimberly Graves, CEH™Official Certified Ethical Hakers, Sibex.(33-34)*

Apéndice B

Ataques lógicos

1. Password cracking

Entre más débil sea dicha contraseña el obtenerla será mucho más sencillo, se considera una contraseña débil el uso de fechas de cumpleaños, nombres de mascotas, palabras relacionadas con los gustos personales y preferencias, apellidos principalmente, un parámetro que también influye en la debilidad de una contraseña es la longitud de la misma.

Por ejemplo, un ataque basado en fuerza bruta, al tener una contraseña de una longitud de cuatro caracteres ocasiona que las opciones para ser adivinada sean mucho más rápidas, ya que se cuenta con menos combinaciones.

Se sabe que el código ASCII emplea 128 caracteres imprimibles y si se utiliza una contraseña de 4 caracteres el espacio muestral se reduce a 128^4 combinaciones, por lo que si la contraseña es de una longitud mayor, esto permite aumentar el espacio muestral considerablemente y por lo tanto hacerle la tarea más difícil al tratar de encontrar la clave.

El avance computacional que se tiene día con día hace posible que los ataques se vuelvan cada vez más sofisticados y rápidos, esto debido a que el procesamiento en cuanto a cómputo se refiere es mucho más potente cada vez.

Actualmente existen supercomputadoras que pueden realizar hasta mil billones de operaciones por segundo, para conocer qué tan rápida es una computadora se utiliza con frecuencia una medida que indica cuántas operaciones aritméticas en punto flotante puede realizar en un segundo. Esta medida se llama FLOPS (Floating Point Operation Per Second –Operaciones de punto flotante por segundo). Por ejemplo, una supercomputadora típica de los 70's, la CRAY-1, realizaba 250 MFLOPS (250 Millones de operaciones en punto flotante en un segundo).

Un procesador Pentium 4 o Athlon 64, típicamente opera a más de 3 GHz y tiene un desempeño computacional del rango de unos cuantos GFLOPS, lo que equivale a 1000, 000,000 de operaciones por segundo, por lo que el tiempo para romper una contraseña que utiliza el código ASCII y si sólo se utilizaran 4 caracteres sería muy poco.

Sin embargo, el hecho de incrementar la longitud de la contraseña no garantiza nada, lo más conveniente es contar con una contraseña lo más robusta posible utilizando una combinación de letras mayúsculas, minúsculas, números, caracteres especiales y con una longitud mínima de 8 caracteres, así como cambiar periódicamente las contraseñas es otra buena medida para evitar este tipo de ataque.

Algunas herramientas utilizadas para encontrar la contraseña por medio de la fuerza bruta son las siguientes:

a) L0pht Crack

Conocida actualmente como LC5 permite recuperar contraseñas del sistema operativo Windows, también puede ser utilizada para verificar la robustez de una contraseña, una herramienta de apoyo a auditorías, se basa en ataques por fuerza bruta, diccionario.

b) John the Ripper

Permite obtener contraseñas, basado en un ataque de diccionario, disponible para Linux, Windows, MacOS. Es capaz de trabajar con algoritmos de cifrado como DES, SHA1, MD5, Blowfish, Kerberos, hash LM (Windows).

2. Malware

El software malicioso o malware se clasifica en distintas categorías de acuerdo con la forma de operar y de propagarse (figura B.1).

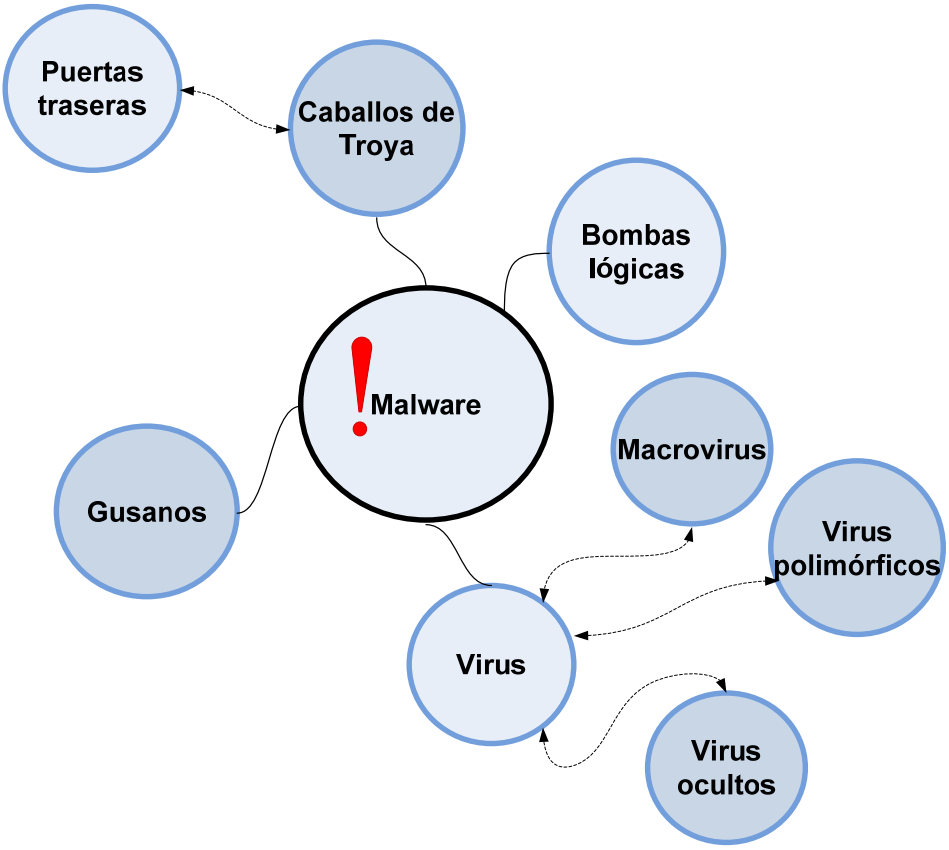


Figura B. 1 Clasificación software malicioso.

Se clasifican en:

- Virus.
- Gusanos.
- Caballos de Troya.

- Spyware.
- Bombas lógicas.
- Back Doors (puertas traseras generadas en los sistemas para ingresar a ellos).
- Spam (Correo no deseado con información publicitaria).
- Dialers (Programas que llaman a números telefónicos de larga distancia o tarifas especiales por medio de un módem).
- Pharming (Modificación de los valores DNS).
- Phishing (Ingeniaría social empleando sitios duplicados y correos electrónicos).
- Rootkit (Programas insertados en un equipo después de tomar el control de éste).
- Adware (Software que muestra o baja anuncios publicitarios).
- Bots (Programa robot que se encarga de realizar funciones rutinarias).
- Exploit (software que explota debilidades de programación).

a) Virus

Es un tipo de código malicioso que necesita ser trasportado por algún otro programa, y se propaga cuando el programa es ejecutado. Los virus se pueden transmitir de varias formas, por ejemplo, pueden formar parte de un archivo que se obtiene de la red o simplemente formar parte de un correo electrónico.

Algunos ejemplos de estos virus son:

- ***Macro virus*:** Cuando una aplicación es abierta los virus ejecutan instrucciones antes de transferir el control de la aplicación, estos virus se replican y se adhieren a otros códigos en el sistema de la computadora.
- ***File infectors:*** Software malicioso que infecta archivos, éstos virus se pueden ejecutar como una de las siguientes extensiones *.com* o *.exe*, se instalan cuando el código es leído, existe otra versión de este tipo de virus los cuales se crean archivos con el mismo nombre pero con extensión *.exe* cuando el archivo es abierto se ejecuta.
- ***Boot infectors:*** Ejecutables que infectan el sistema de arranque de un disco duro o discos, cuando un virus se encuentra alojado en el sector de arranque de un equipo en el momento que el equipo intente cargar el sistema operativo se ejecuta el virus cargándose en memoria obteniendo el control de algunas funciones básicas, además puede propagarse hacia otras computadoras o dispositivo de almacenamiento.

- ***Stealth virus:*** virus ocultos, que actúan sobre funciones del sistema ocultándose ellos mismos además de que comprometen al antivirus, cuando el antivirus genera un reporte de su existencia y éste procede a desinfectar, se ocultan, generalmente aumenta el tamaño del archivo ,fecha de última modificación o fecha de creación.

- ***Virus Polifórmico:*** también conocido como un virus mutante, cambia su firma cada vez que se replica e infecta un nuevo archivo, esto lo hace más difícil de detectar por un antivirus. Esto se debe a que sus firmas digitales no son las mismas cada vez que ejecuta crea una copia de sí mismo. Una de sus técnicas suele ser el auto-cifrado.

Existen programas de hacking para la creación de virus polimórficos como el Mutation Engine, totalmente gratuito y que permite generar virus polimórficos.

En general se puede encontrar una gran cantidad de virus y desde luego cada vez más sofisticados.

b) Gusanos

Los gusanos son un tipo especial de código malicioso ya que se propaga de manera distinta a un virus, a diferencia de éste, no necesita de un portador como un archivo, un gusano contiene procedimientos que le permiten propagarse por distintos equipos a través de la red, generalmente se propagan a través de correos adjuntos, cuando son abiertos se activan y envían una copia de sí mismo a las lista de contactos. El gran peligro de los gusanos es su habilidad para replicarse en grandes números como resultado su propagación por toda la red puede ocasionar una denegación de servicios.

c) Caballos de Troya

Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que en realidad ponen en peligro la seguridad de un equipo de cómputo**,** estos programas realizan la actividad que el usuario requiere pero al mismo tiempo ejecuta otros procesos que ponen en riesgo al equipo. Los intrusos los usan para ocultar su actividad, capturar información de nombres de usuario y contraseñas y crear puntos de acceso para un futuro ingreso o también conocidas como puertas traseras.

d) Spyware

El software espía se aloja en un equipo con la finalidad de recopilar, enviar información y actividad que se realiza en el equipo, como lo es el software que se utiliza, páginas que visita, historial de teclas oprimidas y manejo del mouse principalmente, la función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

e) Bombas lógicas

Es otro tipo de código malicioso diseñado para ejecutarse bajo una condición lógica a una hora determinada, y en un día específico.

3. IP Spoofing

Ataque en el que se suplanta la dirección IP de un equipo, existen otros tipos de suplantación como lo son:

a) ***DNS Spoofing-*** Suplantación de identidad por nombre de dominio.

b) ***ARP Spoofing*** **-** Suplantación de identidad por falsificación de tabla ARP.

c) ***Web Spoofing*** **-** Suplantación de una página web real.

IP spoofing es un problema sin solución fácil ya que la debilidad que explota es inherente al diseño del protocolo TCP/IP, entendiendo cómo y qué ataques de suplantación son utilizados combinados con métodos simples de prevención, se puede ayudar a prevenir ataques contra la red.

4. Fingerprinting

El ataque de Fingerprinting está relacionado con los escaneos, se clasifica en dos, fingerprinting pasivo y fingerprinting activo.

a) Fingerprinting activo

Sucede generalmente cuando el atacante realiza alguna acción con la finalidad de obtener alguna respuesta de la víctima a través del envío de paquetes que le permiten obtener información, Algunas herramientas utilizadas son: RINGv2, Xprobe2, Nmap.

b) Fingerprinting pasivo

En este caso los paquetes a analizar se obtienen directamente de la red local, por lo que el atacante no genera ningún tipo de comunicación hacia el destino con el fin de provocar una respuesta, el atacante pasa inadvertido generalmente por medio de sniffers – analizadores de tráfico, por lo que el atacante necesita colocar su tarjeta de red en modo promiscuo y analizar totalmente el tráfico de la red, por ejemplo la herramienta *Nmap* con la *opción –O* muestra puertos abiertos y el tipo del sistema operativo que se está utilizando.

5. DoS

Una variante de este tipo de ataques es el ataque de denegación de servicios distribuido DDoS, (Distributed denial-of-service attacks –Denegación de Servicios Distribuido), es aquél donde un conjunto de sistemas previamente comprometidos realiza un ataque de denegación de servicios sincronizado a un mismo objetivo, al unir los recursos de todos los sistemas comprometidos saturan al equipo que se desea comprometer.

Este tipo de ataques está relacionado con los zombies o bots, que son equipos que pueden ser controlados de una manera centralizada para cualquier uso, los DDoS constan de 3 partes.

- Master – Maestro.
- Slave/secundary victim/agent/bot/botnet – Esclavo/víctima secundaria/agente/robot/robot.
- Victim/ primary victim – Víctima / víctima principal.

El *maestro* es quien ejecuta el ataque, el *esclavo* quien recibe órdenes del maestro y la *víctima* que es el sistema a comprometer.

Existe una clasificación de este tipo de ataques entre los que se encuentran:

- Buffer overflow (Saturación de la memoria RAM).
- SYN Attack, SYN flooding (Saturación por medio de solicitud de conexiones TCP).
- Smurf (Envío de muchos paquetes ICMP (ping) broadcast).

Algunas herramientas utilizadas para provocar DoS son Ping de la muerte, SSPing, CPU Hog, WinNuke, Jolt2, Bubonic, en el caso de DDoS se tienen Trinoo, Shaft, Tribal Flood Network (TFN), Stacheldraht y Mstream.

Algunas de las contramedidas utilizadas para prevenir, detectar o parar DoS, DDoS son las siguientes:

- Establecer cuotas de almacenamiento, memoria y uso de procesador en los equipos.
- Filtrar los servicios que ingresan a la red que pare o baje el flujo de paquetes que ingresan a la red con direcciones falsas o suplantadas desde Internet.
- Limitar la tasa de transferencia en la red.
- Sistemas detectores de intrusos (IDS).
- Herramientas de auditoría de host y red, las cuales buscan e intentan detectar herramientas conocidas de DDoS corriendo en el host o en la red, como *Find-ddos y Zombie zapper*.
- Herramientas de seguimiento de paquetes que se envían en la red con direcciones suplantadas.

Los ataques causados por DoS o DDoS son los más difíciles de proteger ya que en ocasiones muchos de éstos tienen que ver de manera inicial con seguridad lógica y física, la infraestructura con la que cuenta la organización y sus limitantes, proveedores que brindan algún servicio los cuales también pueden comprometerse.

6. Envenenamiento ARP

Empleado como base para ataques de hombre en el medio, algunas herramientas utilizadas para llevar este tipo de ataques son:

- Cain&Abel.
- Dsniff, arp-sk.
- Arp-tool arpoison. Ettercap.

8. Phishing[44]

Al igual que en el mundo físico, los estafadores continúan desarrollando nuevas y más siniestras formas de engañar a través de Internet. Si se siguen estos cinco sencillos pasos podrá protegerse y preservar la privacidad de la información.

- Nunca responder a solicitudes de información personal a través del correo electrónico. Si se tiene alguna duda, ponerse en contacto con la entidad que supuestamente ha enviado el mensaje.
- Para visitar sitios Web, introducir la dirección URL en la barra de direcciones.
- Asegurarse de que el sitio Web utiliza cifrado (figura B.2).
- Consultar frecuentemente los saldos bancarios y de las tarjetas de crédito.
- Comunicar los posibles delitos relacionados con la información personal a las autoridades competentes.
- Buscar que las instituciones que brindan algún servicio manejen autenticación de 2 factores como contraseña y OTP (One Time Password –Contraseña de una sola vez).
- Si se posee un poco de conocimiento técnico se recomienda verificar el archivo host, el cual contiene información de los DNS con la finalidad de verificar la integridad.

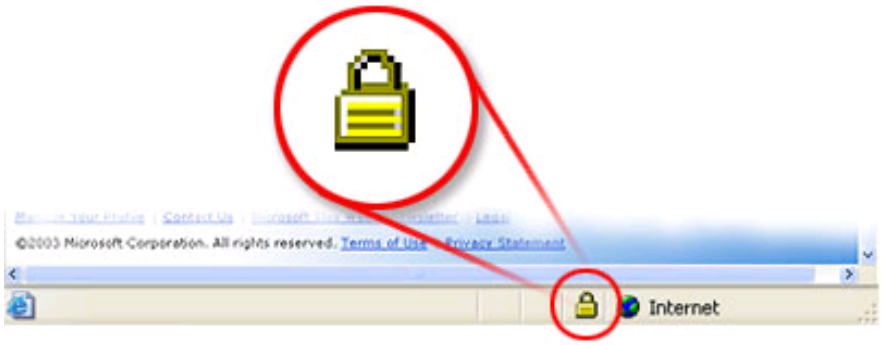


Figura B. 2 Símbolo de cifrado en sitios Web, protección contra phishing.

Actualmente se han tomado medidas para evitar este tipo de problemática, principalmente instituciones en las que su principal activo es proteger el interés de sus clientes como lo son los

[44] http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx

bancos. Por ejemplo, un método utilizado para entrar a las páginas Web de los diferentes bancos de algunos países, es usando el generador de claves dinámicas de las compañías Secure Computing y el RSA SecureID, con lo que se espera disminuir el phishing.

9. Botnet

Un bot – robot/esclavo/agente es un tipo de software automatizado diseñado para actuar en red, por sí solo es un programa capaz de auto replicarse y comportarse de manera inteligente, los cuales son utilizados para enviar correos no deseados (Spam), DDoS, además también pueden ser utilizados como herramientas para realizar ataques de manera remota, algunos de estos tipos de bots se comunican con otros usuarios a través de Internet haciendo uso de mensajería instantánea (IRC-Comunicación en tiempo real basada en texto) o cualquier otro tipo de interfaz basada en web.

Una botnet es un conjunto de equipos comprometidos y controlados por un equipo maestro que actúan en conjunto para lograr su objetivo, se vuelven una herramienta muy peligrosa, son utilizadas para generar correos no deseados y cualquier tipo de fraude, logrando con ello ataques de denegación distribuida.

Una manera de evitar este tipo de ataque es tener habilitado sólo lo necesario en un equipo, es decir, cancelar servicios que no son esenciales, los administradores de la red pueden hacerlo utilizando programas de monitoreo de red para poder detectar alguna anomalía como aumento en el tráfico de red, intermitencia entre otras.

Otra forma de evitar en mayor medida este tipo de ataques es a través de la educación de los usuarios, proporcionando información acerca de este tipo de ataques.

12. SQL injection

Cuando un intruso desea realizar ataques de este tipo, previamente como en cualquier otro ataque, se determina cuál es la configuración y las relaciones de las tablas, vulnerabilidades de las variables, etcétera, los pasos que comúnmente se siguen para determinar las vulnerabilidades del servidor SQL son los siguientes:

- Con ayuda de cualquier navegador se ubican sitios en los que es necesario autenticarse para determinar las posibles vulnerabilidades.
- Utilizar diferentes niveles de usuario y controles de acceso.
- Hacer uso de los comandos *Grant* (dar privilegio a cierta instrucción), *Revoke* (quitar permisos a ciertos recursos).
- Se realizan pruebas para determinar si existe la posibilidad de generar un error a través de consultas y con ello obtener algún dato que pudiera ser de utilidad.
- Se pueden intentar inserciones con el uso del comando *insert* o intentar listar los contenidos de las tablas de la base.

Algunas de las recomendaciones para evitar este tipo de ataques es administrar de manera adecuada la base de datos, por ejemplo, restringir privilegios en la conexión a las bases, utilizar contraseñas robustas, limitar la información que da por *default* el servidor de la base de datos, además de una revisión de los códigos de programación que no permita elaborar consultas.

Actualmente el comercio electrónico es de gran importancia para muchas empresas por lo que el diseño de sitios que eviten este tipo de ataques es primordial, además de otras medidas como el tipo de sistema operativo a utilizar, tecnología, tipo de servidor WEB, ubicación física etcétera.

13. Backdoors

Detectar puertas traseras no es una tarea fácil, pero no imposible, una forma para detectar si algún equipo tiene una puerta trasera generalmente es la adición de un nuevo servicio en los sistemas operativos Windows pues éste podría estar ocultando alguna puerta trasera.

Antes de que un intruso deje una puerta trasera realiza un proceso de análisis como servicios utilizados, puertos abiertos, aplicaciones que nunca se utilizan, pero que están activadas, todo ello con la finalidad de poder hacer uso de ellas y pasar desapercibido, por lo que se vuelve importante contar con una bitácora de servicios instalados, puertos abiertos y eliminar servicios innecesarios para evitar este tipo de ataques.

A pesar de que es una técnica sencilla es muy eficiente ya que el atacante puede ingresar al sistema con privilegios que le permitan obtener o hacerse de una cuenta del sistema para obtener beneficios.

Los RATs(Remote Administration Trojans – Troyanos administrables remotamente), son un ejemplo claro de puertas traseras, son utilizadas para tener el control de un equipo comprometido de manera remota. Cuando un usuario hace uso de su equipo, aparentemente funciona de manera normal pero al mismo tiempo se ejecutan procesos que abren puertos en el equipo víctima lo que permite al atacante estar en contacto con ella.

Este tipo de puertas traseras se compone de dos archivos, uno que se ejecuta del lado del equipo víctima que funciona como servidor y el otro del lado atacante que funciona como cliente, el cual permite al intruso tener el control.

14. Rootkits

Una clasificación muy generalizada es la siguiente:

a) Kits binarios: alcanzan su meta sustituyendo ciertos archivos del sistema por los troyanizados.

b) Kits del núcleo: utilizan los componentes del núcleo (también llamados módulos) que son reemplazados por troyanos.

c) Kits de librerías: emplean librerías del sistema para contener troyanos.

Entre las medidas que se deben tomar para evitar algún tipo de daño, primeramente si ya no se tiene la seguridad de que el equipo no está comprometido, lo recomendable es realizar un respaldo de la información importante y reinstalar los sistemas, por otro lado, si se cuenta con un respaldo del sistema no se recomienda hacer uso de él si no se está completamente seguro de la fecha en que el equipo fue comprometido.

Otra manera es verificando la integridad de los archivos a través de firmas digitales como MD5, además de utilizar aplicaciones que cifren las comunicaciones como SSH, SSL para evadir los ataque por análisis de trafico de red.

15. Footprinting

Obtener información implica todo un proceso por lo que se deben seguir cierto número de pasos lógicos, footprinting es una parte esencial de dicho proceso, catalogado como un proceso esencial. Generalmente la parte de recolección de información utiliza un 90 % del total de tiempo invertido en un ataque.

Existen distintas formas para obtener dicha información, entre ellas se encuentran:

Whois, Nslookup, Sam spade, traceroute, páginas web de la organización que brinde información de los empleados, estas herramientas permiten obtener información acerca de la red, el servidor de dominio, nombre del equipo e información que en algún momento pudiera llegar a ser de utilidad.

16. Escaneos

Los escaneos se pueden clasificar de la siguiente manera de acuerdo con el tipo de información que éstos devuelven.

a) Escaneo de puertos

Se obtiene información acerca de los puertos abiertos y los servicios, durante este proceso se permiten identificar los puertos TCP/IP disponibles, las herramientas utilizadas para el escaneo de puertos como NMAP permite conocer los puertos abiertos y el tipo de servicios asociados a ellos, como por ejemplo los puertos bien conocidos: 80 utilizado por los servidores WEB, SSH (22), FTP (21), TELNET (23), HTTPS (443), herramientas como HPING permiten realizar escaneo, alteración de paquetes e incluso se pude indicar un rango de puertos a escanear.

b) Escaneo de la Red

Permite obtener direcciones IP de una red de los equipos activos, los hosts son identificados individualmente por su dirección IP, los escáneres de redes permiten identificar los equipos que se encuentran activos.

c) Escaneo de vulnerabilidades

Permite obtener información acerca de algunas debilidades conocidas, cuando se realiza un escaneo de este tipo lo primero que se identifica es el tipo de sistema operativo, versión, así como actualizaciones para identificar las debilidades que en un futuro pueden ser explotadas por el intruso, haciendo uso de exploits adecuados para el tipo de debilidad encontrado.

El escaneo de la red y de vulnerabilidades puede ser detectado a través de la implementación de un IDS ya que las herramientas que se utilizan interactúan con la tarjeta de red generando de esta forma tráfico que puede ser detectado con la implementación de un mecanismo de seguridad adecuado.

El escaneo implica una metodología a seguir según Certified Ethical Hacker, incluye los siguientes pasos.

1. Verificar sistemas activos.
2. Verificar puertos abiertos.
3. Identificar servicios.
4. Determinar el sistema operativo utilizado.
5. Escanear vulnerabilidades.
6. Realizar diagrama de red y las vulnerabilidades de los equipos.
7. Preparar proxies (medio por el cual se planea ingresar al objetivo).
8. Atacar.

La aplicación por excelencia para realizar exploración de puertos es *Nmap* (*Network Mapper*), esta herramienta implementa la gran mayoría de las técnicas conocidas para la exploración de puertos y permite descubrir información de los servicios y sistemas encontrados. *Nmap* también implementa un gran número de técnicas de reconocimiento.[45]

Mediante *Nmap* pueden realizarse, por ejemplo, las siguientes acciones de exploración:

a) Descubrimiento de direcciones IP activas mediante una exploración de la red
.nmap -sP IP ADDRESS/NETMASK
b) Exploración de puertos TCP activos.
.nmap -sT IP ADDRESS/NETMASK
c) Exploración de puertos UDP activos.
.nmap -sU IP ADDRESS/NETMASK
d) Exploración del tipo de sistema operativo de un equipo en red.
.nmap -O IP ADDRESS/NETMASK

[45] Jordi Herrera, Joan Comartí. Aspectos avanzados de seguridad en redes, pág 28, Software Libre.

Apéndice C
Mecanismos de seguridad en red

I. Cifrado

1. Cifrado simétrico

Un esquema de cifrado tiene componentes básicos como texto claro, clave de cifrado, algoritmo de cifrado, clave secreta y texto cifrado.

- ***Texto claro*:** es el mensaje o los datos originales que se introducen en el algoritmo de cifrado como entrada.
- ***Algoritmo de cifrado*:** encargado de realizar las sustituciones y transposiciones en el texto claro.
- ***Clave secreta*;** es también una entrada del algoritmo, las sustituciones y transposiciones realizadas por el algoritmo dependen de ella.
- ***Texto cifrado*;** el mensaje ilegible que se produce como salida, depende del texto claro, la clave secreta y el algoritmo empleado, para un mismo texto en claro, dos claves diferentes producirán dos textos cifrados diferentes.

Un aspecto primordial al momento de implementar una solución criptográfica es contemplar el *criptoanálisis*, éste es el proceso por el cual se busca descubrir un texto claro o una clave de cifrado, la estrategia del criptoanalista depende de la naturaleza del esquema de cifrado y de la información disponible. La tabla C.1 resume los diferentes tipos de ataques criptoanalíticos basados en la cantidad de información que posee el criptoanalista.

Tabla C. 1 Comparación de funciones hash seguras.

Tipo de ataque	Información que tiene el criptoanalista
- Sólo texto cifrado.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar.
- Texto claro conocido.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Uno o más pares de texto claro- texto cifrado formado con la contraseña secreta.
- Texto claro elegido.	-Algoritmo de cifrado. -Texto de cifrado que se va a decodificar. -Mensaje de texto en claro elegido por el criptoanalista junto con su correspondiente texto cifrado generado con la contraseña secreta.
- Texto cifrado elegido.	-Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Texto cifrado intencionado elegido por el criptoanalista con su correspondiente texto claro descifrado generado con la contraseña secreta.
-Texto elegido.	- Algoritmo de cifrado. -Texto cifrado que se va a descifrar. -Mensaje de texto claro elegido por el criptoanalista con su correspondiente texto cifrado generado con la contraseña secreta. -Texto cifrado intencionado elegido por el criptoanalista con su correspondiente texto claro generado con la contraseña secreta.

Un esquema de cifrado se dice es computacionalmente seguro, si el texto cifrado generado cumple con los dos o uno de los dos criterios siguientes:

- El costo de romper el cifrado excede el valor de la información cifrada.
- El tiempo necesario para romper el cifrado excede el tiempo de vida útil de la información.

El problema está en que es muy difícil estimar la cantidad de esfuerzos necesarios para realizar satisfactoriamente el criptoanálisis del texto cifrado, sin embargo, si no hay debilidades inherentes en el algoritmo, lo que procede es un enfoque de fuerza bruta.[46]

En el caso del cifrado simétrico en la tabla C.2 se muestran los cifrados más utilizados hasta la fecha, así como las características principales de cada uno de ellos.

Tabla C. 2 Algoritmos de cifrado simétrico convencionales.

Algoritmo	Tamaño de clave (bits)	Tamaño de bloque (bits)	Número de etapas	Aplicaciones
DES (1977)	56	64	16	SET, Kerberos.
3DES (1985)	112 o 168	64	48	Financial Key Management, PGP, S/MIME.
AES (1997)	128, 192, 256	128	10,12, 14	Destinado a sustituir DES y 3DES.
IDEA (1991)	128	64	8	PGP.
RC5 (1994)	Variable hasta 2048	64	Variable hasta 255	Varios paquetes de software.
BLOWFISH (1993)	Variable hasta 448	64	16	Varios paquetes de software.

Para que el cifrado simétrico funcione, las dos partes deben tener la misma clave o contraseña para un intercambio seguro y esa clave debe protegerse del acceso de otros, más aun, es deseable cambiar frecuentemente la clave para limitar la cantidad de datos comprometidos si un atacante la descubre. Por lo tanto, la robustez del sistema criptográfico depende de la técnica de distribución de claves, término que se refiere al mecanismo de entregar una clave a dos partes que deseen intercambiar datos, sin permitir que otros vean dicha clave, la distribución de claves se puede realizar por diferentes maneras para dos partes *A* y *B*.

- Una clave puede ser elegida por *A* y entregada físicamente a *B*.
- Una tercera parte puede elegir la clave, entregarla físicamente a *A* y a *B*.
- Si con anterioridad *A* y *B* han estado usando una clave, una parte podría transmitir la nueva clave a la otra cifrada, utilizando la antigua clave.
- Si *A* y *B* disponen de una conexión cifrada a una tercera parte *C*, *C* podría distribuir mediante los enlaces cifrados, una clave a *A* y a *B*.

[46] William Stallings, Fundamentos de Seguridad en Redes Aplicaciones y Estándares, Prentice Hall, 2da ed., 2005 pág 32

2. Cifrado asimétrico

También llamado criptografía de clave pública, permite brindar cifrado, intercambio de claves y firma digital. De igual importancia que la confidencialidad, como medida de seguridad, es la autenticación, la autenticación de mensaje por medio de firma digital garantiza que el mensaje proviene de las fuentes esperadas, además la autenticación puede incluir protección contra la modificación, el retraso, la repetición y el reordenamiento.

Un esquema de cifrado de clave pública tiene seis componentes básicos:

- ***Texto claro:*** es el mensaje o los datos originales que se introducen en el algoritmo de cifrado como entrada.
- ***Algoritmo de cifrado*****:** realiza diferentes transformaciones en el texto en claro.
- ***Clave pública y privada*****:** es una pareja de claves que han sido seleccionadas, de las cuales una se usa para el cifrado y otra para el descifrado, clave privada y pública respectivamente.
- ***Texto cifrado:*** el mensaje ilegible que se produce como salida depende del texto claro, la clave secreta y el algoritmo empleado, para un mismo texto en claro, dos claves diferentes producirán dos textos cifrados diferentes.
- ***Algoritmo de descifrado*****:** este algoritmo acepta el texto cifrado y la clave correspondientes para producir el texto claro original.
- ***Entidad certificadora*****:** ésta contiene la clave pública de todos los usuarios para que otros las usen con la finalidad de descifrar mensajes, mientras que la clave privada sólo es conocida por el propietario, es importante mencionar que este elemento es opcional pero altamente recomendado contemplarlo.

Los sistemas de clave pública se caracterizan por el uso de algoritmo criptográfico con dos claves, una no se revela y la otra sí, dependiendo de la aplicación, el emisor hace uso de su clave privada o la clave pública del receptor o las dos para realizar algún tipo de función criptográfica, en términos generales, se puede clasificar el uso de criptosistemas de clave pública en tres categorías:

- ***Cifrado/descifrado***: el emisor cifra un mensaje con la clave pública del receptor.
- ***Firma digital***: El emisor *firma* un mensaje con su clave privada, esto se consigue mediante un algoritmo criptográfico aplicado al mensaje o a un pequeño bloque de datos que es una función del mensaje.
- ***Intercambio de claves***: dos partes cooperan para intercambiar una clave de sesión. Hay distintas posibilidades que implican la clave privada de una o de las dos partes.

Algunos algoritmos son adecuados para las tres aplicaciones, mientras otros sólo se pueden emplear para una o dos de ellas. La tabla C.3 muestra algunos de los algoritmos que se emplean en el cifrado asimétrico o de clave pública.

Tabla C. 3 Aplicaciones para criptosistemas de clave pública.

Algoritmo	Cifrado /Descifrado	Firma digital	Intercambio de claves
RSA (1977)	Sí	Sí	Sí
ElGamal (1978)	Sí	Sí	Sí
Diffie-Hellman (1976)	No	No	Sí
DSS (1991)	No	Sí	No
Curva Elíptica-ECC(1985)	Sí	Sí	Sí

a) Firma digital

El cifrado de clave pública se puede utilizar para realizar firmas digitales como lo ilustra la figura C.1, éste se puede utilizar con cifrado o trabajar solo, en este caso A envía el mensaje aplicándole algún algoritmo que soporte firma digital con su clave privada a un usuario B, B podrá verificar el origen del archivo al llevar a cabo el descifrado con la clave pública de A, en este momento el cifrado sirve como firma digital, además de que es imposible alterar el mensaje sin la clave privada de A, así que el mensaje queda autenticado de origen y permite confirmar integridad.

En el caso del descifrado se cifra con la clave pública de la entidad a la que se desea enviar datos y el receptor descifra el mensaje con su clave privada, ya que es el único que conoce dicha clave, sólo él podrá descifrar, de esta manera se genera un canal seguro.

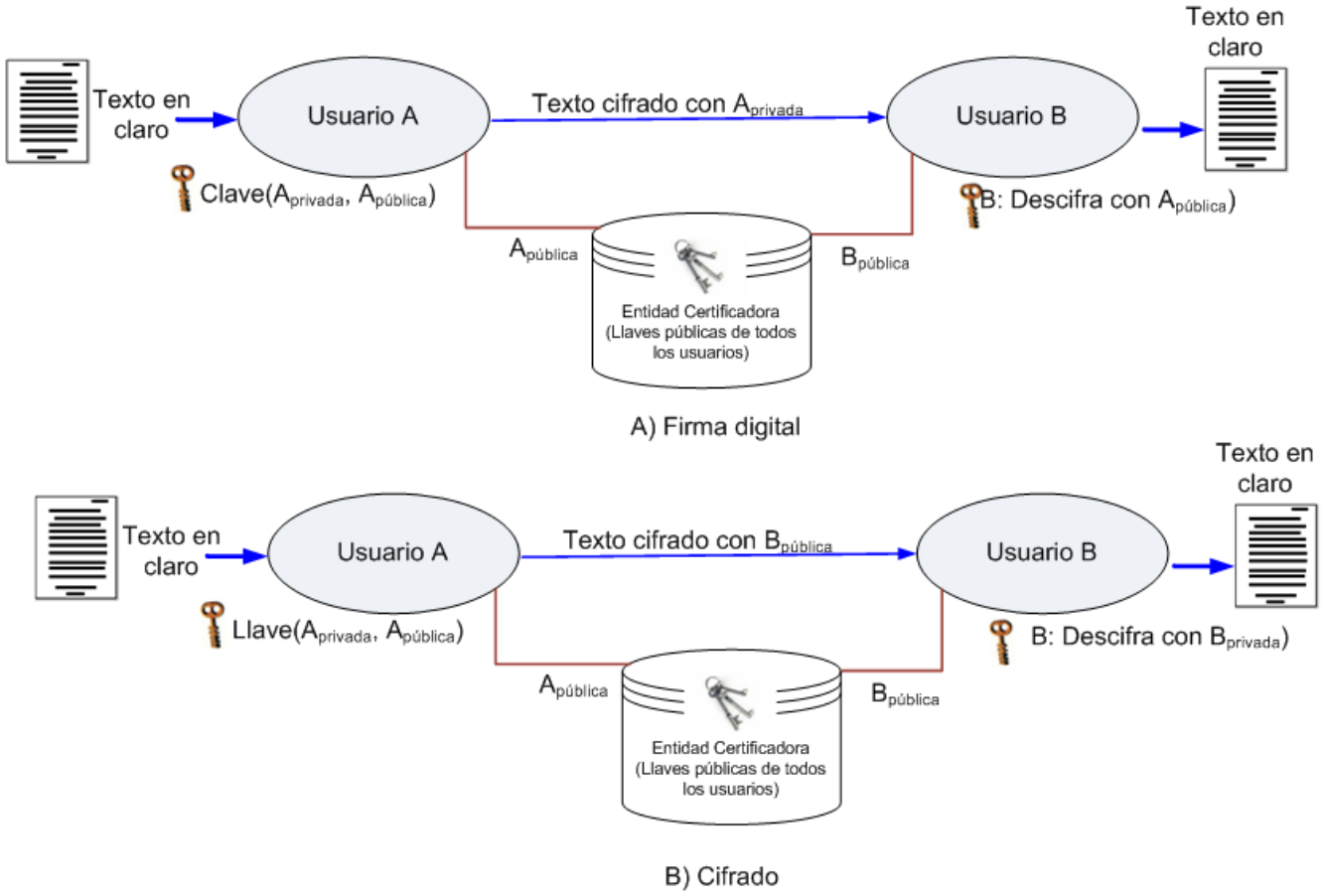


Figura C. 1 Cifrado criptografía de clave pública.

En el mundo real se firma un documento para autenticar que sólo el firmante legítimo puede producirlo, como es el caso de las identificaciones personales, pagos con tarjetas bancarias al utilizar terminales, entre otros, la analogía en el cómputo es la firma digital, en el caso de falsificación, una tercera parte interviene para juzgar la autenticidad en el mundo digital, esta función queda a cargo de las entidades certificadoras. Las características que ofrece una firma digital son autenticación, infalsificable, única para cada documento, inalterable y no repudiada, es decir, el firmante no puede negar la firma.

b) Entidades certificadoras

Adicional a estos dos funcionamientos mostrados en la figura C.1, el cifrado de clave pública trata el problema de distribución de claves y he aquí donde surge un gran problema, ya que la base de este tipo de cifrado establece que la clave pública es de carácter público, así, si hay un algoritmo de clave pública aceptado como RSA, cualquier participante puede enviar su clave pública a otro o difundir su clave a toda la comunidad en general. Aunque este enfoque es conveniente, se tiene la debilidad que cualquiera puede falsificar ese dato público, es decir, un usuario podría hacerse pasar por el usuario *A* y enviar su clave pública a otro participante o difundirla. Hasta el momento en que *A* descubre la falsificación y alerta a los otros participantes, el falsificador puede leer todos los mensajes cifrados enviados a *A* y puede usar las claves falsificadas para la autenticación.

La solución a este problema es el certificado de clave pública, este certificado consiste en una clave pública y un identificador o nombre de usuario del dueño de la clave, además de información como fecha de expiración, número de serie, firma digital del emisor, con todo el bloque firmado por una tercera parte confiable. Comúnmente la tercera parte es una autoridad certificadora (CA- Certificate Authority), en la que confía la comunidad de usuarios. Algunas CA de las más prestigiosas son las siguientes:

- Verysing (comercial). http://www.verisign.com/
- Verizonbusiness (comercial). http://www.verizonbusiness.com
- Darthseven system (comercial). http://darth7.supersite.myorderbox.com/
- PyCA(Solución libre). http://www.pyca.de/
- OpenCA (Solución libre). http://www.openca.org/
- Open source PKI Mozilla. http://www.mozilla.org/projects/security/pki/
- Bibliotecas criptográficas para java y C#. http://www.bouncycastle.org
- Sistema central propio.

El nivel de seguridad en la validación del certificado está limitado a la dificultad del impostor que relacione su clave pública con la identidad de otra persona, se podrá hacer pasar por otra persona y hacer actividades maliciosas, de cualquier manera el usuario deberá almacenar de forma segura su clave privada ya que en ella recae la seguridad.
Las autoridades certificadoras garantizan que sean infalsificables las claves públicas, ya que implementan los servicios de autenticación y no repudio, además de ser una forma segura de distribuir claves públicas en comunidades grandes como lo es Internet.

c) Funciones Hash

Utilizadas para obtener integridad en la transmisión de mensajes o datos almacenados, además de permitir detectar o prevenir alteraciones durante la transmisión, esta función se caracteriza por ser unidireccional, acepta un mensaje de tamaño variable M como entrada y produce un resumen del mensaje de tamaño fijo H(M) como salida, es importante saber que se produce una única cadena diferente a todas las demás para cada M.

La finalidad de una función hash es la de obtener una *huella* de un archivo, mensaje u otro bloque de datos para que resulte útil a la autenticación del mensaje, una función hash H debe poseer las siguientes propiedades:

I. H puede aplicarse a un bloque de datos de cualquier tamaño.
II. H produce una salida de tamaño fijo.
III. H(x) es relativamente fácil de computar para cualquier *x* dado, haciendo que tanto las implementaciones de hardware y software sean prácticas.
IV. Para cualquier valor *h* dado, es imposible desde el punto de vista computacional, encontrar *x* tal que H(x)=h, lo cual con frecuencia, se conoce en la literatura como propiedad unidireccional.
V. Para cualquier bloque dado x, es imposible desde el punto de vista computacional, encontrar con y≠ x que H(y)=H(x), lo que se conoce como colisiones si se presenta el caso.

Las cuatro primeras propiedades son requisito para la aplicación práctica, en el caso de la quinta propiedad existen algoritmos que presentan colisiones ya que diferentes mensajes producen el mismo valor hash. Una función hash que cumple con las primeras cuatro propiedades se conoce como función hash débil, si también posee la sexta propiedad se denomina función hash robusta, a continuación en la tabla C.4 se hace una comparación de las funciones hash seguras.

Tabla C. 4 Comparación de funciones hash seguras.

	MD5	**SHA-1 (1994)**	**RIPEMD-160 (1996)**
Longitud del resumen	128 bits	160 bits	160 bits
Unidad básica de procesamiento	512 bits	512 bits	512 bits
Número de pasos	64 (4 etapas de 16)	80 (4 etapas de 20)	160(5 pares de etapas de 16)
Tamaño máximo del mensaje	∞	264 -1 bit	∞

Existe una versión más reciente de SHA-1 denominada SHA2, ésta genera cadenas de 512 bits, existen variantes de SHA-1 con cadenas de resumen con una longitud de 224, 256 y 384, adicional a estos algoritmos existen otros como N-Hash de 128 bits, Snefru 128 y 256 bits, Tiger hasta 192 bits optimizado para máquinas de 64 bits, Haval hasta 256 bits.

La ventaja que tienen estos enfoques es que sólo se cifra un fragmento del mensaje para generar la función hash, lo que significa un costo computacional menor, pero sólo garantiza integridad, por esta razón se contemplaron los algoritmos como MD5, SHA-1 y RIPEMD.

Las funciones hash tienen varios usos dentro de los más comunes se encuentran:

- ***Hash de contraseñas***: como método de almacenamiento de contraseñas.
- ***Integridad de archivos***: utilizando la cadena que produce cada archivo digital con algún algoritmo en particular.
- ***Huella digital:*** de mensajes enviados y eficiencia en firmas digitales.

II. Topologías, Filosofías y tipos de filtrado de Firewalls

Cuando se desea implementar un firewall para protegerse de ciertos tipos de ataques, entra en juego otra decisión muy importante como la ubicación correcta que debería tener un firewall dentro de la red, bajo este principio se han diseñado distintas topologías de acuerdo con las necesidades y el grado de seguridad que se desee tener, se entiende por topología como la ubicación física que éste tendrá dentro de una red, cabe mencionar que las topologías o distribución de firewalls implican costos dentro de la implementación.

Se utilizan tres modelos, aunque éstos son flexibles y pueden ser modificados de acuerdo con las necesidades, además de que es posible combinar las distintas arquitecturas y tipos de filtrado.

a) Multi-homed host: equipo conectado a múltiples redes, el equipo cuenta con más de una tarjeta de red con la cual se puede conectar física y lógicamente con distintos segmentos de red, sin embargo, existe una variante de esta topología conocido como dual host-equipo con dos tarjetas de red.
b) Dual homed firewall: es un firewall con dos tarjetas de red, cada una conectada a distintas redes, por lo general se conecta una red segura (interna) contra otra red insegura (externa), por lo que todo el tráfico proveniente de una red insegura es filtrada antes de pasar a la red segura, en este caso el firewall actúa en la mayoría de los casos como un intermediario entre ambas redes, en la figura C.2 se puede observar dicha topología.

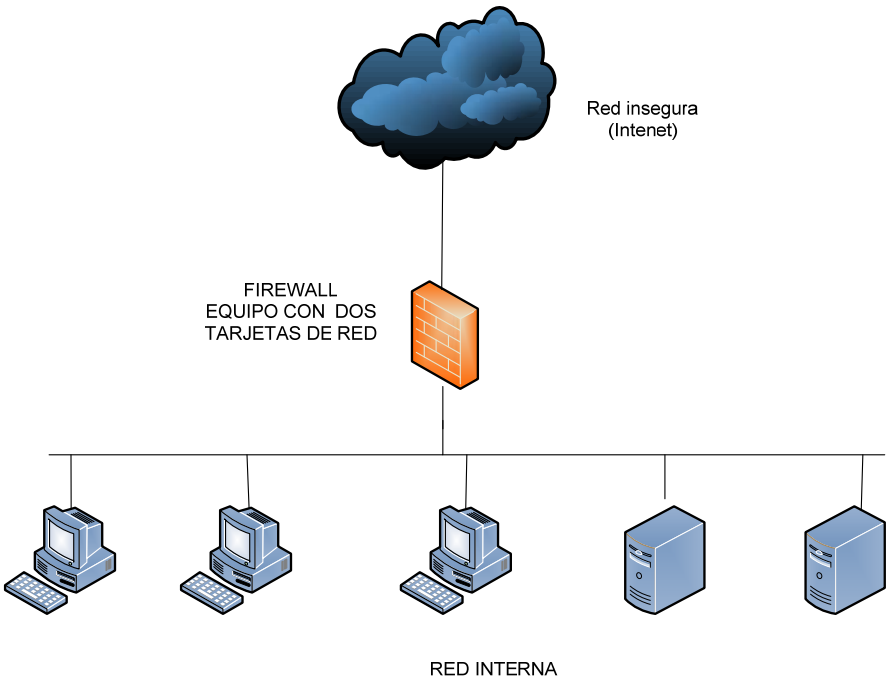


Figura C. 2 Firewall con dos interfaces de red.

La desventaja de esta arquitectura se debe a que si un atacante consigue comprometer cualquiera de los servidores que se encuentre detrás de este punto único, los otros equipos, podrán ser atacados sin ninguna restricción desde el equipo que acaba de ser comprometido.

c) Screened host*:* topología de firewall, hace uso de un equipo llamado bastión host- equipo donde se instala el software necesario para que éste pueda retener los ataques provenientes de internet, en este modelo la conexión de las redes se realiza con el apoyo de un router configurado para bloquear todo el tráfico entre la red externa y los hosts de la red interna excluyendo el equipo bastión host, este tipo de arquitectura permite soportar servicios proxy en bastión host, así como filtrado de paquetes en el router.

En la forma de operar todas las conexiones provenientes de la red insegura son re direccionadas por el router al bastión host y de ahí a los equipos de la red interna, evitando de esta manera una conexión directa con la red externa.

La debilidad de esta configuración es que si el bastión host es comprometido, existe libertad para tener acceso a cualquier host ya que no existe ningún mecanismo entre el bastión host y los equipos de la red interna, esta topología se puede observar en la figura C.3.

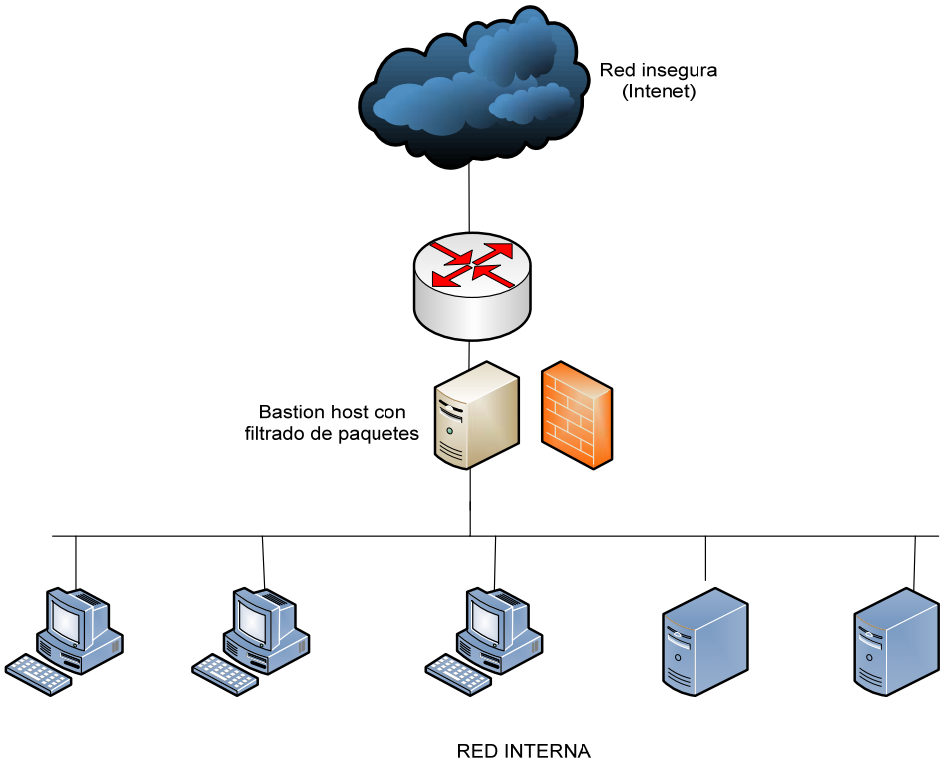


Figura C. 3 Screened host firewall.

d) Screened subset: En una arquitectura screened subnet, se agrega una red en la zona de bastión host, esta red es llamada red perimetral, se encuentra separada de la red interna, también es denominada Demilitarized Zone- Zona desmilitarizada(DMZ).

Los routers se configuran, mediante reglas de filtrado para que tanto los nodos de la red interna como los de la externa sólo puedan comunicarse con nodos de la red del perímetro. Esto permite a la red interna ser invisible a la externa.

En este esquema por lo general se utilizan dos routers: uno exterior y otro interior. El router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la

red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno) (figura C.4).

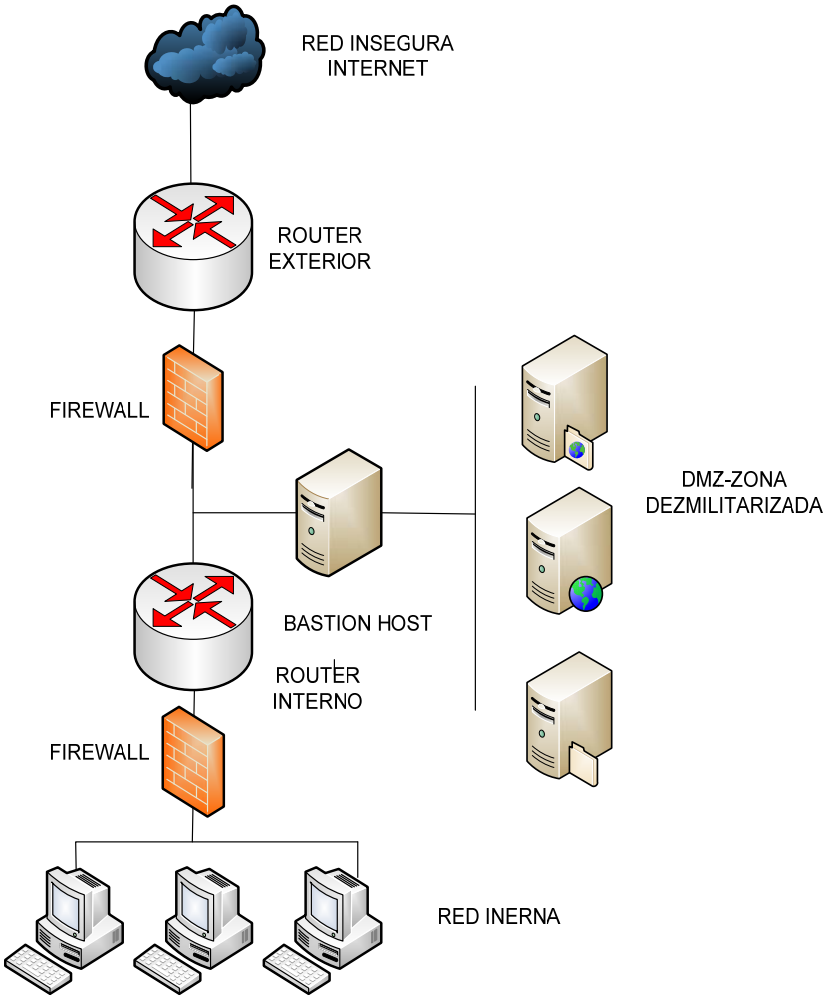


Figura C. 4 Screened subnet firewall.

Filosofía de firewall

El concepto de filosofías de firewall está relacionado directamente con la forma de establecer las reglas dentro del firewall, para permitir o negar el flujo de datos desde una red insegura a otra segura o viceversa. Se manejan dos filosofías.

La primera filosofía es bloquear todo el tráfico que no se desea permitir ingresar a la red o aquel que desea salir, esta filosofía es denominada permisiva, sin embargo, ésta resulta bastante peligrosa, ya que si se consideran los 65535 puertos disponibles para los protocolos TCP, UDP, establecer reglas para las distintas aplicaciones resultaría complicado y con ello el nivel de seguridad disminuye.

Por otro lado, la filosofía prohibitiva consiste en negar todo el tráfico entrante o saliente a excepción de aquel que se encuentra estrictamente permitido, con esta filosofía el control del flujo de datos de una red a otra se torna mucho más sencilla, es la filosofía más utilizada, además de que por default es una regla establecida por la mayoría de firewalls.

Tipos de Filtrado

Implementar un firewall implica un análisis del tipo de tráfico a bloquear, para ello se cuenta con una clasificación de configuración, de acuerdo con el tipo de filtrado que éstos son capaces de realizar, el nivel de seguridad dependerá directamente de los objetivos de la institución.

Se clasifican principalmente en los siguientes tipos:

- Filtrado de paquetes.
  - Estático.
  - Dinámico.
  - Estado.
- Gateways de aplicación.
- Filtrado híbrido.

Cada uno de ellos garantiza un nivel de seguridad, y desde luego cada uno implica un costo, en tabla C.5, se muestra a grandes rasgos el nivel de seguridad, que cada uno ofrece así como instituciones que pueden implementarlos.

Tabla C. 5 Uso y Nivel de Seguridad de Firewall.

Tipo de Firewall	Nivel de Seguridad Alto Ambiente (Hospital)	Nivel de Seguridad Medio Ambiente (Universidad)	Nivel de Seguridad Bajo Ambiente (Negocios pequeños)
Filtrado de paquetes	0	1	4
Gateway de aplicación conocido como proxy	3	4	2
Gateways híbridos	4	3	2

Nota: el número 4 indica que es recomendable utilizarlo, 3 se considera una solución efectiva, 2 aceptable, 1 no recomendable y 0 no aceptable, en la actualidad la implementación de uno u otro tipo de firewall depende directamente de los objetivos de la institución, por lo que la elección requiere de un previo análisis de los recursos a proteger.

a) Filtrado de paquetes

Este tipo de filtrado conocido también como firewalls de primera generación, son los más simples y sencillos comparados con los firewalls actuales, sin embargo, esto no quiere decir que son obsoletos, las reglas que permiten o niegan el paso de paquetes basadas en la dirección destino u origen y puertos ofrecen un nivel de seguridad mínimo, son un tipo de firewall apropiado si la seguridad que se requiere es mínima.

El firewall de filtrado de paquetes realiza la transmisión con base en el contenido de la cabecera IP, UDP o TCP. Aplicando reglas a la entrada o salida de las interfaces de red. Las reglas de filtrado se encargan de determinar si a un paquete le está permitido pasar de la parte interna de la red a la parte externa y viceversa, verificando el tráfico de paquetes legítimo entre ambas partes.

Este tipo de firewall se basa en la información que el paquete IP contiene en su cabecera para permitir o negar el tráfico de datos a través de la red, el tipo de información contenida en la cabecera es dirección destino, dirección origen, así como el estado de fragmentación del paquete. La cabecera TCP contiene información acerca del estado de la conexión, puerto origen y destino, dicha información permite determinar el tipo de aplicación que envía información, así como el host destino. En la figura C.5 se muestra un esquema de este tipo.

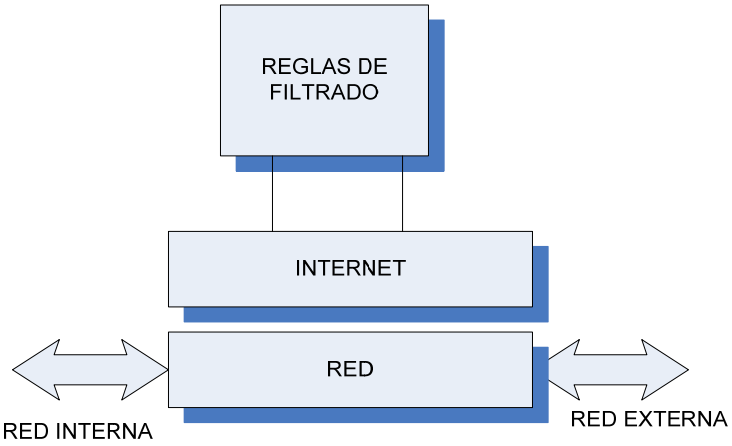


Figura C. 5 Filtrado de paquetes.

Cabe mencionar que las reglas establecidas pueden ser de manera jerárquica bajo una política por defecto de negar todo o aceptarlo todo, se debe tener especial cuidado en el diseño de las mismas ya que una mala configuración estaría dejando una puerta de entrada para el intruso.

Algunos tipos de filtrado comunes son:

- Con base en la dirección destino o fuente.
- Tipos de indicadores con algunas banderas.
- Contenido del paquete.
- Tamaño del paquete.
- Puertos de origen y de destino.

El hecho de negar todo generalmente se recomienda establecer como la última regla, después de colocar arriba de ella sólo las permitidas, este tipo de firewalls sólo es considerado una primera línea de defensa ya que por naturaleza del mismo no es posible prevenir ataques del tipo IP spoofing, DNS spoofing. La autenticación robusta no es soportada por algunos gateways que utilizan el filtrado de paquetes.

Entre las ventajas que ofrece este tipo de firewalls es de gran utilidad para redes con una carga de tráfico elevada, esta tecnología permite la implantación de la mayor parte de las políticas de seguridad necesarias.

b) Filtrado de paquetes por estado

El filtrado por estado es un tipo de firewall más avanzado, ya que analiza los paquetes con mayor detalle, provee un alto grado seguridad en comparación con los firewalls de primera generación

(filtrado de paquetes), en este tipo de firewalls los protocolos de Internet TCP, UDP son analizados con mayor profundidad, así como los servicios FTP, mail, web, telnet, entre otros, además de aplicaciones de negocios como RPC, SQL a través de un constante monitoreo y evaluación del estado y progreso para cada conexión o transacción, entre las ventajas que este tipo de firewalls ofrece, se encuentra la mayor precisión en el filtrado ya que analiza el payload –carga útil de un paquete, permite determinar cuántas conexiones simultáneas puede aceptar, inspección de filtrado por estado, sin embargo, también presenta desventajas ya que requiere mayor procesamiento.

Los estados de conexión son vigilados de principio a fin, cuando un paquete llega al firewall se verifica que éste sea parte de la conexión para permitir el paso o de lo contrario se descarta.

En la tabla C.6 se muestran los estados de una conexión.

Tabla C. 6 Estados de una conexión.

Estado	Significado
ESTABLISHED	Conexión establecida.
SYN_SENT	Intentando establecer una conexión.
SYN_RECV	Petición de conexión recibida.
FIN_WAIT1	El socket está cerrado y la conexión finalizando.
FIN_WAIT2	La conexión está cerrada, y el socket está esperando que finalice la conexión.
CLOSED	El socket está esperando después de cerrarse.
CLOSE_WAIT	El socket no está siendo usado.
LAST_ACK	La conexión remota ha finalizado y se espera que se cierre el socket.
LISTEN	El socket está esperando posibles conexiones entrantes.
CLOSING	Ambos sockets han finalizado pero aún no fueron enviados todos los datos.
UNKNOWN	El estado del socket se conoce.

En el momento que se establece la conexión se está verificando constantemente el estado de la misma, e incluso es posible eliminar una conexión si durante un periodo de tiempo no se observa comunicación.

c) **Gateway de aplicación.**

En este tipo de firewall, conocido como Gateway de aplicación o como servidor intermediario, los paquetes son analizados a nivel de aplicación, por lo que cuando un usuario desea comunicarse deberá pasar a través de este servidor, el cual funciona como un proxy-servidor intermediario asociado a una o más aplicaciones.

El servidor *proxy* se encargará de realizar las conexiones solicitadas con el exterior y cuando reciba una respuesta la retransmitirá al equipo que había iniciado la conexión, por lo que éste determina si acepta o rechaza una petición de conexión, para los usuarios este proceso es transparente como se puede observar en la figura C.6.

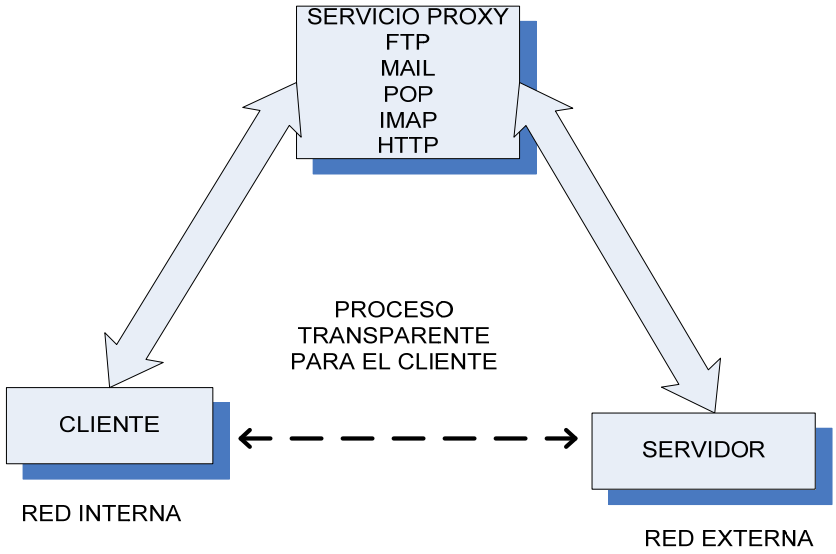


Figura C. 6 Firewall de aplicación.

Una de las desventajas de este tipo de firewalls es que requieren de un procesamiento mayor, debido a que atienden a un gran número de peticiones y analiza todo el contenido de cada paquete, a cambio de mayor seguridad ya que sólo los servicios para las cuales hay un servidor proxy, se les permite el acceso, por lo que si se compara con un firewall de filtrado de paquetes éste resulta ser menos eficiente, en la práctica se suele utilizar ambos tipos.

Otros tipos de firewall

a) Firewalls comerciales

Los firewalls también se clasifican en firewalls comerciales y de distribución libre, los firewalls comerciales pueden ser appliance o de software, dichos dispositivos basados en software o como una combinación de hardware y software cuya finalidad básica es bloquear el tráfico de datos desde una red segura a otra insegura o viceversa.

Algunas de las ventajas de estos dispositivos son:

- Facilidad de implementación.
- Ofrecen una administración más sencilla.
- Definen reglas utilizadas en el mercado.
- Actualizaciones constantes.
- Posibilidad de crecimiento y comunicación con otros dispositivos de monitoreo.
- Ofrecen un alto procesamiento, lo que los hace eficientes.
- Soporte.

Desventajas:

- Presentan un alto costo.
- Aunque presentan facilidad de comunicación con otros dispositivos, en su mayoría deben ser de la misma marca.
- Ofrecen menos flexibilidad en cuanto a necesidades se refiere.

Existen en el mercado diversas compañías encargadas de producir estos firewalls como son CISCO, 3com, Juniper, Cyberoam, Endian, Barracuda Networks, WatchGuard, Fortinet, Check Point, ZyXEL, entre muchos otros, cada uno tratando de ofrecer más características con la finalidad de obtener el beneficio de compra, en la figura C.7 se muestra un diagrama de un firewall basado en hardware.

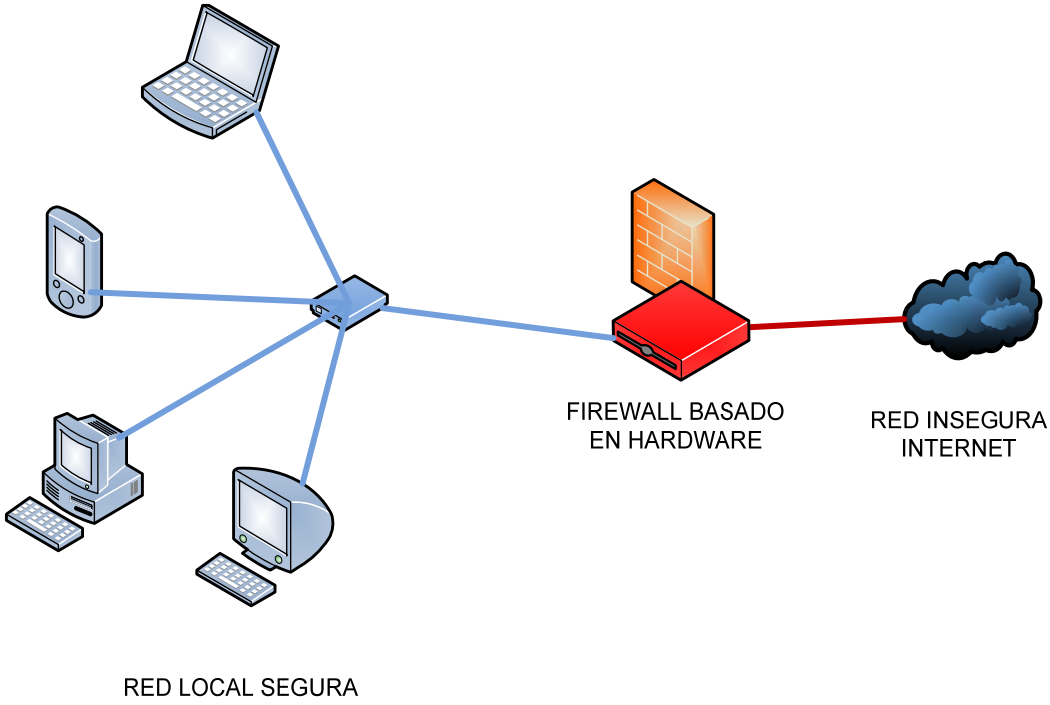


Figura C. 7 Firewall basado en hardware.

b) Firewall por software

Los firewalls basados en software existen en sus versiones comerciales y libres, en el caso de los comerciales ofrecen cierta facilidad de implementación, los costos no simpre son menores comparados con appliance – hardware de propósito dedicado, algunos ejemplos son Microsoft ISA server, Microsoft ForeFront, otros de distribución libre de UNIX emplean iptables y pf, éstos últimos ofrecen flexibilidad para su implementación ya que se adaptan fácilmente a las necesidades, aunque su implementación requiere invertir más tiempo y monitoreo constante, además de no brindar soporte en tiempo real.

III. Tipos de detectores de intrusos

Tipos de IDS

De acuerdo con la funcionalidad de los sistemas detectores de intrusos, se clasifican en tres categorías principales, detector de intrusos para un solo equipo llamado HIDS, detector de intrusos para una red (NIDS), y el sistema detector de intrusos distribuido (DIDS).

- Sistema detector de intrusos de red - Network Based Intrusion Detection System (NIDS).
- Sistema detector de intrusos para un equipo Host-Based Intrusion Detection System (HIDS).

- Sistema detector de intrusos distribuido Distributed Intrusion Detection System (DIDS).

La utilidad de cada uno depende del tipo de actividad a monitorear, finalmente en la práctica se utiliza una combinación de HIDS y NIDS.

a) Host IDS

El sistema detector de intrusos de un equipo, opera a nivel local, analizando eventos y bitácoras de un solo equipo, lanzando una alerta si detecta comportamientos extraños, el hecho de que la tarjeta de red no opere en modo promiscuo ofrece ventajas en cuanto a recursos de equipo se refiere, ya que disminuye la carga de trabajo. Otra de las ventajas que se tienen al implementar un HIDS es la facilidad de implementación de las reglas ya que sólo es necesario tener las reglas específicas para cada servicio con el que se cuente.

Si alguna institución cuenta con servidores de correo, web y se instala un HIDS para cada servidor, las reglas se personalizan de acuerdo con el tipo de ataques a los que cada servidor está propenso, de esta manera se están protegiendo servicios críticos y sólo será necesario actualizar de manera constante las reglas dependiendo de las nuevas vulnerabilidades que surjan, y las necesidades propias de cada organización.

Sin embargo, los HIDS pueden ser instalados en cualquier equipo que se desee monitorear, en la figura C.8 se muestra este tipo de IDS.

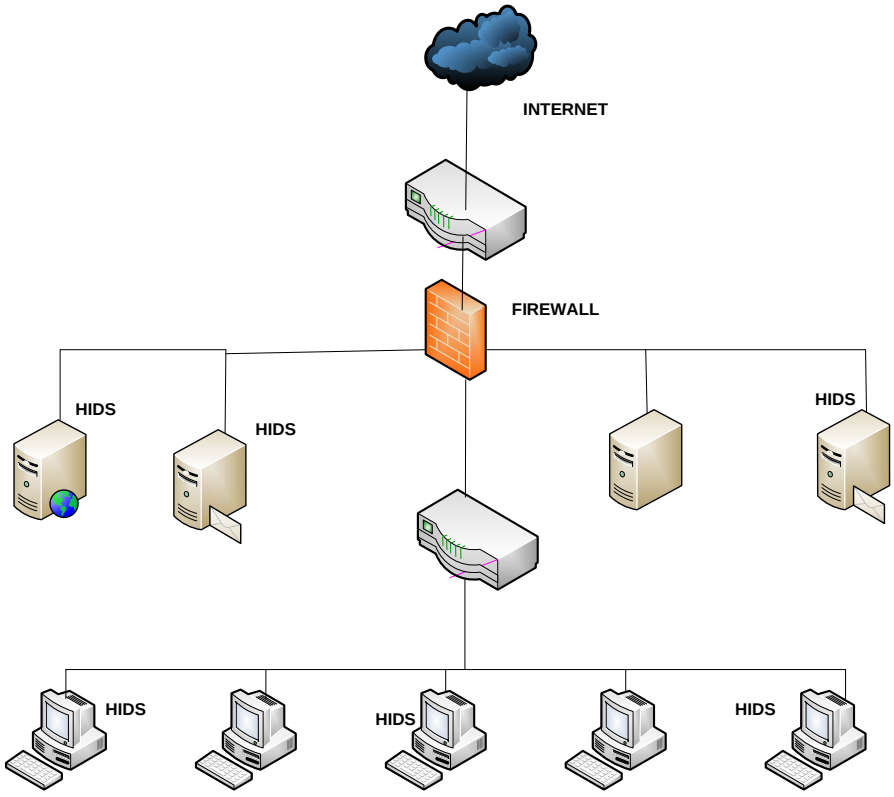


Figura C. 8 IDS.

En la tabla C.7 se resumen algunos HIDS actualmente utilizados.

Tabla C. 7 HIDS.

Nombre	Sistema operativo	Comercial	Código Abierto	Características principales
Open Source Tripwire 2.x	GNU /Linux	Sí		Verifica integridad de los archivos. Una licencia por equipo. Soporte sólo por la comunidad
Tripwire Enterprise 7.x	Solaris/SPARC, Solaris/x86, AIX, HP-UX Red Hat, SUSE, CentOS and Fedora Core 2	Sí	NO	Analiza cambios en los sistemas de archivos y propiedades del sistema, administración centralizada, las reglas pueden ser aplicadas a distintos dispositivos, soporte por Tripwire.
Tripwire for Servers 4.x	Solaris/SPARC, AIX, HP-UX, FreeBSD Red Hat, SUSE, TurboLinux	Sí	NO	Analiza cambios en los sistemas de archivos y propiedades del mismo. Genera reportes de manera gráfica. Soporte por Tripwire.
SNORT	Windows/Linux/ OpenBSD		Sí	Sistema detector de intrusos de código abierto. Capaz de analizar paquete en tiempo real. Es posible configurarlo de tres maneras distintas snnifer, IDS y como analizador de bitácoras.

b) Network IDS

NIDS este un tipo de sistema detector de intrusos encargado de monitorear toda una red, es decir, que actúa sobre todo un segmento de red, generalmente una tarjeta de red no está configurada en modo promiscuo, por lo que sólo puede ver el tráfico dirigido a ella, sin embargo, si se desea analizar todo el tráfico sin importar el destinatario, es necesario configurar la tarjeta de red en modo promiscuo, NIDS opera en modo promiscuo para monitorear todo el tráfico del segmento tanto el que entra como el que sale e incluso el tráfico local.

Aunque es una de las arquitecturas más utilizadas, demanda un alto procesamiento de recursos, de igual manera que los firewalls, es posible contar con la cantidad de NIDS que se deseen dependiendo de la estrategia de seguridad o necesidades, por otro lado, cabe mencionar que el análisis de los paquetes que circulan por la red debe de ser tratado con especial cuidado para evitar un mal uso, en la figura C.9 se muestra una arquitectura NIDS.

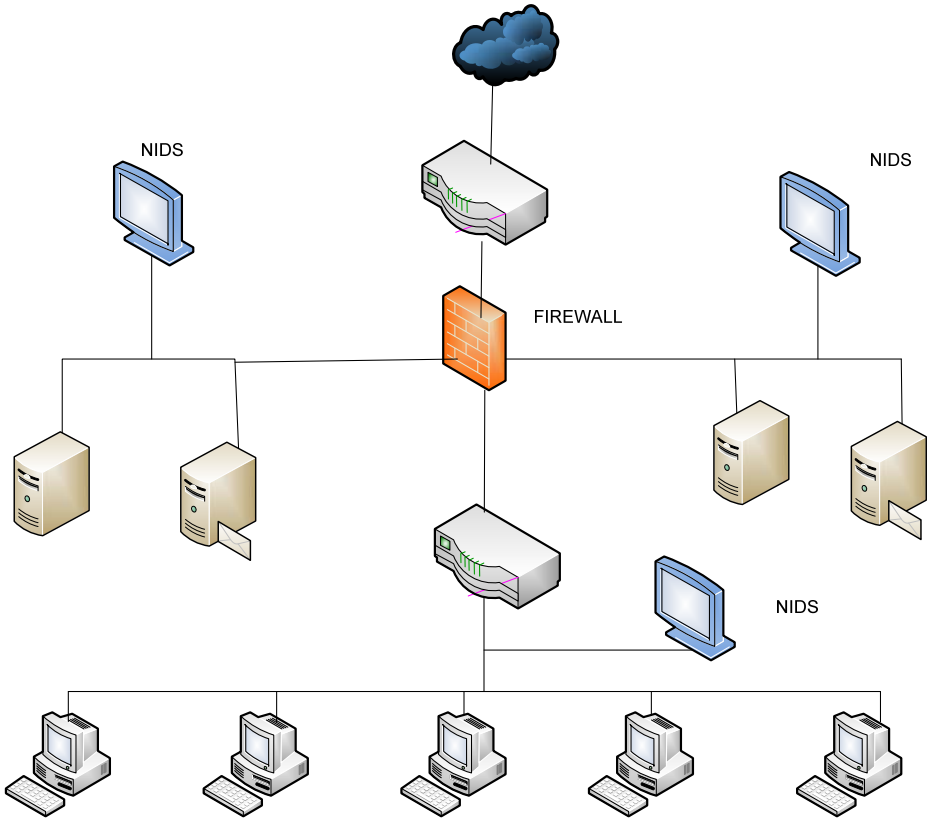


Figura C. 9 NIDS.

En la figura C.9 se observa que existen varios NIDS que se encargan de monitorear la red, éste es un ejemplo de arquitectura de seguridad en profundidad.

c) DIDS network

Los DIDS son otra variante de los sistemas detectores de intrusos, para esta arquitectura se cuenta con una estación central encargada de administrar los sistemas detectores remotos, lo cual permite una administración centralizada, la estación es la encargada de administrar bitácoras de los ataques de manera continua, las reglas de cada sistema se encuentran centralizadas y sólo si es necesario, las reglas son adaptadas para cada dispositivo en particular.

Cuando existe una alerta lanzada por alguno de los sistemas detectores, ésta es enviada a la estación de administración, la información es utilizada para notificar a los administradores de cada IDS.

Los DIDS pueden estar formados por HIDS, NIDS o una combinación de los dos, también pueden estar configurados en modo promiscuo, lo único que se requiere es que cada HIDS o NIDS envíe reportes a la estación de administración.

La comunicación entre los sensores y la base encargada de la administración se puede implementar a través de VPN's, utilizando la infraestructura existente.

En la figura C.10 se muestra un esquema de arquitectura DIDS.

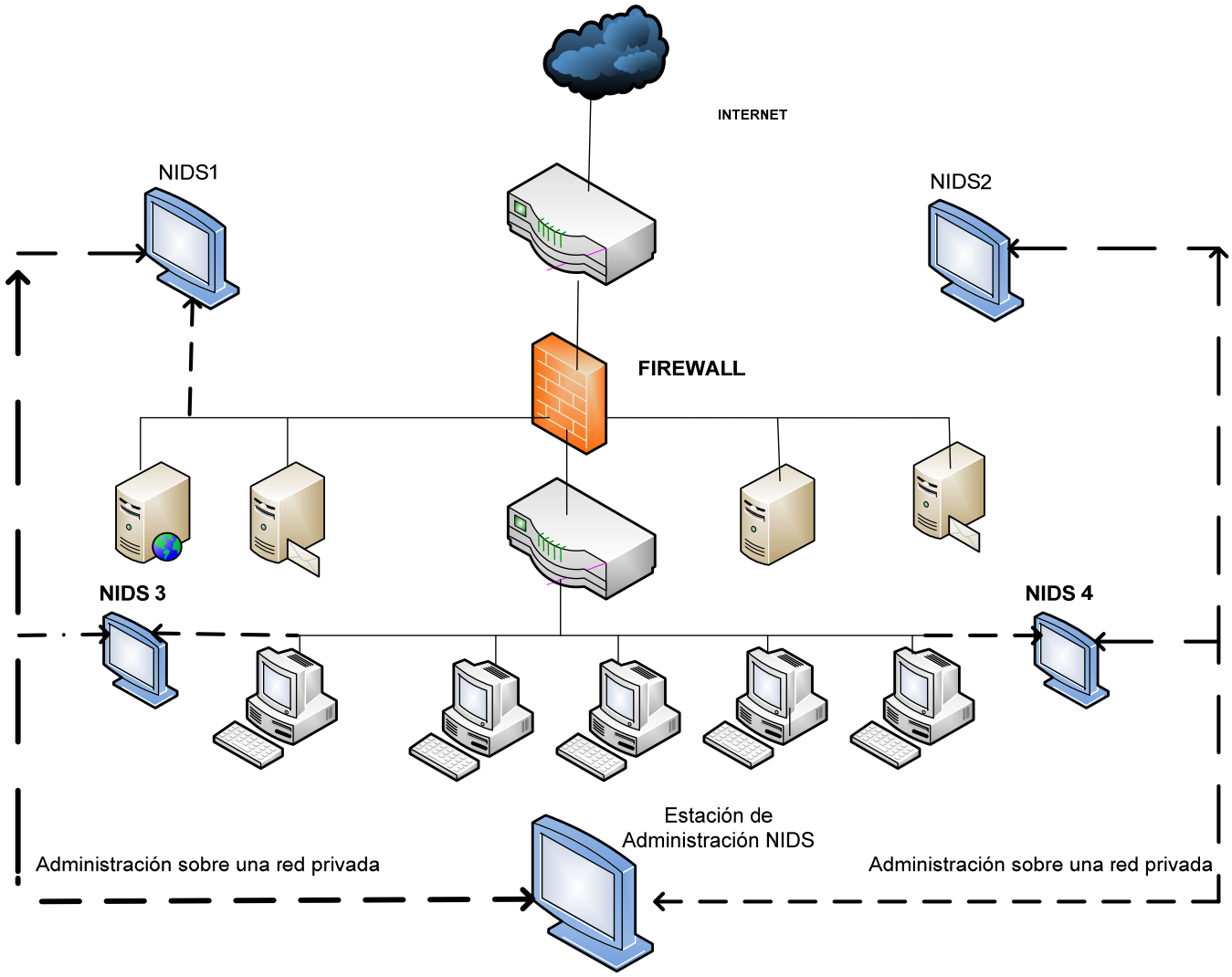


Figura C. 10 DIDS.

Los IDS pueden clasificarse también en:

a) IDS comerciales

Dentro de la clasificación de sistemas detectores de intrusos existen IDS comerciales y aquellos que son de código abierto.

Actualmente existe una gran cantidad de empresas que se dedican a producir IDS comerciales entre los que se encuentran CISCO, check point, Fortinet, IDS sourcefire, Dragon IDS, IDS Center.

b) IDS por software

De acuerdo con una de las clasificaciones de sistemas detectores de intrusos pueden estar basados sólo en software o una combinación de software y hardware, los IDS que se basan en software

deben instalarse en el equipo que se desea monitorear o en equipos dependiendo de si éstos son es un HIDS o NIDS.

Para la implementación de los distintos IDS que existen en el mercado se requiere de una cuidadoso análisis de los requerimientos de cada uno, ya que muchos de ellos dependen de otras herramientas además del tipo de sistema operativo para un adecuado funcionamiento, por lo que es conveniente contar con la documentación.

En la tabla C.8 se muestra un resumen de IDS basados en software.

Tabla C. 8 IDS por software.

Nombre	Comercial	Libre	Tipo
Snort		Sí	NIDS
Tripwire	Sí	Sí	HIDS
IDS center			NIDS, IPS
Cisco	Sí		NIDS
Nagios		Sí	HIDS
ELM			
DRAGON SQUIRE			HIDS
INTERNET SECURITY SYSTEMS	Sí		HIDS ,NIDS
DRAGON CENSOR	Sí		NIDS
SNARE	Sí		NIDS

Sistemas encargados de prevenir intrusiones (IPS)

Intrusión Prevention System- Sistemas encargados de prevenir intrusiones, cuando surgieron los primeros sistemas detectores de intrusos, las tareas que éstos realizaban eran simples, sin embargo, se han desarrollado sistemas que no únicamente lanzan alertas de posibles anomalías, debido a que los ataques cada día son más sofisticados, surge la necesidad inherente de evadir ataques en tiempo real con el uso de sistemas detectores que no sólo lancen alertas sino que además tengan la capacidad de responder a los ataques.

Un IPS opera de la siguiente manera, cuando se detecta un ataque la comunicación entre el intruso y el equipo comprometido, es bloqueada, se eliminan procesos que sean sospechosos o que intenten provocar un desbordamiento de memoria, se bloquea en el router o firewall el puerto o dirección IP del atacante para evitar ataques futuros.

Sin embargo, se debe tener especial cuidado en el manejo de un IPS ya que existen riesgos como el hecho de que un atacante pueda buscar nuevas alternativas para evadir su detección haciendo uso de

herramientas de escaneo pasivo que le permitan determinar nuevos caminos e incluso cabe la posibilidad de estar bloqueando tráfico legítimo.

Los conocidos falsos positivos permiten que un IPS realice un bloqueo tráfico legítimo, por lo que conocer el comportamiento normal de la red es recomendable para evitar problemas de bloqueo, aunque esto no es una regla conveniente para realizar pruebas de estrés que permitan analizar si el IPS bloquea tráfico legítimo.

Cabe mencionar que los sistemas detectores de intrusos han permitido investigar nuevas técnicas para detectar y mitigar ataques. Desde hace ya varios años se han desarrollado y buscado nuevas técnica que han permitido a los sistemas detectores de intrusos ser mucho más eficientes y sofisticados, entre algunas de esas técnicas se encuentra el uso de métodos distribuidos para la detección de intrusiones, detección de intrusiones basada en grafos, entre otras muchas más.

Apéndice D
Análisis de controles, políticas de uso de red y acceso a internet, encuestas aplicadas y sus resultados

I. Análisis de controles

Vulnerabilidad	Nivel de riesgo	Control sugerido
Red inalámbrica abierta.	Alto	Hotspot, servidor Radius, cifrado.
Inexistencia de controles sobre el uso de la red inalámbrica.	Alto	Hotspot, servidor Radius, cifrado.
Poco control en la administración de direcciones IP.	Alto	Inventario de gestión de direcciones IP.
Inexistencia de control en la información descargada a través de la red de la institución.	Alto	Firewall, filtrado de contenido.
Falta de cuidado del equipo de cómputo.	Alto	Concientización en temas de seguridad.
Limitantes de potencia en UPS.	Alto	Evaluación y adquisición de un UPS.
Falta de mecanismos de control perimetral de la red.	Alto	Firewall, IDS, gestor de uso de red.
Uso de protocolos de administración inseguros.	Alto	Políticas de configuración de equipos activos.
Inexistencia de políticas de uso de red.	Alto	Elaboración de políticas de uso de red.
Inexistencia de políticas para servidores.	Alto	Elaboración de políticas para servidores.
Inexistencia de respaldos en equipos activos.	Alto	Elaboración de políticas de respaldo.
Acceso a todos los recursos de red institucional.	Alto	Firewall perimetral, firewall site de servidores, vlan's, NAT's.
Uso de una misma contraseña por periodos largos de tiempo.	Alto	Políticas de contraseñas.
Uso de una contraseña única en varios equipos.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Uso de contraseñas no robustas.	Alto	Políticas de contraseñas, concientización en temas de seguridad.
Confianza en otras personas.	Alto	Concientización en temas de seguridad.
Uso de IP's homologadas para usuarios en general.	Alto	Vlan, NAT.
Fallas por parte del proveedor del suministro eléctrico.	Alto	----------
Puertos abiertos sin uso en estación de trabajo.	Alto	Políticas de hardening en estaciones de trabajo.
Inexistencia de respaldos en las diferentes Secretarías.	Medio	Políticas de respaldo.
Tableros eléctricos expuestos.	Medio	Informar de la observación a la Secretaría Administrativa.
Controles de acceso físicos, inseguros para administración de servidores.	Medio	Implementar controles biométricos en los sites.
Vulnerabilidades inherentes del protocolo TCP/IP.	Medio	Políticas de monitoreo.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Daño en hardware por fallas eléctricas.	Medio	UPS.
Inexistencia de control en el tráfico de red generado por la institución.	Medio	Gestor de uso de red.
Fuga de información.	Medio	Políticas de confidencialidad.
Daño físico a la infraestructura de red.	Medio	Cableado estructurado.
Puertos abiertos sin motivo en servidores críticos.	Medio	Políticas de hardening en servidores.
Inexistencia de controles de seguridad en portátiles.	Medio	RFID, bandas magnéticas, cintas de seguridad para portátiles.
Inexistencia de monitoreo de uso de la red.	Medio	Políticas de monitoreo.
Fallas en sistemas de aire acondicionado.	Medio	Mantenimiento preventivo.
Control de acceso débil en aplicaciones.	Medio	Políticas desarrollo de software seguro.
Personal poco capacitado en temas de seguridad.	Medio	Capacitación del personal.
Inexistencia de actualizaciones en terminales de trabajo, servidores, antivirus y equipos de red.	Medio	Políticas de hardening en estaciones de trabajo y Políticas de hardening en servidores.
Falta de mantenimiento preventivo en servidores y equipos activos.	Medio	Mantenimiento preventivo en servidores y equipo activo.
Falta de mantenimiento de estaciones eléctricas.	Medio	Mantenimiento preventivo en estaciones eléctricas.
Falta de corriente eléctrica regulada.	Medio	Implementar reguladores en la mayoría de los equipos.
Inexistencia de fuente de corriente eléctrica alterna.	Medio	Planta eléctrica.
Inexistencia de planes de capacitación.	Medio	Capacitación del personal.
Inexistencia de sites alternos.	Medio	Contratos con compañías o acuerdos con otras instituciones.
Cableado de red expuesto.	Medio	Cableado estructurado.
Respaldos en mismo disco duro.	Medio	Políticas de respaldo.
Parámetros por default en equipos activos.	Medio	Políticas de configuración de equipos activos.
Acceso a todas las terminales de administración.	Medio	Firewall perimetral, firewall Site servidores, listas de control de acceso.
Acceso a todos los recursos de internet.	Medio	Firewall, gestor de contenido.
Uso de protocolos de comunicación inseguros.	Medio	Implementación de comunicaciones cifradas.
Falta de mantenimiento en cableado eléctrico.	Medio	Mantenimiento preventivo en la institución.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Inexistencia de controles de humedad.	Medio	Sensor de humedad.
Inexistencia de controles de temperatura.	Medio	Sensor de temperatura.
Consultas de sitios con software malicioso.	Medio	Gestor de contenido, capacitación al usuario.
Descarga de ejecutables de sitios no confiables.	Medio	Gestor de contenido, capacitación al usuario.
Inexistencia de políticas sobre el uso del equipo de cómputo.	Medio	Políticas sobre el uso del equipo de cómputo.
Autoarranque de dispositivos extraíbles.	Medio	Políticas de hardening en estaciones de trabajo.
Falta de políticas de desarrollo de software seguro.	Medio	Políticas de desarrollo de software seguro.
Inexistencia de controles de integridad en equipos activos.	Medio	Memorias técnicas y respaldos de configuración.
Firmas antivirus deficientes.	Medio	Evaluación y adquisición de un antivirus.
Inexistencia de políticas de uso de software.	Medio	Políticas de hardening en estaciones de trabajo.
Poco control sobre los respaldos.	Medio	Políticas de control de cambios y políticas de respaldo.
Filtrado de agua a Sites.	Medio	Mantenimiento preventivo.
Inexistencia de controles sobre el uso de procesador, memoria, disco duro y ancho de banda.	Medio	Políticas de hardening en servidores.
Falta de procedimientos de creación de cuentas.	Medio	Políticas de contraseñas.
Vulnerabilidades inherentes a las aplicaciones.	Medio	Actualizaciones.
Tiempo de vida útil de los equipos.	Medio	Mantenimiento preventivo, renovación de hardware.
Tuberías expuestas.	Medio	Restructuración de instalación eléctrica, mantenimiento.
Uso de versiones viejas en aplicaciones.	Medio	Actualizaciones.
Vulnerabilidades conocidas en sistemas operativos.	Medio	Actualizaciones.
Empleo de software sin actualizaciones.	Medio	Actualizaciones.
Inexistencia de auditorías.	Bajo	Planificación de auditorías.
Limitantes de espacio en disco duro en servidores.	Bajo	Evaluación y adquisición de medios de almacenamiento masivo.
Fallas eléctricas.	Bajo	Mantenimiento general a la red Eléctrica.
Inexistencia de cultura de seguridad en usuarios finales.	Bajo	Capacitación del personal.
Inexistencia de control perimetral de los puertos permitidos.	Bajo	Firewall perimetral, IDS.
Inexistencia de procedimientos de cambios en sistemas.	Bajo	Políticas de control de cambios.

Vulnerabilidad	Nivel de riesgo	Control sugerido
Inexistencia de políticas en sistemas operativos.	Bajo	Políticas de hardening en estaciones de trabajo.
Inexistencia de cifrado en discos duros.	Bajo	Cifrado.
Poca separación de funciones críticas.	Bajo	Definir responsabilidades, separación de funciones.
Dispositivos extraíbles sin cifrado.	Bajo	Cifrado.
Fallas por parte del proveedor de servicios de internet.	Bajo	Enlaces redundantes, acuerdos de LSA.
Daños en la configuración de los equipos por poco mantenimiento.	Bajo	Mantenimiento preventivo.
Descuido en el manejo del hardware.	Bajo	Capacitación del personal.
Errores de cambios en la configuración de equipos activos y servidores.	Bajo	Capacitación del personal.
Inexistencia de control a servicios de servidores.	Bajo	Políticas de hardening en servidores.
Inexistencia de políticas de confidencialidad.	Bajo	Políticas de confidencialidad.
Inexistencia de monitoreo de las aplicaciones.	Bajo	Políticas de monitoreo, implementación de herramientas de monitoreo.
Poca educación sobre seguridad a usuarios finales.	Bajo	Capacitación del personal.
Errores humanos.	Bajo	Capacitación del personal.
Aprovechamiento de vulnerabilidades de controles físicos.	Bajo	Implementación de controles de acceso de 2 o más factores.
Falta de gestión de garantías.	Bajo	Adquisición de periodos de garantía más largos.
Interferencias magnéticas.	Bajo	----------
Desastres naturales en la institución.	Bajo	Prevención.

II. Políticas de uso de red y acceso a internet

Objetivo del documento

Definir los criterios normativos para implementar, preservar y hacer uso eficiente, racional y correcto de los recursos de red.

Alcance

Al utilizar la red de datos del Colegio de Ciencias y Humanidades se espera que el usuario (académico, administrativo, estudiante) use los servicios con respeto, responsabilidad.

La aplicación y seguimiento de las siguientes políticas, serán supervisadas y aplicadas por la Secretaría de Informática.

Definiciones

1. Red DGCCH: nombre dado al conjunto de instalaciones y recursos informáticos que conforman parte de la infraestructura de telecomunicaciones.
2. Usuario: Se entiende por usuario de la red, todo ente que reciba o provea información a través de la Red DGCCH.
3. Servicio: Se entiende por servicio, los aplicativos y/o conjunto de programas que apoyan la labor académica y administrativa del quehacer cotidiano de los usuarios.
4. Cuenta: Mecanismo de identificación asignado a un usuario, dicho mecanismo será personal, único e intransferible, vigente durante el tiempo de vinculación del usuario con la Institución.
5. SG: Acrónimo de Secretaría General.
6. SA: Acrónimo de Secretaría Administrativa.
7. Monitoreo: Estadísticas de uso de red y verificación de que los paquetes de datos estén formados adecuadamente.

Generalidades

La UNAM, a través de la Secretaría de Informática, encargada de cómputo y redes de datos del plantel o dirección del Colegio de Ciencias y Humanidades, brindará a la comunidad académica, administrativa y estudiantil el servicio de acceso a la red para la navegación en internet, servicios adicionales sobre la misma y consulta de correo electrónico, como un recurso de apoyo a la labor académica, de investigación, difusión cultural y actividades administrativas. Los académicos, empleados y alumnos deben emplearlos para su trabajo y estudio.

Toda persona que utilice los servicios que ofrece la red de datos de la Dirección General del Colegio de Ciencias y Humanidades deberá conocer y apegarse a las políticas vigentes de uso de red, el desconocimiento del mismo no exonera de las responsabilidades asignadas. Quedan explícitamente prohibidas todas aquellas actividades que no estén expresamente permitidas en este documento.

Emisión y modificación de normas

La Secretaría de Informática, con previa autorización de la Secretaría General, Secretaría Administrativa y Junta de directores del Colegio de Ciencias y Humanidades, tiene la facultad de crear, modificar y emitir nuevas políticas de uso de la red que son aplicables a todos los usuarios.

De la información transportada en la Red

La Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades, no controla ni es responsable del contenido y veracidad de la información que se transporta en la red, en consecuencia los usuarios aceptan utilizar el servicio de comunicación sólo para enviar y recibir mensajes e información.

El acceso al contenido publicado en internet, archivos descargados, programas ejecutados desde Internet, mensajes recibidos y demás información que pueda estar en Internet es susceptible de contener malware. Por lo anterior es responsabilidad del usuario, ingresar sólo a sitios que considere seguros.

Personal autorizado

Están autorizados a utilizar los servicios de red de la DGCCH todo el personal que se encuentre en la siguiente clasificación.

- Académicos del Colegio de Ciencias y Humanidades.
- Personal administrativo.
- Personas que presten servicios a la institución de manera directa.
- Personal de apoyo institucional.
- Administradores de servicios.
- Becarios.
- Alumnos.

Responsabilidades de los administradores de red y cómputo

Se definen como administradores de red y cómputo a:

- Secretaría de Informática para Dirección General del Colegio de Ciencias y Humanidades.
- Encargados de cómputo y telecomunicaciones definidos en cada plantel.

Dentro de sus responsabilidades se contemplan los siguientes puntos.

- Realizar y vigilar que sean cumplidas las políticas de uso de red y acceso a internet.
- Llevar un control y resguardo de los recursos informáticos del plantel o dirección general.
- La configuración y asignación de direcciones IP.
- Instalación y administración de equipos activos de red.

- Desarrollar estrategias que permitan el control de las diferentes aulas, centros de cómputo y recursos informáticos del plantel.
- Mantener en funcionamiento los servicios que les corresponde administrar, en caso de alguna falla se realizará un informe detallado del problema presentado.
- Monitoreo del tráfico de la red de datos.
- Informar a los usuarios sobre el funcionamiento y la forma como debe ser utilizado.
- Informar a los usuarios sobre cambios de la suspensión temporal y/o mantenimiento de los servicios.
- Prestación de soporte técnico en materia, de instalación, configuración y mantenimiento de los equipos de cómputo e infraestructura de red.
- Gestionar y autorizar la solicitud de dominios, subdominios en nic.unam.mx.
- Actualización de la contraseña de correo "cch.unam.mx", sólo la Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades realiza este proceso.

De los recursos

- El servicio de conexión a la red, estará disponible las 24 horas del día, los 365 días del año. Salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio de Internet.

- La infraestructura de red de la DGCCH, se utilizará únicamente para desarrollos académicos, de investigación, técnicos y administrativos de la institución, así mismo sólo podrán ser usados de acuerdo con lo previsto por las especificaciones de cada dispositivo.

- Se prohíbe, salvo autorización escrita y supervisión de la Secretaría de Informática de la DGCCH, la intervención física de los usuarios sobre los recursos de la red (cables, enlaces, equipos activos y/o pasivos) y el acceso a los centros de cableado de los edificios.

- Sólo la Secretaría de Informática de la Dirección General del Colegio de Ciencias y Humanidades, está facultado para conceder acceso a los recursos y/o servicios de la red.

- Todos los usuarios con recursos de cómputo bajo su responsabilidad, sólo harán uso de los mismos en beneficio de la institución, deberán velar por la protección física de los mismos.

- Sólo el personal debidamente autorizado por la Secretaría de Informática, podrá modificar la configuración y conexión física de los equipos de telecomunicaciones de la institución.

Usos inaceptables

Queda prohibido.

- Cambiar parámetros de red configurados en su equipo de cómputo.
- Transmisión de información de terceros, sin previa autorización de la autoridad competente.
- Transmisión de contenido pornográfico.
- Distribución no autorizada o copia de software sin licencia.

- Distribución de información de carácter comercial o cualquier otra forma, que represente un lucro para la persona que la origina.
- Distribución de material obsceno o que incite la violencia.
- Envío de correos no solicitados en un alto volumen (spam).
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Publicación de material electrónico con derechos de autor, sin previa autorización por escrito de su titular.
- Propagación de código malicioso, virus, gusanos, spyware, etcétera.
- Exploración no autorizada de los servidores.
- Acoso informático y/o electrónico a cualquier miembro o usuario de la red.
- Atacar a otros usuarios por cualquier medio (negación de servicio, phising, pharming, fuerza bruta, etcétera.).
- Atentar contra la disponibilidad, integridad, confidencialidad de la red.
- Extender el alcance de la red a más equipos por medio de cualquier dispositivo físico o lógico (NAT, túneles, switch, hub, ruteador, conexiones compartidas, etcétera.).
- Montar servidores sin previa autorización por escrito, al área de cómputo encargada de la administración de red de la Dirección General o planteles, según sea el caso.
- Utilizar los recursos de la red para juegos online.
- Transgredir cualquier recurso computacional, sistema o sitios de telecomunicaciones a los que está permitido acceder.

De los derechos y responsabilidades de los usuarios de red

- Es responsabilidad de los empleados que tengan personal a su cargo: la difusión y el apego a las políticas.
- Mantener en óptimas condiciones el equipo, accesorios y demás dispositivos de cómputo que se les haya asignado.
- Solicitar por escrito a los responsables de red, la asignación de una dirección IP y los servicios que en su caso brindará, dicho equipo.
- Reportar inmediatamente el robo o extravío de algún equipo.
- Reportar a los administradores de red, el daño de nodos de red que se encuentren localizados en su área de trabajo.
- Respetar la configuración de los equipos de cómputo que se les asignen.
- Mantener la confidencialidad de sus cuentas de acceso.
- Utilizar los recursos de red, con las limitantes consignadas en el punto de usos inaceptables.
- Es responsabilidad del usuario, el tipo de información al cual accede, ya que ésta puede ser contenido inapropiado.
- Realizar el respaldo de su información.

- Los usuarios gozan de la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la red de la DGCCH o de cualquier otra red.
- Cualquier cambio en el hardware de red en un equipo de cómputo, deberá ser notificado en un lapso no mayor a 4 días a la Secretaría de Informática.
- La Secretaría de Informática, se reserva el derecho de cancelar temporalmente o definitivamente el servicio, con previa notificación al usuario, cuando se haga uso inapropiado de la red, dentro de las actividades especificadas en usos inapropiados.

Monitoreo de comunicaciones

A solicitud escrita de la autoridad competente o cuando exista alguna orden judicial para responder ante procesos legales, la Secretaría de Informática proporcionará la información transmitida en la Dirección General del Colegio de Ciencias y Humanidades y que esté disponible para su acceso de conformidad con las leyes aplicables.

El usuario al momento de utilizar la red de la Dirección General del Colegio de Ciencias y Humanidades, conoce y manifiesta su consentimiento para que la Secretaría de Informática realice monitoreo en su conexión, cuando lo juzgue necesario, únicamente con el propósito de mantener la integridad y operación efectiva de los equipos de telecomunicaciones o cuando responda a un requerimiento de las autoridades administrativas o judiciales.

III. Encuesta administradores

ANÁLISIS DE RIESGO CON BASE EN EL NIST 800-30, 800-53
ADMINISTRADORES

Institución	Dirección General del Colegio de Ciencias y Humanidades
Nombre:	
Secretaría a la que pertenece:	
Fecha	Firma

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Controles de Seguridad

1. Se tiene definidas políticas de confidencialidad, para la información que maneja.
   SÍ ☐ NO ☐
2. Conoce si existen dispositivos de seguridad y monitoreo de la red en su institución, si su respuesta es afirmativa indique los elementos que identifica.
   SÍ ☐ NO ☐
3. Se tienen definidas políticas de respaldos en los equipos que administra, si la respuesta es afirmativa indique la frecuencia de respaldo.
   SÍ ☐ NO ☐
4. En los dispositivos que administra, aplica algún esquema de políticas de seguridad, si la respuesta es afirmativa indique qué puntos cubre.
   SÍ ☐ NO ☐
5. Cuenta la institución con un documento oficial de Políticas y Procedimientos de Seguridad de la Información.
   SÍ ☐ NO ☐
6. En caso de existir un documento de políticas de seguridad, indique cuáles de los siguientes aspectos hacen parte de su contenido:

Descripción	SÍ	NO
Objetivos de las políticas		
Normas y políticas a ser implementadas		
Definición de responsabilidades en la gestión de la seguridad		
El manejo de los incidentes relacionados con la seguridad de la información		
Referencias a la información que soporte las políticas de seguridad		

7. En caso de existir un documento de políticas de seguridad, el mismo ha sido publicado y comunicado a todos los empleados y contratistas de la institución.

SÍ		NO	

Organización de la Seguridad

8. Existe en la institución una estructura de personal y recursos que permita la implementación y control de las políticas de seguridad de la información.

SÍ		NO	

Gestión de Activos de Información

9. Existe en la institución un inventario detallado de activos que incluya la información del activo, como tipo de activo, ubicación, formato, información de soporte y mantenimiento, licencias y valor para el negocio, su responsable o dueño designado, etcétera.

SÍ		NO	

10. Si la respuesta a la pregunta No. 1 fue un "SÍ", se tiene una clasificación de activos con base en la necesidad, las prioridades y el grado esperado de protección del activo de información.

SÍ		NO	

Seguridad de los Recursos Humanos

11. Se han revisado todas las posiciones y cargos en función de las responsabilidades en materia de seguridad de la información.

SÍ		NO	

12. Existen documentos tales como manuales de procedimientos que reflejen de manera precisa los roles y responsabilidades para cada cargo.

SÍ		NO	

13. Las tareas críticas y más sensibles son distribuidas entre varios funcionarios.

SÍ		NO	

14. Existen procedimientos escritos para la contratación, transferencia y terminación de contratos de funcionarios.

SÍ		NO	

15. Se han firmado acuerdos o contratos de confidencialidad con todos los funcionarios y contratistas que manejan información sensible.

SÍ		NO	

Seguridad Física y del Entorno

16. El acceso a las instalaciones que albergan información vital, tales como Centros de Cómputo, site de servidores y bodegas de cintas, es controlado y restringido por guardias de seguridad, tarjetas de proximidad, claves de acceso o controles biométricos de acceso, o algún otro, indique cual.

SÍ		NO	

17. Las instalaciones que albergan información vital, cuentan con controles de adecuados, tales como muros, y puertas con seguridad.

SÍ		NO	

18. Las claves de acceso son revisadas y cambiadas con una periodicidad determinada, si la respuesta es afirmativa indique la frecuencia de cambio.

SÍ		NO	

19. Existen procedimientos de revisión periódica de las listas de personal con acceso a instalaciones que albergan información vital.

SÍ		NO	

20. Los visitantes a las áreas que albergan información vital son registrados y escoltados.

SÍ		NO	

21. Los sistemas de detección y extinción de incendios se encuentran correctamente instalados y en operación.

SÍ		NO	

22. Los sistemas de Aire Acondicionado se encuentran correctamente instalados y en operación.

SÍ		NO	

23. Cuenta la institución con un sistema de suministro no interrumpido de potencia o UPS (Uninterruptible Power Supply) que respalde la totalidad de equipos de cómputo, servidores y equipos de comunicaciones de la institución.

SÍ		NO		Parcialmente	

24. Los monitores de los equipos de cómputo están localizados para evitar el acceso y visualización de personas no autorizadas.

SÍ		NO	

25. Los sistemas de cableado estructurado y eléctrico están protegidos contra interceptaciones y daños.

SÍ		NO	

Gestión de Operaciones y Comunicaciones

26. Existe un procedimiento de control de cambios a nivel de los sistemas de procesamiento de información.

SÍ		NO	

27. Se tienen claramente definidos y separados, ambientes de desarrollo, ensayo y operación para los sistemas de procesamiento de información.

SÍ		NO	

28. Se hace la planeación de capacidad para los sistemas de procesamiento de información.

SÍ		NO	

29. Se tiene implementado un sistema de protección contra código malicioso que cubra la totalidad de activos de información.

SÍ		NO	

30. Se tienen implementados sistemas y procedimientos de respaldo o backup para los sistemas que usted administra.

SÍ		NO	

31. Para controlar la seguridad de la red, se tienen implementados sistemas de autenticación.

SÍ		NO	

32. Para controlar la privacidad de la información de la red, se tienen implementados sistemas de cifrado.

SÍ		NO	

33. Existe en los equipos que administra firewall de host. Por favor indique la cantidad.

SÍ		NO		Cantidad	

34. Existe en su institución firewall perimetral. Por favor indique la cantidad existente.

SÍ		NO		Cantidad	

35. Especifique el tipo de tecnología utilizada por el(los) firewall(s).

Firewall basado en hardware dedicado	
Firewall basado en software para Servidor	

36. Marque con una “X” las redes protegidas mediante puertos independientes en el(los) firewall(s) de su institución.

Host	
Red LAN	
Red WAN	
Extranet	
DMZ	

37. Cuenta su institución con Sistemas de Detección de intrusos – IDS.

SÍ		NO	

38. Cuenta su institución con equipos de monitoreo de red, si su respuesta fue afirmativa indique qué dispositivos.

SÍ		NO	

39. Se realiza bloqueo de algunos sitios en el segmento de red.

SÍ		NO	

40. Cuenta su institución con equipos concentradores de VPN´s

SÍ		NO	

Control de Acceso

41. Existen sistemas de control capaces de detectar intentos de acceso no autorizados.

SÍ		NO	

42. Las estaciones de trabajo se desconectan o los salva pantallas protegidos por contraseña se activan después de un periodo determinado de inactividad.

SÍ		NO	

43. Las cuentas de usuario no activas son removidas cuando no se requieren.

SÍ		NO	

44. Si se manejan sistemas de cifrado, existen procedimientos para generación de claves, almacenamiento, uso y destrucción de las mismas.

SÍ		NO	

45. Los parámetros por defecto suministrados por los fabricantes han sido cambiados por parámetros de configuración más seguros.

SÍ		NO	

46. Existen procedimientos para mantener y revisar los logs de actividad de red.

SÍ		NO	

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

47. Para la adquisición de infraestructura de hardware y software, se realizan documentos detallados de especificaciones técnicas.

SÍ		NO	

48. Se tiene un procedimiento de control de versiones.

SÍ		NO	

49. Se tienen restricciones en sitio para quienes realizan actividades de mantenimiento y reparación.

SÍ		NO	

Gestión de Incidentes de Seguridad

50. Existe un procedimiento para el reporte de incidentes de seguridad.

SÍ		NO	

51. Existe un procedimiento de seguimiento y control de los incidentes de seguridad hasta que los mismos son resueltos.

SÍ		NO	

52. La institución cuenta con personal entrenado para identificar y resolver incidentes de seguridad.

SÍ		NO	

53. La institución cuenta con un plan de continuidad, contingencia y recuperación ante desastres.

SÍ		NO	

54. El plan de continuidad es revisado y probado periódicamente.

SÍ		NO	

55. El plan de continuidad de la institución tiene en cuenta los aspectos relacionados con la seguridad de la información.

SÍ		NO	

Gestión y Procedimientos

Documentación

A nivel de seguridad de la información, existe en su institución documentación de:
Marque con una “X”, en caso de existir.

Documento de políticas, normas y procedimientos de seguridad de la Información.	
Documento de evaluación y análisis de riesgos.	
Diagramas de topología de seguridad perimetral.	
Reglas de seguridad.	

¿Cuál es el porcentaje de actualización de la documentación de seguridad de la información en su institución? Marque con “X” su elección.

Porcentaje de actualización de la documentación	Menos de 25%	Entre 25% y 50%	Entre 50% y 80%	Más de 80%
Documento de políticas, normas y procedimientos de seguridad de la Información.				
Documento de evaluación y análisis de riesgos.				
Diagramas de topología de seguridad perimetral.				
Reglas de seguridad.				

¿Cuáles de las siguientes actividades relacionadas con el Sistema de Gestión de Seguridad de la información se realizan en su institución? En caso de indicar que sí se lleva a cabo la actividad, marque con "X" en el campo que más se asemeje a su periodicidad.

Ítem	Actividades	¿Esta actividad se ejecuta actualmente en su institución? (SÍ / NO)	Periodicidad				
			Diario	Mensual	Trimestral	Semestral	Anual
Actividades de operación y configuración							
3.1	Monitoreo de equipos de seguridad Firewalls.						
3.2	Monitoreo de equipos de seguridad sistemas de detección de intrusos.						
3.3	Cambios en la configuración de los equipos de seguridad.						
Actividades de soporte técnico y mantenimiento							
3.4	Monitoreo y gestión de incidentes de seguridad.						
3.5	Generación de reportes de incidentes de seguridad.						
3.6	Mantenimiento preventivo de equipos de seguridad.						
3.7	Mantenimiento correctivo (reparaciones y arreglos) de equipos de seguridad.						
3.8	Administración de garantías) de equipos de seguridad.						
3.9	Gestión de inventarios de activos de información.						
Actividades de medición y análisis							
3.10	Medición y control de incidentes de seguridad.						
3.11	Monitoreo y revisión de logs de seguridad.						
3.12	Revisión del cumplimiento de las políticas de seguridad.						
3.13	Auditoría del Sistema de Gestión de Seguridad de la Información.						

Ítem	Actividades	¿Esta actividad se ejecuta actualmente en su institución? (SÍ / NO)	Periodicidad				
Actividades de planeación							
3.14	Evaluación y revisión del plan de tratamiento de riesgos.						
3.15	Definición y revisión del plan de continuidad de la organización.						
Actividades de capacitación y entrenamiento							
3.16	Entrenamiento para el personal en la operación del sistema de gestión de seguridad.						
Gestión de Servicios							
3.17	Proceso de gestión de incidentes y mesa de ayuda.						
3.18	Proceso de gestión de problemas.						
3.19	Proceso de gestión de configuraciones, cambios y liberaciones.						
3.20	Gestión de niveles de servicio.						
3.21	Medición del factor de calidad del servicio.						

Indique las herramientas con las que su institución cuenta actualmente para realizar las actividades de gestión de seguridad de información.

	Herramienta utilizada
Monitoreo de incidentes de seguridad.	
Administración y configuración de equipos de seguridad.	
Gestión de inventario de activos.	

Identificación de servidores

Si es responsable de algún servidor o servidores favor de llenar la siguiente tabla con los datos correspondientes.

	Servidor 1	Servidor 2	Servidor 3
Dirección IP			
Sistema operativo			
Servicios			
Puertos			
Nombre del Host			
Cuenta con memoria técnicas Sí o No			
Frecuencia con la que realiza los ~~de~~ respaldos			
Considera que su equipo es seguro Sí o No			
Conoce el término hardening Sí o No			
Qué controles aplica para garantizar un nivel de seguridad			

IV. Encuesta usuarios

ANÁLISIS DE RIESGO CON BASE EN EL NIST 800-30, 800-53
USUARIO

Entidad	Dirección General del Colegio de Ciencias y Humanidades	
Nombre:		
Secretaría a la que pertenece:		
Fecha:		Firma

I. Identificación y evaluación de activos

1. Describa las principales actividades que realiza.

2. Definir los principales activos con los que se cuenta; entendiendo como un activo aquello que tiene valor para el departamento y que requiere protección.

	Activos
Hardware (equipo de cómputo físico)	
Software (aplicaciones para realizar su trabajo)	
Sistemas (aplicaciones adicionales)	
Datos e Información	
Personal	

Con base en los activos citados anteriormente indicar el grado de importancia (valor), mediante una X. (En caso de requerirlo anexe una hoja para sus repuestas)

ACTIVOS	Muy importante	Importante	Medianamente importante	Sin importancia

3. Cuál es la forma de almacenamiento para la información manipulada por su departamento. Enumérela con base en el orden de uso. (En caso de emplear otras formas mencione y escriba brevemente).

- ☐ Disco duro.
- ☐ Archivero.
- ☐ CD, DVD, Blue Ray.
- ☐ Diskette.
- ☐ Cintas magnéticas.
- ☐ Cuarto especial para almacenar información.
- ☐ USB.
- ☐ Otro:_____

4. Considera que los medios de almacenamiento para la información, implementados en el departamento son seguros. Justifique su respuesta.

SÍ ☐ NO ☐ Parcialmente ☐

II. Identificación y descripción de amenazas

1. La gente con quién labora, tiene conocimientos acerca de los temas relacionados con la seguridad de la información.

SÍ ☐ NO ☐ Parcialmente ☐

2. Indique con qué frecuencia se presentan las siguientes situaciones marcando con una “X”, la situación que más se acerque a la realidad de su organización. (En caso de presentarse suceso diferente a los listados en la siguiente tabla, mencione y describa brevemente).

Suceso	Muy probable	Probable	Poco probable	Probabilidad nula
Robo de información.				
Ex empleados que hayan tenido acceso a la información sin autorización.				
Extravío de información por descuido del personal que la manipula.				
Alteración de información por personal no autorizado.				
Fallas en los dispositivos donde almacene información.				
Lentitud en la respuesta cuando se trabaja con la red.				
Denegación de los servicios brindados por la RED implementada en la institución.				
Falta de mantenimiento en el cableado de red.				
Desastres naturales que dañen equipo de la institución.				
Personal ajeno al departamento que haya intentado recabar información por medio del personal que labora dentro de su departamento.				
Infección de los equipos de cómputo (virus, gusanos, spyware, malware en general).				
Modificación en la configuración de red de sus equipos, por terceros.				
Fallas en los equipos de cómputo.				
Fallas eléctricas.				
Robo de equipos de cómputo, que contenga información de la institución.				
Acceso no autorizado a la información.				
Revelación de información confidencial por el personal que lo manipula.				
Copias no autorizadas de la información.				
Desconfiguración del sistema o de los dispositivos con los cuales se manipula la información.				
Personas que hayan aceptado un soborno y brindado información confidencial.				
Accidentes por desconocer las políticas de seguridad o (inexistencia de políticas).				
Falta de conocimiento técnicos para realizar alguna tarea.				
Otros.				

3. Si se presentaran cualquiera de las situaciones anteriores, qué sucedería en el departamento.

4. ¿Se cuenta con algún método de control de acceso a la información? Describa brevemente en qué consiste.

Password ☐ Tarjeta electrónica ☐ Certificados electrónicos ☐
Cerradura ☐ No ☐ No sé ☐ Cifrado ☐

III. Identificación y descripción de vulnerabilidades

1. Existen procedimientos establecidos que indiquen como realizar un respaldo de información en su área.

SÍ		NO		NO SÉ	

2. Se cuenta con respaldo de la información.

SÍ		NO		NO SÉ	

3. Dispositivos empleados para llevar a cabo el respaldo de la información (Puede seleccionarse más de una opción), en caso de tener otro tipo mencione y describa brevemente) enumere de mayor a menor, en caso de no utilizar colocar 0.

☐	Cintas magnéticas.	
☐	Folder -> (Archivero).	
☐	CD, DVD, Blue Ray.	
☐	Diskette.	
☐	Discos duros.	
☐	USB.	
☐	Otro.	

4. La información contenida en su equipo de cómputo está protegida con contraseña.

SÍ		NO		NO SÉ	

5. la información contenida en su equipo de cómputo se encuentra cifrada (emplea dos contraseñas para iniciar sesión en su equipo).

SÍ		NO		NO SÉ	

6. Las contraseñas que emplea son cambiadas con una periodicidad determinada.

SÍ		NO		NO SÉ	

7. El personal que ingresa a la institución se identifica al ingresar a la misma.

SÍ		NO		NO SÉ	

8. Existen bitácoras del personal que ingresa al a institución.

SÍ		NO		NO SÉ	

9. Se cuenta con antivirus actualizados en los equipos de cómputo.

SÍ		NO		NO SÉ	

10. Se realizan actualizaciones del sistema operativo en su equipo de cómputo.

SÍ		NO		NO SÉ	

11. Se cuenta con corriente eléctrica regulada en la instalación.

SÍ		NO		NO SÉ	

12. Se cuenta con "no break" para el cuidado de los equipos.

SÍ		NO		NO SÉ	

13. Se da mantenimiento preventivo a los equipos de cómputo a su cargo.

SÍ		NO		NO SÉ	

14. Las instalaciones están en condiciones adecuadas para el resguardo del equipo y de la información. En caso de responder NO especificar las problemáticas que tienen las instalaciones.

SÍ		NO		NO SÉ	

15. Con qué frecuencia se va la luz dentro del departamento. Indique el número de veces al mes (aproximado).

SÍ		NO	

16. Se cuenta con políticas de uso de red para la institución.

SÍ		NO		NO SÉ	

17. Se cuentan con políticas de seguridad particulares para su departamento.

SÍ		NO		NO SÉ	

18. Se cuentan con chapas que resguarden la seguridad de las oficinas que integran el departamento.

SÍ		NO		NO SÉ	

19. Se cuentan con extinguidores para incendios.

SÍ		NO		NO SÉ	

20. Al instalar o emplear un equipo nuevo, se leen los manuales adjuntos al equipo.

21. Considera adecuada la administración de la RED implementada, en caso de ser negativa la respuesta, describir cuál es la problemática que se tiene con la administración de la red.

SÍ		NO	

22. Se permite el acceso a cualquier persona a su departamento.

SÍ		NO	

23. Cómo se controla el acceso de personas dentro del departamento.

24. Se cuenta con pararrayos en la estructura física de la institución.

SÍ		NO		NO SÉ	

25. Existe filtrado de agua en su departamento, si la respuesta es "sí" indique el lugar.

SÍ		NO		NO SÉ	

26. En caso de un temblor, ¿Cómo se puede recuperar la información, cuando se haya dañado el edificio?

_____

27. Se cuenta con algún mecanismo de autenticación en la red inalámbrica de su institución.

SÍ		NO		NO SÉ	

28. Conoce si existen herramientas implementadas en la institución que garanticen o aumenten la seguridad de su equipo de cómputo.

SÍ		NO		NO SÉ	

29. Conoce si existe monitoreo de la seguridad de su red, en caso de ser "sí" su respuesta coloque el nombre del mecanismo que conoce.

SÍ		NO		NO SÉ	

IV. Identificación de controles

1. Cuando la información ha sufrido un ataque, qué consecuencias se han presentado. Enumérelas en orden de mayor (4) a menor (1) frecuencia de haber ocurrido:

Situación	Ocurrencia
La información es accedida por usuarios no autorizados.	
Se han realizado modificaciones de la información del departamento y esta información ha perdido su estado original.	
Se ha perdido de forma irreparable la información debido al ataque y no se pudo recuperar.	
Debido al ataque se han perdido temporalmente los servicios.	

2. Qué medidas ha tomado usted para el control de la seguridad en el área donde labora (Describa brevemente su área y sus funciones en ella).

3. Conoce qué medidas ha tomado el administrador de la RED del departamento para la protección de la seguridad de la institución.

4. La institución cuenta con controles de acceso físicos a los equipos de cómputo y elementos de red.

SÍ ☐ NO ☐ CUÁLES:_____

V. DETERMINACIÓN DE RIESGOS RESIDUALES

1. Considera necesario e importante el contar con respaldos de la información que maneja su departamento.

SÍ ☐ NO ☐ NO SÉ ☐

2. Realiza respaldo de la información que maneja.

SÍ ☐ NO ☐

Con qué frecuencia:_____

3. Tiene conocimiento de la existencia de programas antivirus, si su respuesta a la pregunta anterior fue afirmativa cual conoce.

SÍ ☐ NO ☐ NO SÉ ☐

4. ¿Cuenta con nombre de usuario y contraseña para ingresar al equipo?

SÍ ☐ NO ☐

5. Usted puede instalar cualquier programa en su equipo sin restricción alguna.

SÍ ☐ NO ☐ NO SÉ ☐

6. ¿Qué sistema operativo maneja en su equipo de cómputo?

Windows XP ☐ UNIX ☐
Windows 2000 ☐ Linux ☐
Windows Vista ☐ Otro:_____
Windows 7 ☐
Windows server 2003 ☐
Windows server 2008 ☐

7. Cuenta el equipo que maneja con un firewall personal:

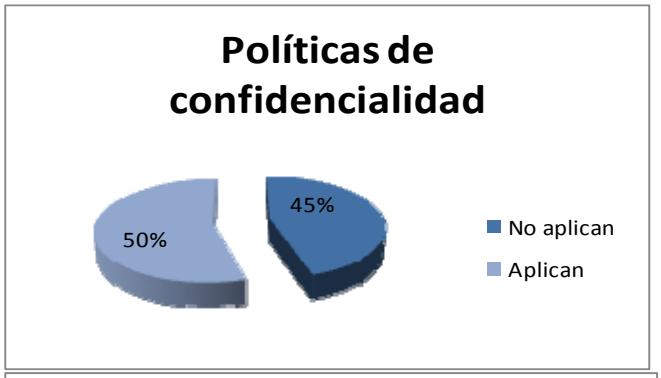
SÍ ☐ NO ☐ NO SÉ ☐

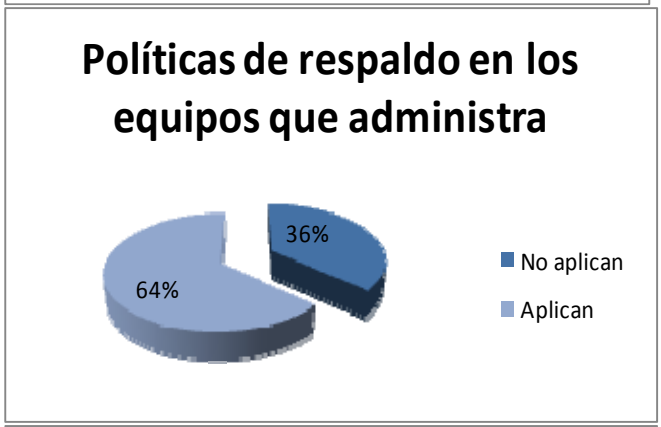
8. Aplica las actualizaciones que se liberan para sus aplicaciones y sistema operativo.

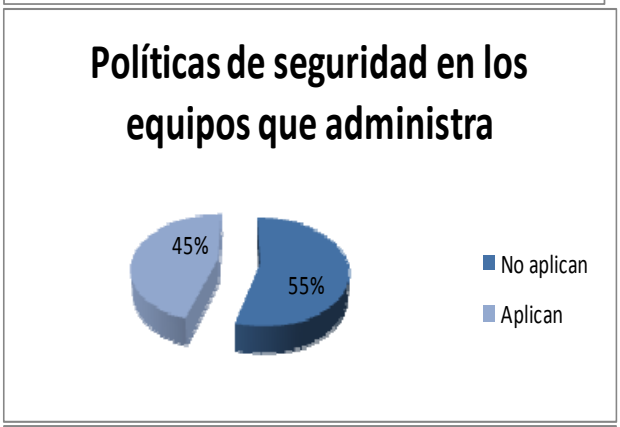
SÍ ☐ NO ☐ Parcialmente ☐

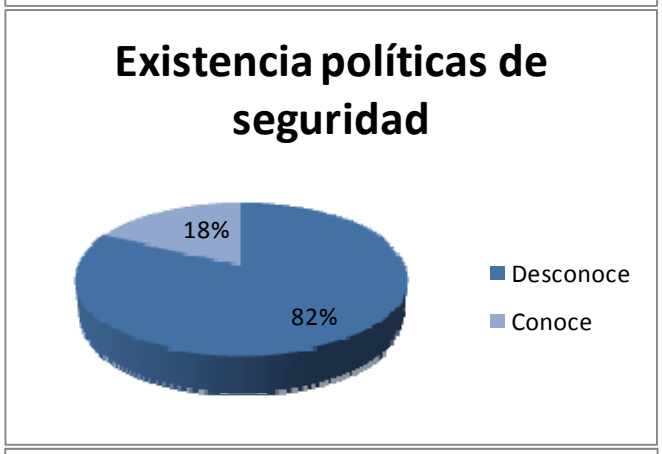
9. ¿Qué tipo de uso le da a Internet?

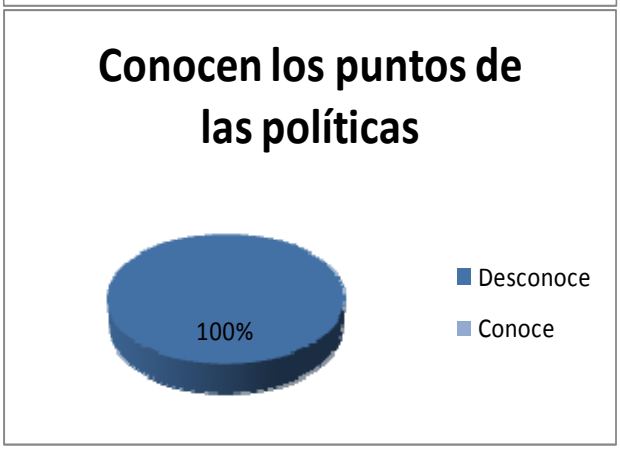
V Resultados encuestas administradores

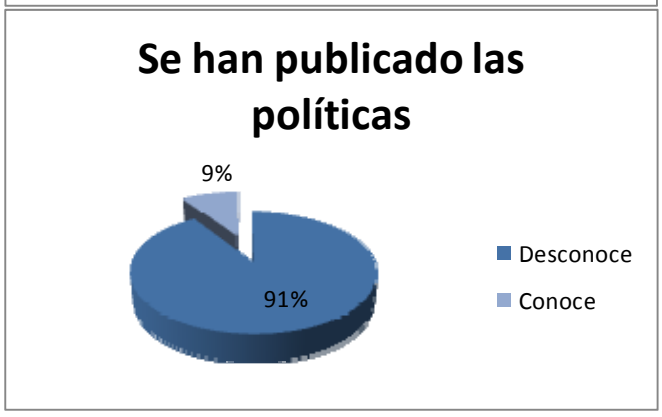


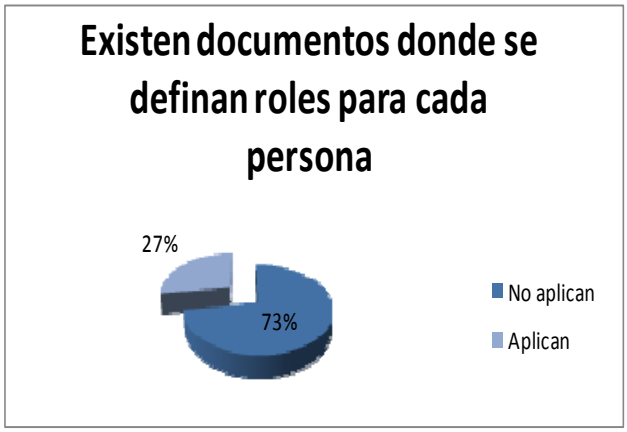


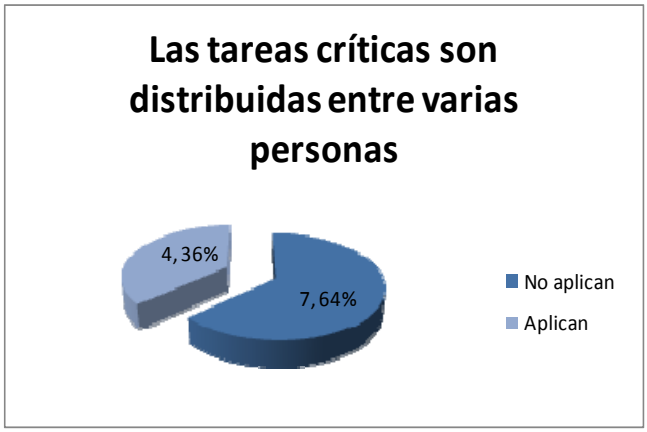


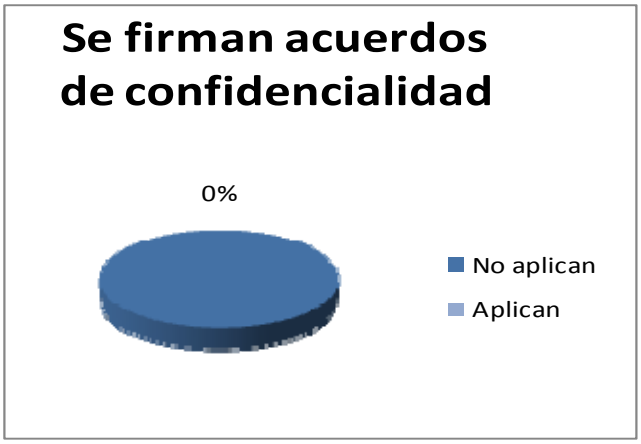




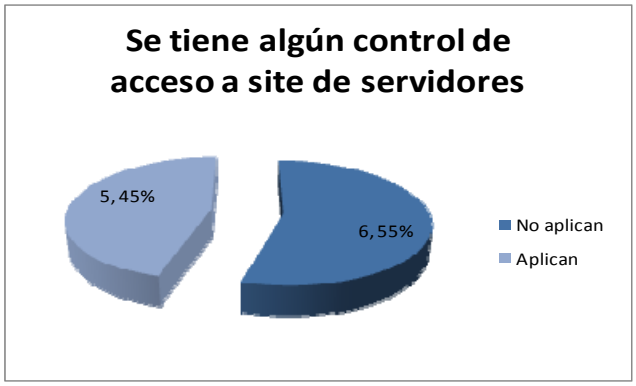






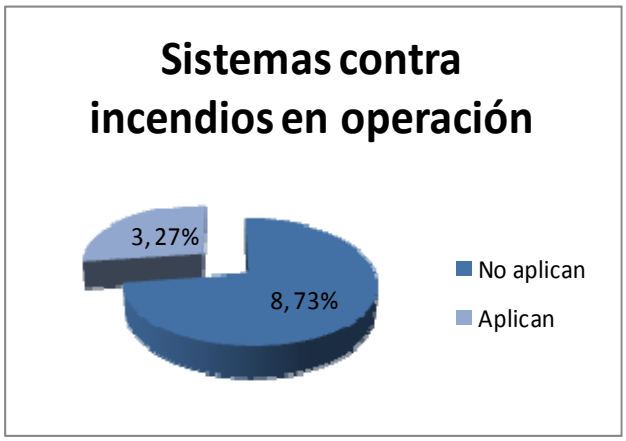


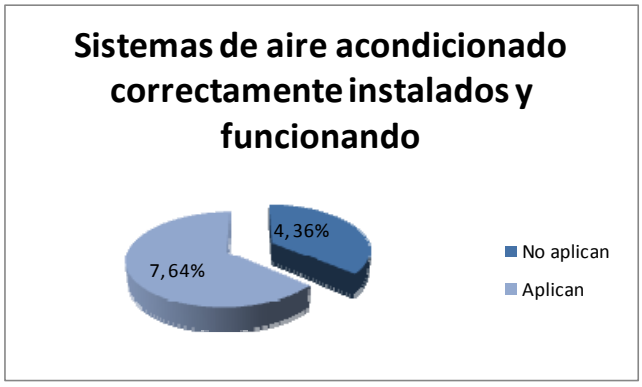
Nota: "0%" del personal firma acuerdos de confidencialidad

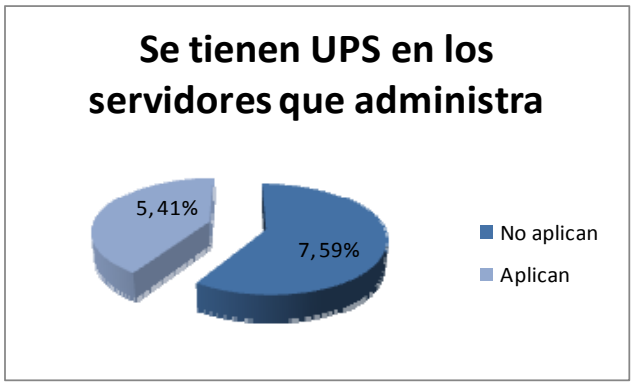

Se tiene algún control de acceso a site de servidores
5, 45%
6, 55%
No aplican
Aplican


Se tienen muros y puertas de seguridad
2, 18%
9, 82%
No aplican
Aplican

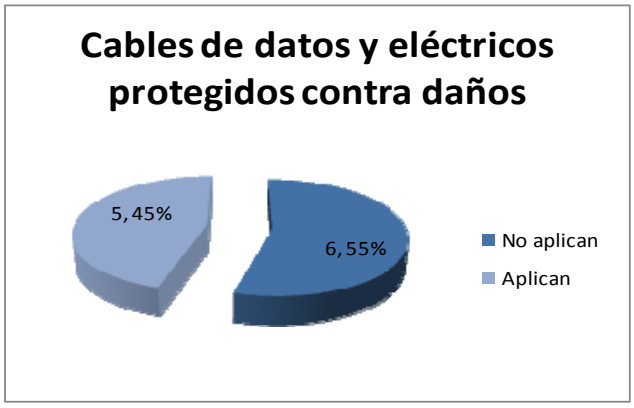

Los visitantes son registrados y escoltados
1, 9%
10, 91%
No aplican
Aplican

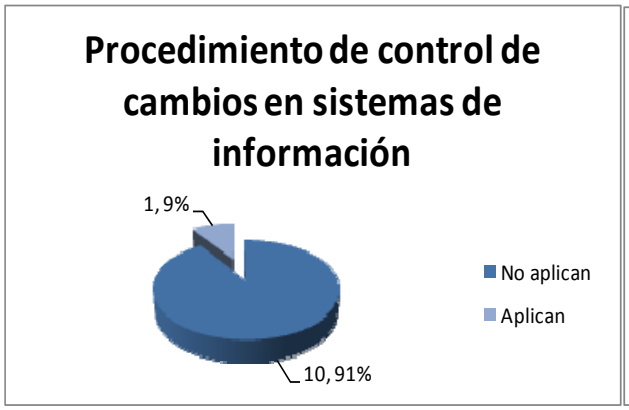

Sistemas contra incendios en operación
3, 27%
8, 73%
No aplican
Aplican

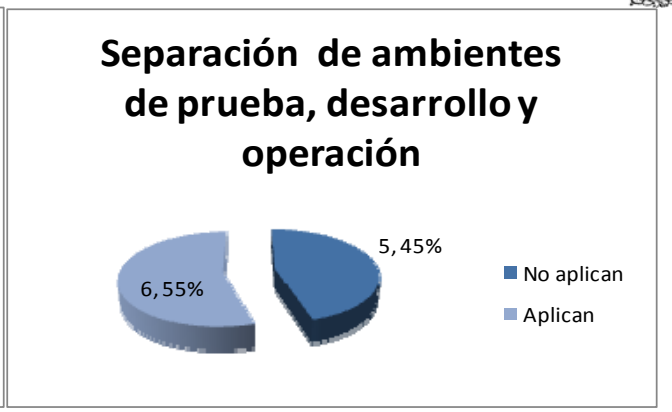

Sistemas de aire acondicionado correctamente instalados y funcionando
4, 36%
7, 64%
No aplican
Aplican

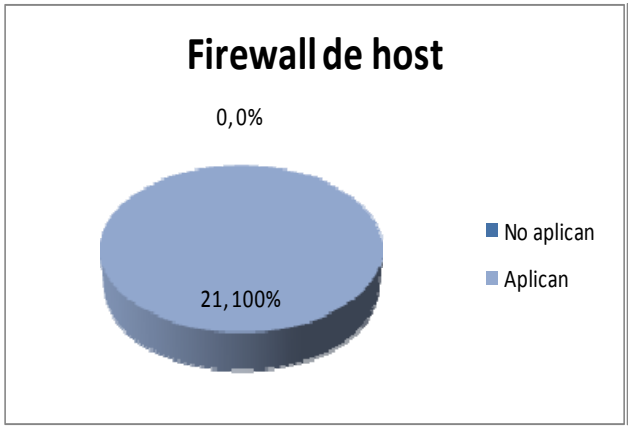

Se tienen UPS en los servidores que administra
5, 41%
7, 59%
No aplican
Aplican

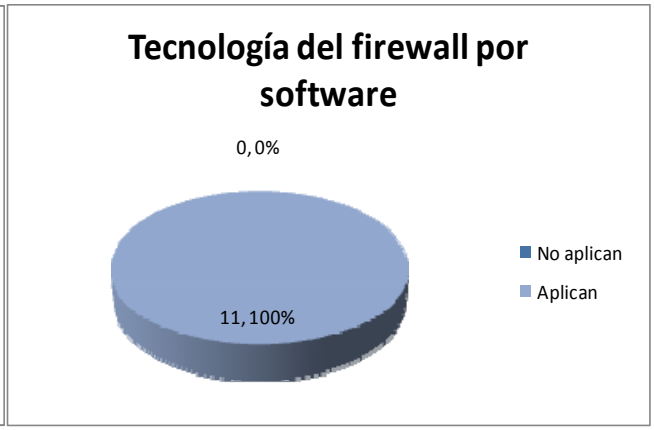

Existe un documento que contega el personal con acceso a sites vitales
2, 18%
9, 82%
No aplican
Aplican

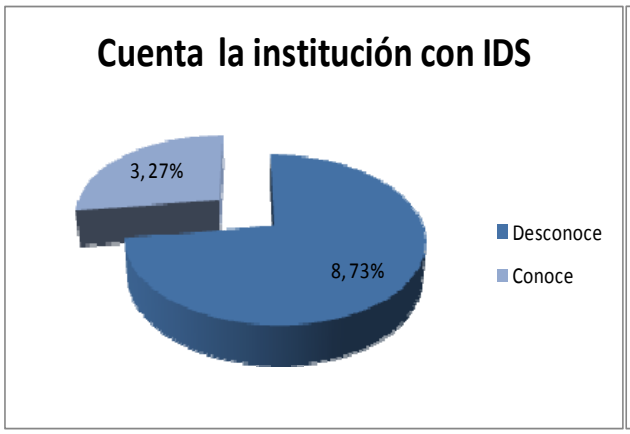

Cables de datos y eléctricos protegidos contra daños
5, 45%
6, 55%
No aplican
Aplican

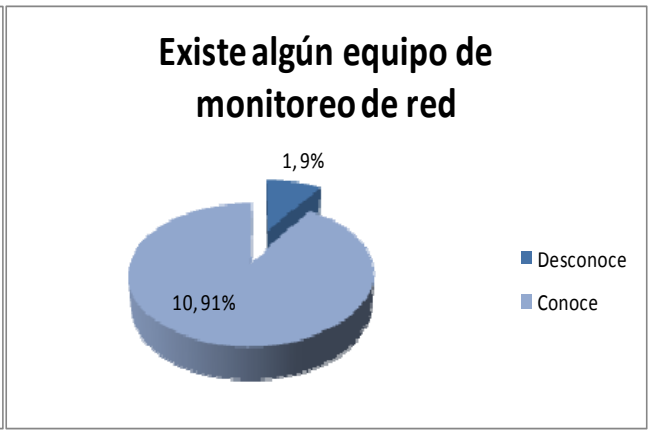

Procedimiento de control de cambios en sistemas de información
1, 9%
10, 91%
No aplican
Aplican

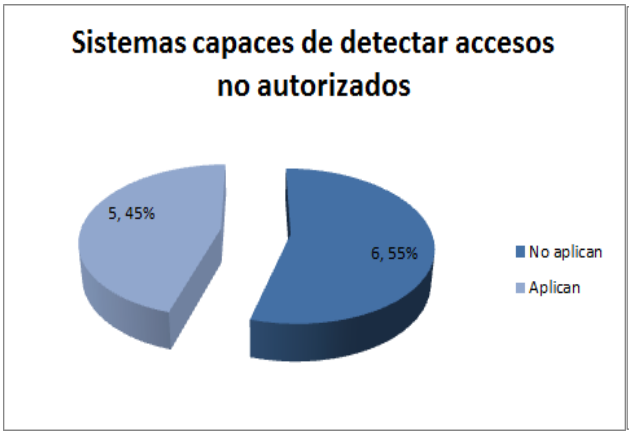

Separación de ambientes de prueba, desarrollo y operación
5, 45%
6, 55%
No aplican
Aplican

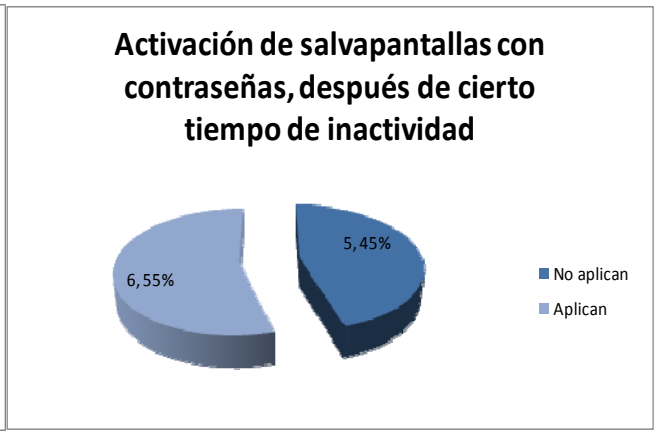

Firewall de host
0, 0%
21, 100%
No aplican
Aplican

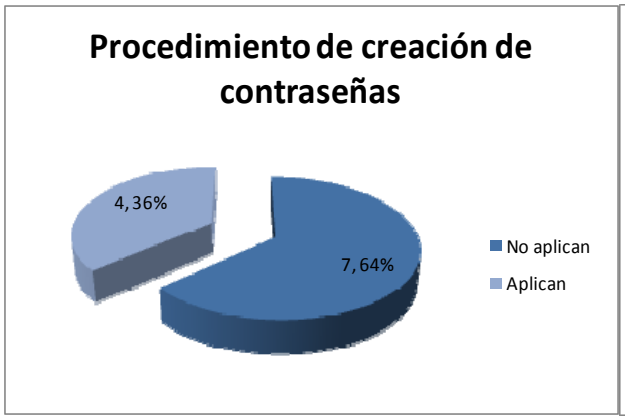

Tecnología del firewall por software
0, 0%
11, 100%
No aplican
Aplican

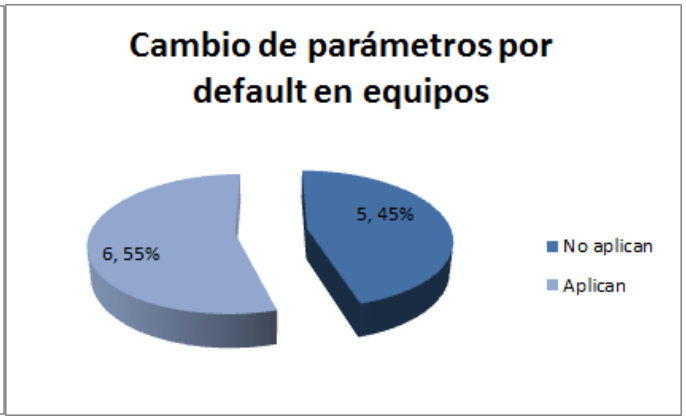

Cuenta la institución con IDS
3, 27%
8, 73%
Desconoce
Conoce


Existe algún equipo de monitoreo de red
1, 9%
10, 91%
Desconoce
Conoce

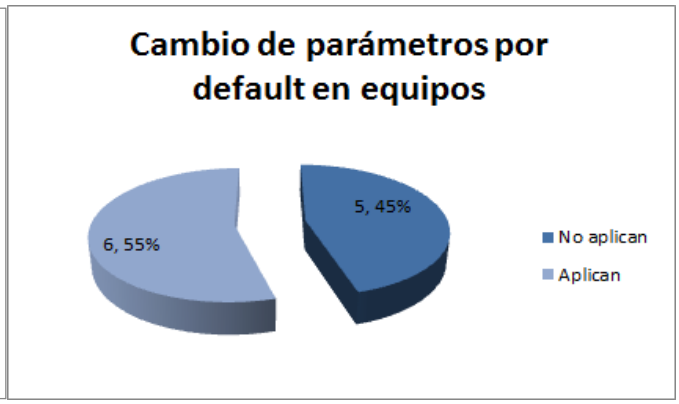

Sistemas capaces de detectar accesos no autorizados
5, 45%
6, 55%
No aplican
Aplican

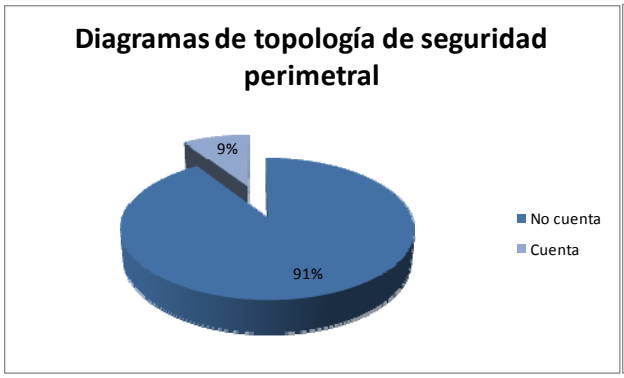

Activación de salvapantallas con contraseñas, después de cierto tiempo de inactividad
5, 45%
6, 55%
No aplican
Aplican


Procedimiento de creación de contraseñas
4,36%
7,64%
No aplican
Aplican


Cambio de parámetros por default en equipos
6, 55%
5, 45%
No aplican
Aplican

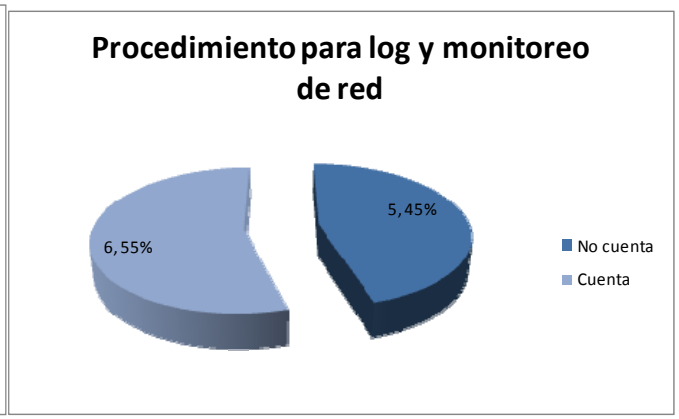

Existencia de políticas, normas y procedimientos de seguridad de la información
2
9,82%
Desconoce
Conoce


Cambio de parámetros por default en equipos
6, 55%
5, 45%
No aplican
Aplican

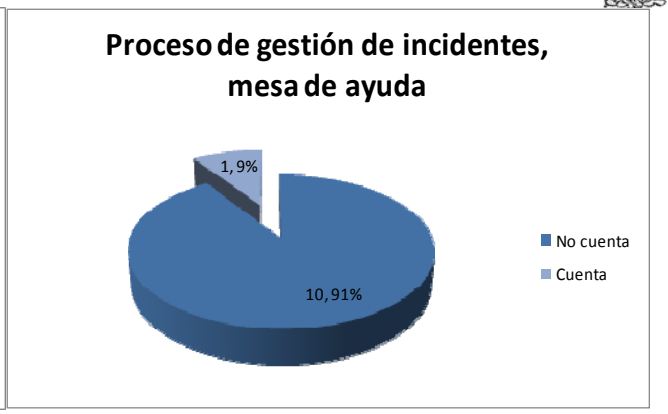

Diagramas de topología de seguridad perimetral
9%
91%
No cuenta
Cuenta

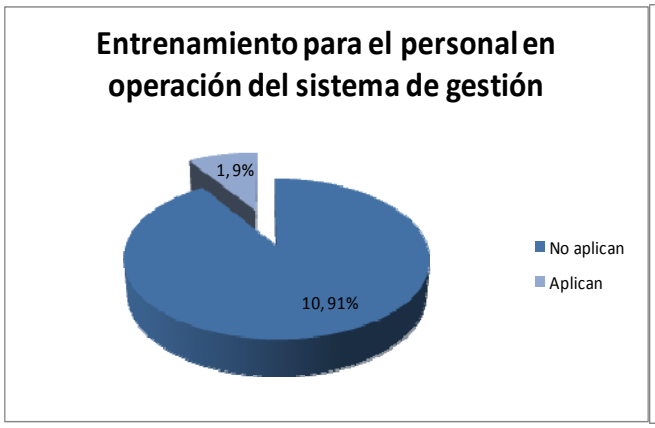

Personal entrenado para identificar y resolver incidentes
3,27%
8,73%
Desconoce
Conoce


Existe plan de continuidad, contingencia y recuperación ante desastres
2,18%
9,82%
No cuenta
Cuenta

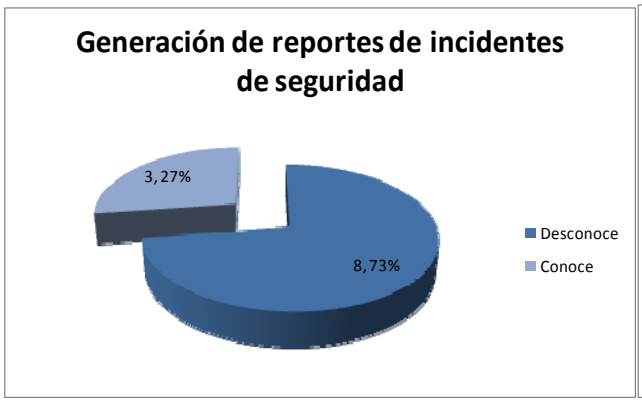

Procedimiento para log y monitoreo de red
6,55%
5,45%
No cuenta
Cuenta

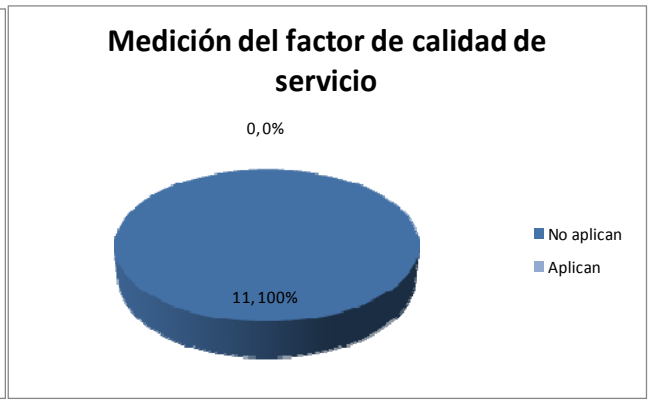

El plan de continuidad tiene contemplado aspectos de seguridad
11, 100%
0, 0%
No aplican
Aplican

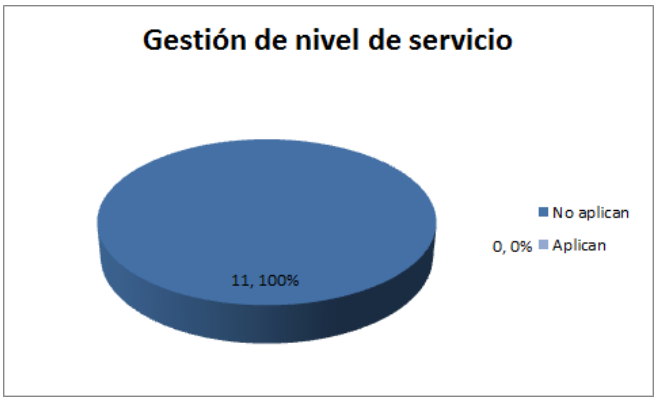

Proceso de gestión de incidentes, mesa de ayuda
1, 9%
10, 91%
No cuenta
Cuenta


Entrenamiento para el personal en operación del sistema de gestión
1, 9%
10, 91%
No aplican
Aplican

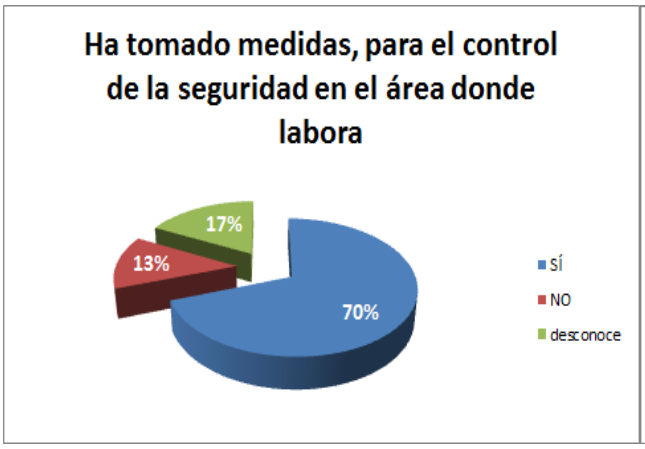

Se realiza auditoría del sistema de gestión de seguridad
No aplican
Aplican
0, 0%
11, 100%

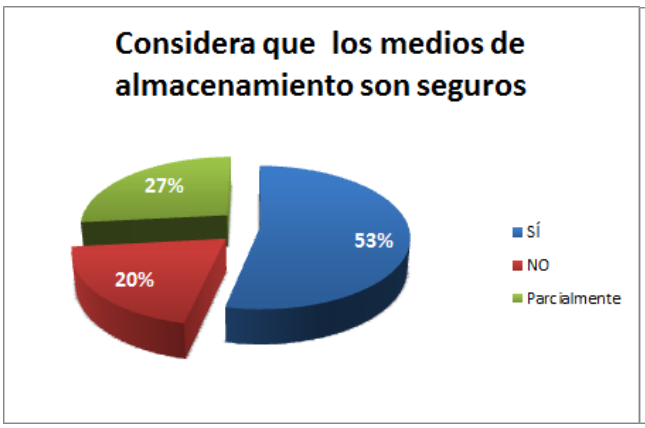

Generación de reportes de incidentes de seguridad
3, 27%
8, 73%
Desconoce
Conoce

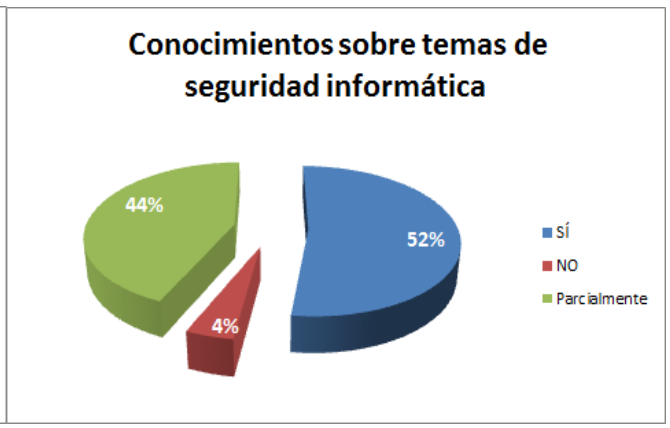

Medición del factor de calidad de servicio
0, 0%
11, 100%
No aplican
Aplican

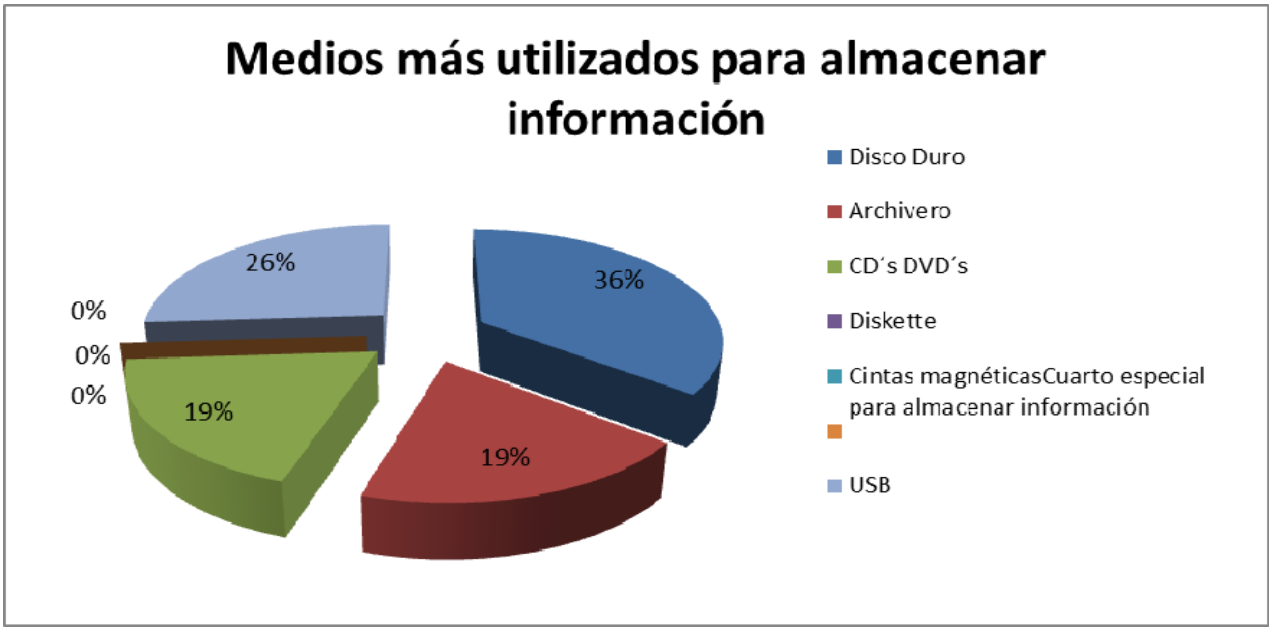

Gestión de nivel de servicio
11, 100%
0, 0%
No aplican
Aplican

IV Resultados encuestas usuarios

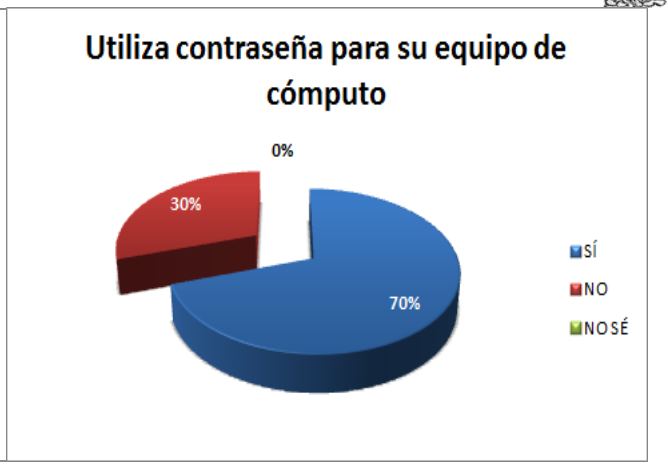


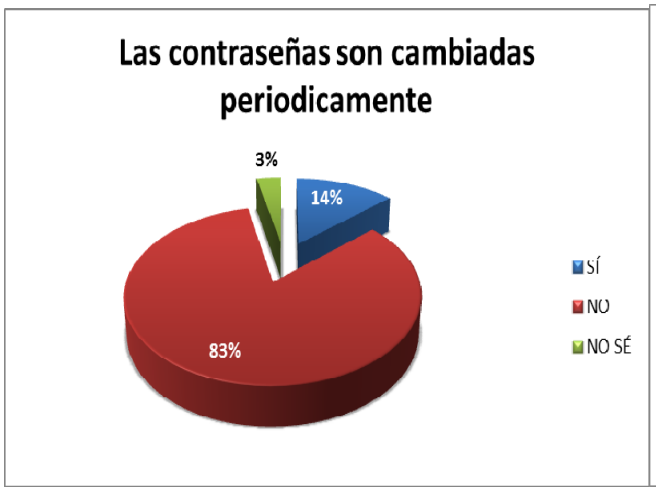


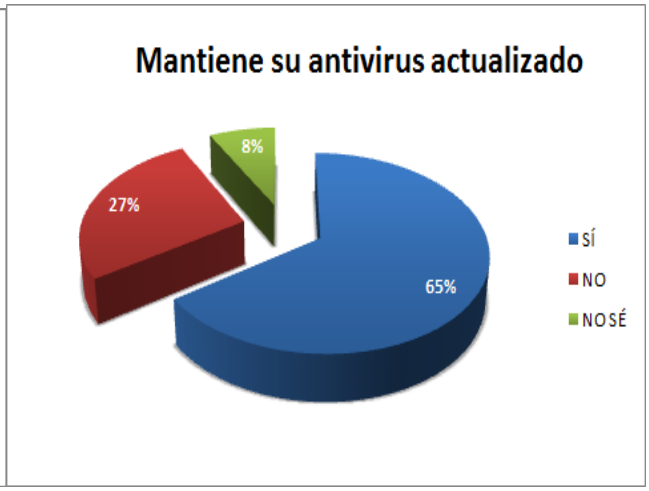




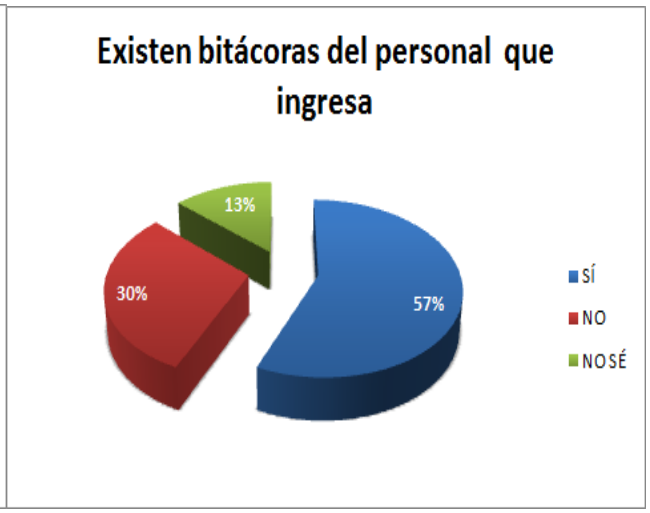

¿Existen políticas de respaldo de información?
20%
23%
57%
SÍ
NO
NO SÉ

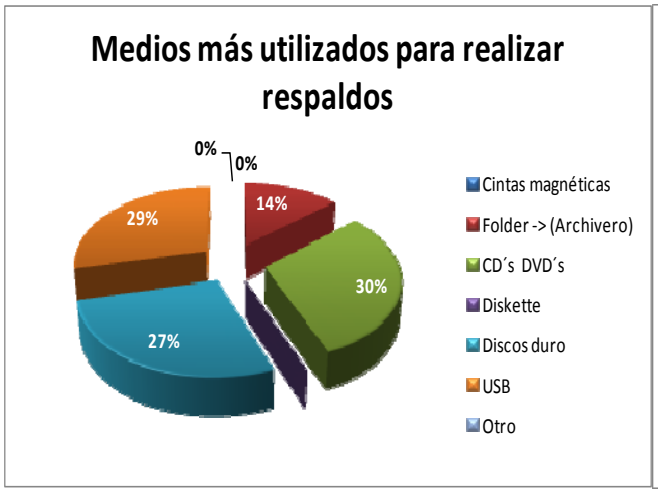

Utiliza contraseña para su equipo de cómputo
0%
30%
70%
SÍ
NO
NO SÉ

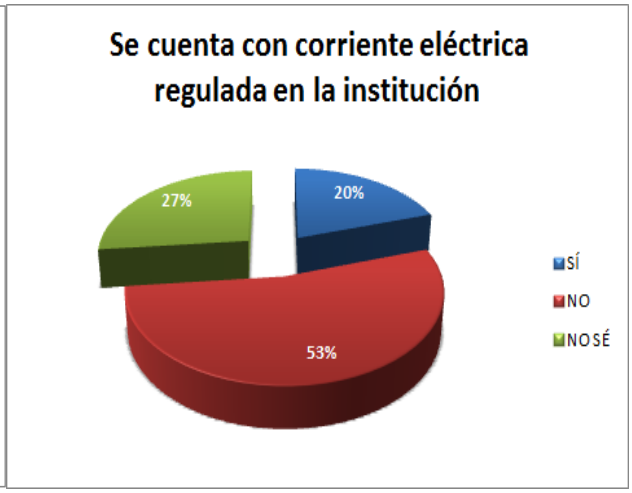

Las contraseñas son cambiadas periodicamente
3%
14%
83%
SÍ
NO
NO SÉ


Mantiene su antivirus actualizado
8%
27%
65%
SÍ
NO
NO SÉ


Se aplican las actualizaciones del sistema operativo
7%
30%
63%
SÍ
NO
NO SÉ

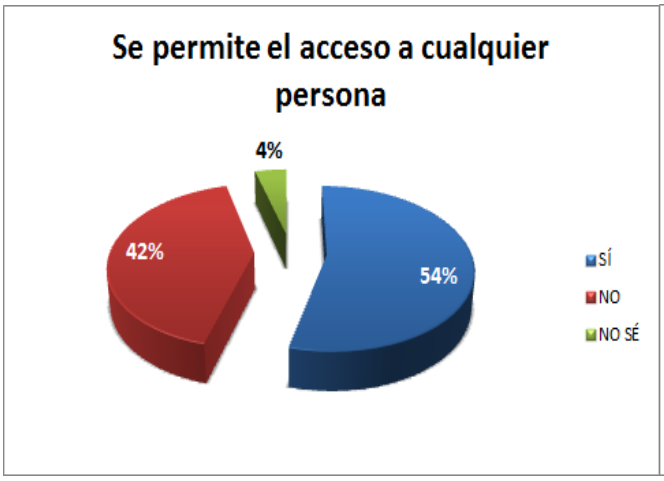

Existen bitácoras del personal que ingresa
13%
30%
57%
SÍ
NO
NO SÉ

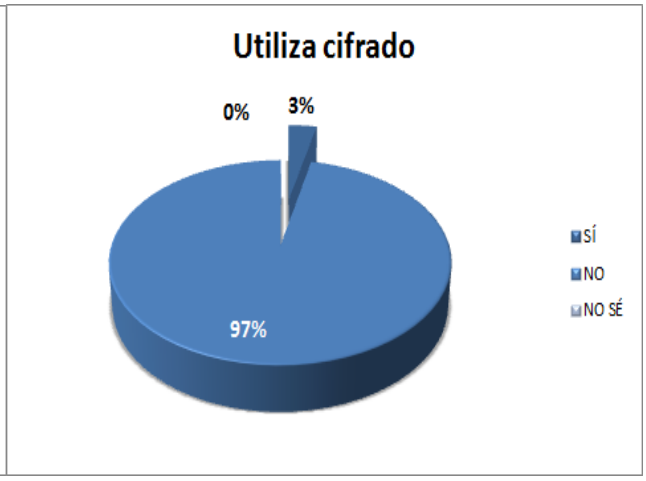

Medios más utilizados para realizar respaldos
0%
0%
14%
29%
30%
27%
Cintas magnéticas
Folder -> (Archivero)
CD´s DVD´s
Diskette
Discos duro
USB
Otro

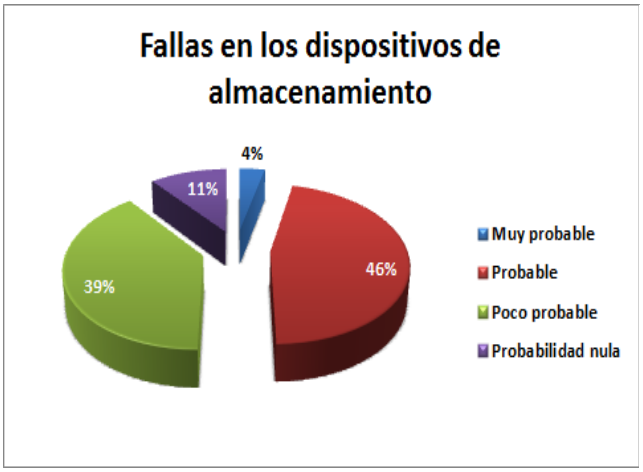

Se cuenta con corriente eléctrica regulada en la institución
27%
20%
53%
SÍ
NO
NO SÉ

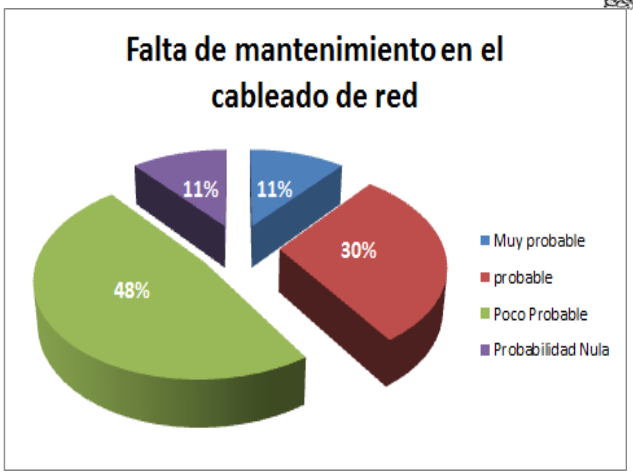

Cuenta con "no break" para el cuidado de los equipos
3%
40%
57%
SÍ
NO
NO SÉ

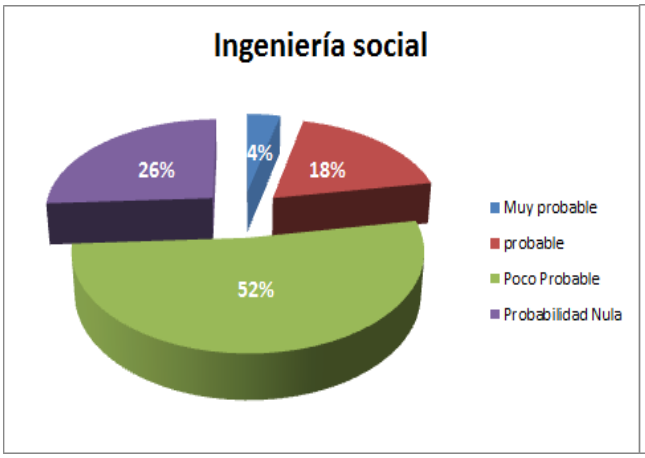

Se cuentan con extinguidores para incendio
3%
14%
83%
SÍ
NO
NO SÉ

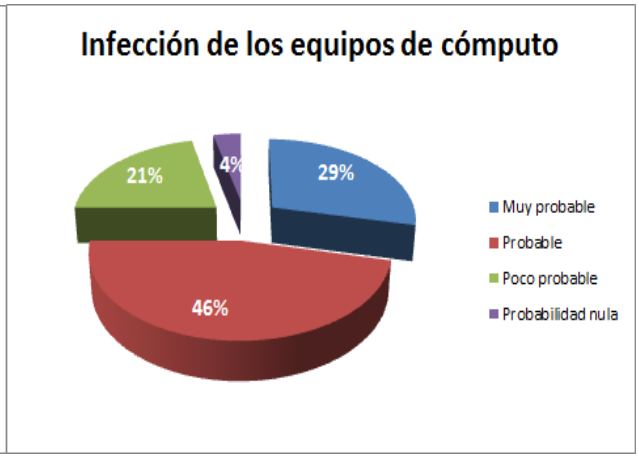

Se permite el acceso a cualquier persona
4%
42%
54%
SÍ
NO
NO SÉ

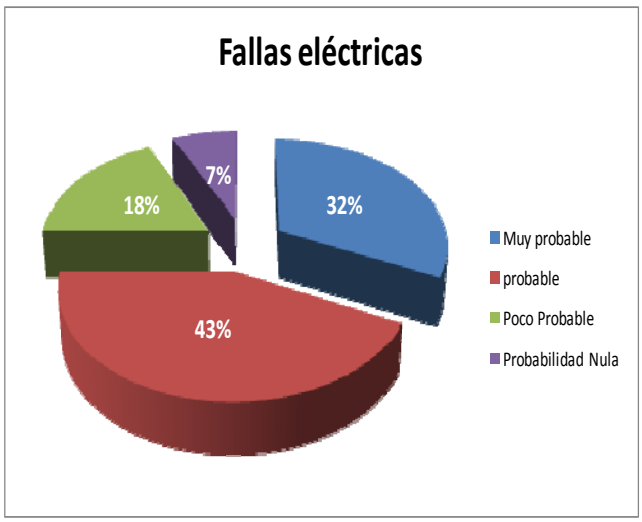

Utiliza cifrado
0%
3%
97%
SÍ
NO
NO SÉ

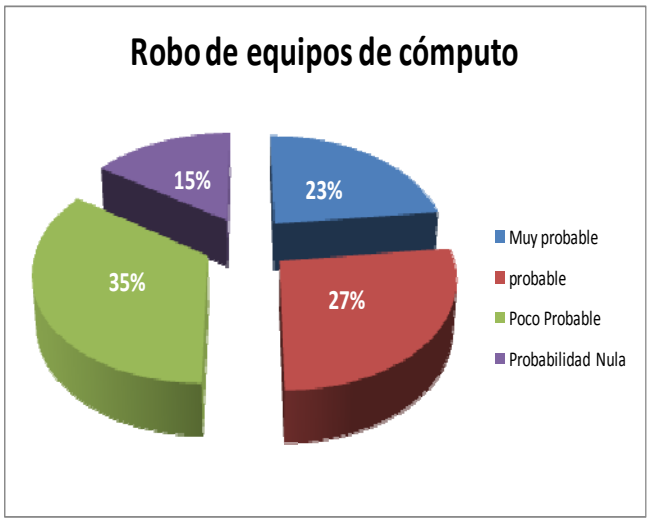

Fallas en los dispositivos de almacenamiento
4%
11%
46%
39%
Muy probable
Probable
Poco probable
Probabilidad nula

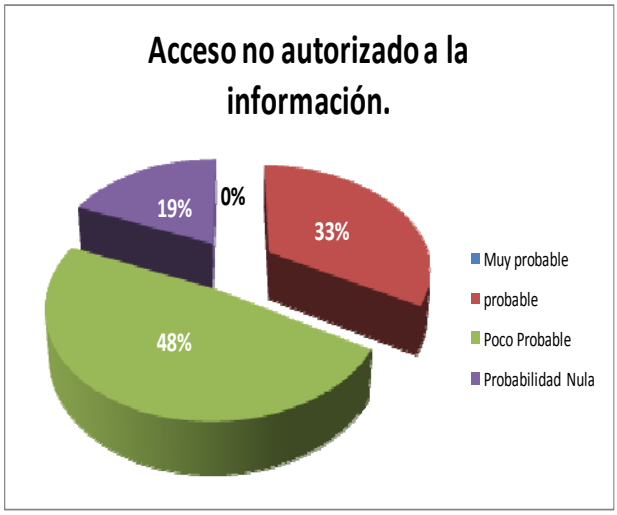

Falta de mantenimiento en el cableado de red
11%
11%
30%
48%
Muy probable
probable
Poco Probable
Probabilidad Nula

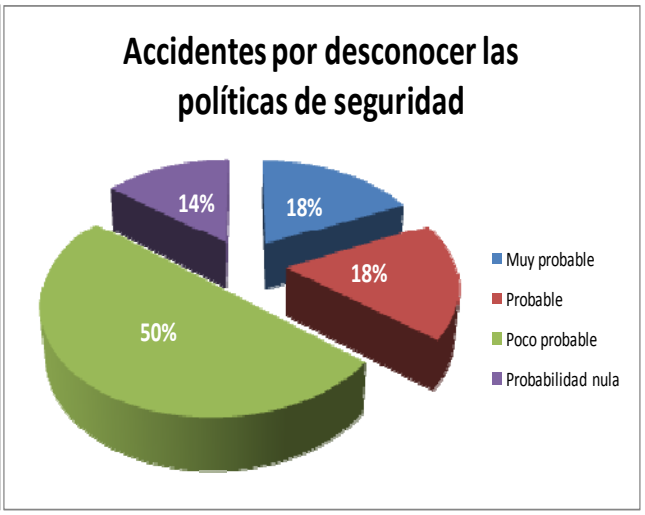

Ingeniería social
26%
4%
18%
52%
Muy probable
probable
Poco Probable
Probabilidad Nula

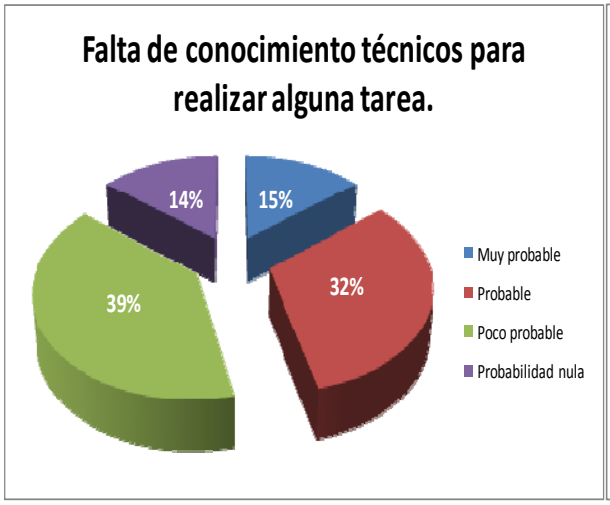

Infección de los equipos de cómputo
21%
4%
29%
46%
Muy probable
Probable
Poco probable
Probabilidad nula


Fallas eléctricas
7%
18%
32%
43%
Muy probable
probable
Poco Probable
Probabilidad Nula

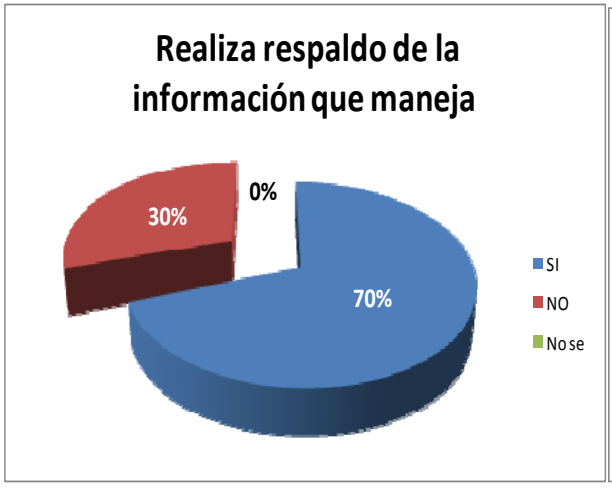

Robo de equipos de cómputo
15%
23%
35%
27%
Muy probable
probable
Poco Probable
Probabilidad Nula

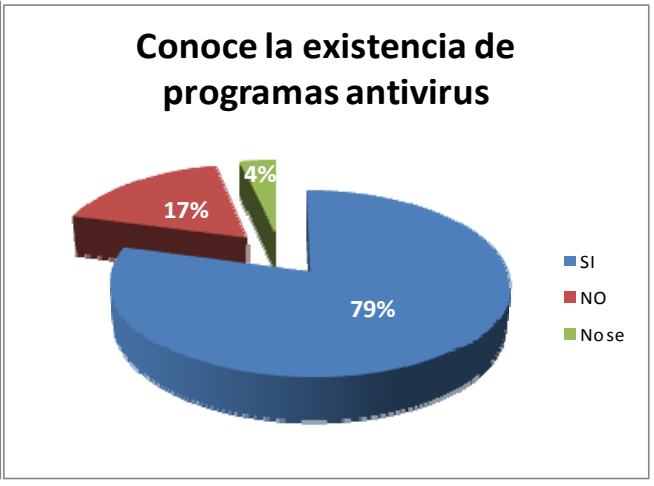

Acceso no autorizado a la información.
19%
0%
33%
48%
Muy probable
probable
Poco Probable
Probabilidad Nula

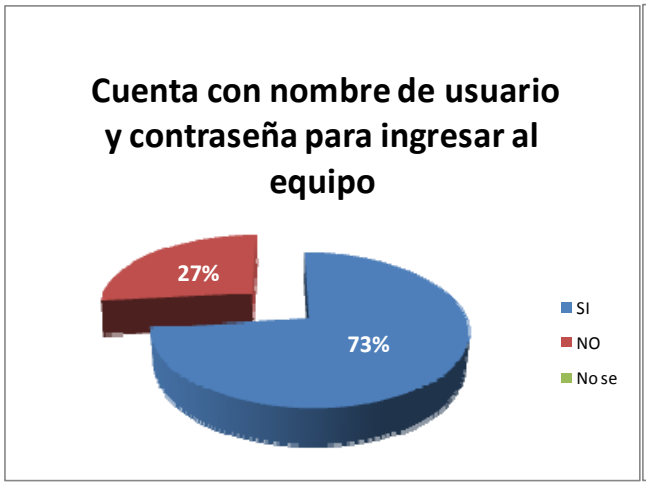

Accidentes por desconocer las políticas de seguridad
14%
18%
18%
50%
Muy probable
Probable
Poco probable
Probabilidad nula

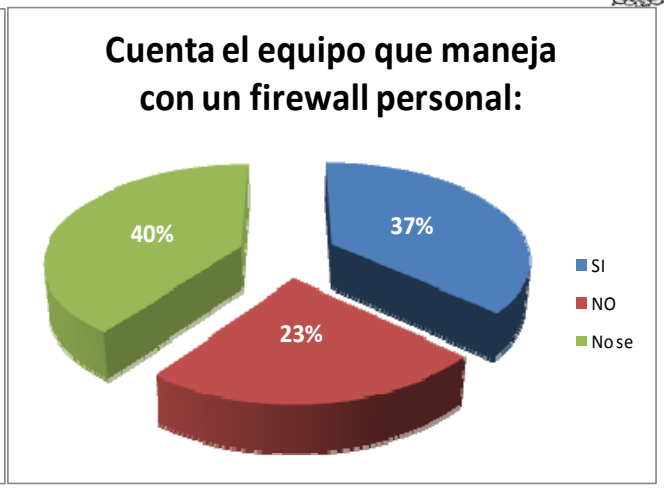

Falta de conocimiento técnicos para realizar alguna tarea.
14%
15%
32%
39%
Muy probable
Probable
Poco probable
Probabilidad nula


Considera necesario el respaldo de información
7%
93%
Si
No


Realiza respaldo de la información que maneja
30%
0%
70%
SI
NO
No se


Conoce la existencia de programas antivirus
17%
4%
79%
SI
NO
No se


Cuenta con nombre de usuario y contraseña para ingresar al equipo
27%
73%
SI
NO
No se


Cuenta el equipo que maneja con un firewall personal:
40%
37%
23%
SI
NO
No se


Aplica las actualizaciones que se liberan para sus aplicaciones y sistema operativo
16%
13%
71%
SI
NO
No se

Glosario

A

ACL: Acrónimo de Access Control List - lista de control de acceso, mecanismo para asignar permisos sobre algún objeto.
Active Directory: Acrónimo de Directorio Activo, servicio que brindan los sistemas operativos de Microsoft en su versión de servidores para brindar una administración centralizada y robusta de los dispositivos que conforman la red.
Activo: Cualquier bien que tenga valor para la organización.
ADSL: Acrónimo de Asymmetric Digital Subscriber Line - Línea de Suscripción Digital Asimétrica, especifica diferente velocidad en la recepción y el envío de datos.
AES: Advanced Encryption Standard - Estándar de cifrado avanzado, algoritmo de cifrado simétrico.
Algoritmo simétrico: Algoritmo que utiliza la misma clave secreta para cifrar y descifrar.
Algoritmo: Método expresado de manera matemática (código de cómputo) para ejecutar una función u operación específica.
Amenaza: Cualquier entidad físico, lógico y natural que provoque un evento, permitiendo desencadenar un incidente en la organización.
Análisis de riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo que presentan los activos de una organización.
AP: Acrónimo de Access Point - punto de acceso, dispositivo empleado para brindar acceso inalámbrico en los estándares 802.11a/b/g/n.
Appliance: Cualquier sistema que se vende como listo para ser usado, presentado como una caja negra, en la que el aplicativo está preinstalado. No sirve para ejecutar otras tareas que aquellas para las cuales ha sido su desarrollo.
ARP: Address Resolution Protocol –Protocolo de Resolución de Dirección física.
ARPA: Acrónimo de Advanced Research Proyect Agency - Agencia de Proyectos de Investigación Avanzada del gobierno de los Estados Unidos.
ARPAnet: Red de computadoras creada por un proyecto del gobierno de los Estados Unidos como medio de comunicación para los diferentes organismos del país.
Ataque: Es la explotación por medio de una amenaza a una vulnerabilidad.
Autenticación: Proceso de determinar la identidad de un usuario.

B

Back Door: Conocida como puerta trasera, es empleada para generar una conexión hacia algún equipo de manera no autorizada.
Backbone: Nivel más alto en una red jerárquica.
Bastion host: Host con procedimientos de Hardening aplicados.
BCP: Acrónimo de Business Continuity Plan- Plan de continuidad del negocio, conjunto de tareas que permite a las organizaciones continuar su actividad en situaciones que un evento afecte sus actividades.

Bien: Cualquier cosa que represente un valor para la organización.
BIOS: Basic Input Output System- Sistema de entrada y salida básico, empleado como la base de comunicación en la configuración lógica del hardware.
Blowfish: Algoritmo de cifrado por bloques, simétrico, generado como algoritmo de uso general, opción de sustitución a DES.
BOOTP: Bootstrap Protocol – Protocolo Bootstrap, empleado para asignar IP a estaciones UNIX antes de cargar el sistema operativo.
Bot: Programa informático que realiza funciones muy diversas, tratando de imitar el comportamiento humano.
Botnet: Red de equipos comprometidos, controlados por software de manera centralizada, empleados principalmente para un fin malicioso.
Bridge (puente): Utilizado para unir dos redes a nivel de capa de enlace (capa 3 modelo OSI).
Broadcast: Transmisión de un paquete que será recibido por todos los miembros de un segmento de red.
BRP: Acrónimo de Business Recovery Plan, Plan de recuperación del negocio.
Buffer overflow: Ataque caracterizado por sobrecargar la memoria de un programa o proceso, un buffer es creado para contener una cantidad de datos finitos, en caso de llenar de más el buffer ocasiona fallas en el programa.

C

CA: Acrónimo de Certificate Authority - autoridad certificadora.
CEH: Acrónimo de Certified Ethical Hacker – Certificación Hacker Ético.
CERT: Acrónimo de Computer Emergency Response Team, Equipo de Respuesta a Incidentes de Cómputo.
Checksum: También conocido como resumen hash, es una cadena de tamaño fijo que identifica una cantidad de datos de tamaño variable.
CIA: Acrónimo de Confidenciality, Integrity, Availability - Confidencialidad, Integridad y Disponibilidad, los tres pilares de la seguridad.
Cifrado asimétrico: Emplea dos contraseñas diferentes, una para ocultar la información y otra para recuperarla.
Cifrado simétrico: Emplean una misma contraseña para ocultar y para recuperar la información.
Cliente – Servidor: Arquitectura en donde básicamente un cliente realiza peticiones a un programa (servidor) el cual da respuesta a las peticiones.
COBIT: Acrónimo de Control OBjetives for Information and related Technology – Objetivos de Control para tecnología de la información, modelo que permite implementar un marco de control y gobernabilidad de TI.
Confidencialidad: La propiedad de que la información esté disponible y no sea divulgada, a personas, entidades o procesos no autorizados.
Contraseña: Un secreto conocido por un usuario y por un sistema, utilizado como mecanismo para identificar a un usuario.

Control de Acceso: Es la metodología de seguridad que permite acceso a la información o recurso con base en la identidad.
Control: Políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
CPU: Acrónimo de Central processing unit- Unidad central de procesamiento.
Criptografía: Es la ciencia de cifrar y descifrar información, utilizando técnicas que hagan posible el intercambio de mensajes de manera segura, que sólo pueden ser leídos por las entidades a quien va dirigido.
Cross Site Scripting: Vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada, y permite el ingreso y envío de datos sin validación alguna.
Cuenta de usuario: Registro que contiene información que identifica un usuario, incluyendo su password.
Cybercrimen: Symantec define Cybercrimen como un crimen que es realizado utilizando una computadora, red o hardware.

D

Datagrama: Parte de un paquete de información.
DB: Acrónimo de Data Base –Base de Datos.
DCA: Acrónimo de Defense Communications Agency-Agencia de defensa para las comunicaciones del gobierno de los Estados Unidos.
DDoS: Acrónimo de Distributed Denial of Service – Denegación de servicio distribuido, tipo de ataque lógico.
Denegación de Servicio: concepto utilizado para referirse a la no disponibilidad.
DES: “Data Encription Standard”, estándar de cifrado de clave secreta, emplea el algoritmo Lucifer desarrollado por IBM.
DGTIC: Dirección General de Cómputo y Tecnologías de Información y Comunicación
DHCP: Dynamic Host Configuration Protocol –Protocolo de configuración dinámica de host.
Dial-up: Conexión a INTERNET vía telefónica.
Diffie – Hellman: Estándar de intercambio de claves.
DISA: Defense Information Systems Agency- Agencia para la defensa de sistemas de información del gobierno de los Estados Unidos.
Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
DMZ: Acrónimo de Desmilitarized Zone -Zona desmilitarizada, una red local que se ubica entre la red interna de una organización y una red externa.
DNS: Domain Name System- Sistema de nombre de Dominios, conjunto de protocolos y mecanismos que permiten la traducción de las URL en una dirección de Internet (IP- Internet Protocol).
DoS: Por sus siglas Denial of Services – Denegación de servicio, familia de ataques que atenta contra la disponibilidad.

DRP: Inglés Disaster Recovery Plan- Un plan de recuperación ante desastres, proceso de recuperación que cubre datos, hardware y software, para que un negocio pueda comenzar de nuevo sus operaciones.
DSL: Digital Subscriber Line -línea de abonado digital.

E

EAP: Acrónimo de Extensible Authentication Protocol – Protocolo de autenticación extensible, permite utilizar nuevos métodos de autenticación para medios cableados e inalámbricos.
ECC: Acrónimo de Elliptic Curve Cryptography – Criptografía con Curvas Elípticas.
Enumeración: Organizar la información recopilada como lo es nombres de usuario, nombres de equipos, redes, puertos abiertos, sistema operativo utilizado, obtener este tipo de información requiere de una constate interacción entre el sistema y el intruso, razón por la cual puede ser identificado.
Estándar: Orientaciones obligatorias que buscan cumplir las políticas.
Ethernet: Es el estándar de red de área local más ampliamente utilizado, define las características de cableado, señalización de nivel físico y los formatos de trama del nivel del enlace de datos del modelo OSI.
Exploit: Del inglés *to exploit*, explotar o aprovechar es una pieza de software, un fragmento de datos, o una secuencia de comandos que se aprovecha de un error, falla o vulnerabilidad para obtener beneficios, dañar el sistema.

F

Falso negativo: Cuando una acción legítima es considerada un problema.
Falso positivo: Cuando un problema no es identificado y se considera una acción legítima.
Fibra Óptica: medio físico utilizado en las redes de datos, para la transmisión de paquetes.
Fingerprinting: Técnica para identificar datos en la red por medio de información pública del objetivo.
Firewall: Un dispositivo físico o lógico que filtra paquetes entre una red privada y una red pública decide qué información puede ser entregada con base en políticas programadas.
Firma digital: Es un conjunto de datos asociados a un mensaje digital que permitan asegurar la integridad del mensaje y la autenticación del emisor.
Firmware: Programa grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos.
FLOPS: Acrónimo de Floating Point Operation Per Second –Operaciones de punto flotante por segundo.
FTP: Acrónimo de File Transport Protocol - Protocolo de transferencia de archivos.

G

Gateway: Punto de conexión entre diferentes redes.
GPS: Acrónimo de Global Positioning System – Sistema de posicionamiento Global.
Gusano: Algún programa que toma medidas activas para reproducirse él mismo.

H

Hacker: Profesional de la seguridad en cómputo, según CEH, Certification Ethical Hacker- Certificación de Hacker Ético.
Handshake: Saludo de tres vías, empleado para comenzar una comunicación entre dos equipo dentro de TCP/IP.
Hardening: Es el proceso de asegurar un sistema, acción compuesta por un conjunto de actividades para reforzar al máximo la seguridad de un equipo, que permite disminuir el riesgo de ser vulnerados.
Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro o archivo.
Help Desk: Recurso para información y asistencia, planteado para resolver problemas relacionados con equipos de cómputo y similares.
HIDS: Acrónimo de Host-based Intrusion Detection System- Sistema detector de intrusos basado en host, el IDS basado en host implica utilizar programas instalados en los sistemas que se requiere sean monitoreados.
Hombre en el medio: técnica de ataque lógico para ver toda la comunicación entre 2 equipos.
Host: Nombre empleado en el argot de redes para hacer referencia a un equipo de cómputo.
Hotspot: También conocido como portal cautivo, mecanismo de seguridad para redes inalámbricas el cual brinda control de acceso y privacidad.
HTTP: Hypertext Transfer Protocol – Protocolo de transferencia de hipertexto.

I

El robo de información sobre un objeto por un atacante.
IANA: Acrónimo de Internet Assigned Numbers Authority - Agencia de Asignación de Números de Internet.
ICMP: Acrónimo de Internet Control Messages Protocol, protocolo de la pila TCP/IP encargado de hacer pruebas de conexión.
IDEA: Acrónimo de International Data Encryption Algorithm – Algoritmo Internacional de Cifrado de datos, algoritmo de bloques cifrado simétrico.

IDS: Acrónimo de Intrusion Detection System – Sistema detector de intrusos, conjunto de programas y dispositivos que permiten la detección de actividades inusuales, incorrectas o anómalas en una red o equipo en particular.
IEC: Acrónimo de Electrotechnical Commission –Comisión Electrónica Internacional.
IETF: Acrónimo de Internet Engineering Task Force – Destacamento de Ingeniería en Internet.
IMAP: Internet Message Access Protocol – Protocolo de acceso a mensajes de internet
Incidente de seguridad: Situación que posiblemente compromete algún activo de la institución.
Incidente de seguridad: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
Integridad: Propiedad de salvaguardar la exactitud de los archivos.
Intrusión: Acción de introducirse sin derecho en una jurisdicción, cargo, propiedad, etcétera.
IP Homologada: Denominación que se le da a toda dirección que tiene acceso directo en internet.
IP: Parte de la suite de protocolos TCP/IP que es responsable de la transferencia de paquetes de información en la red.
IPS: Acrónimo de Intrusion Prevention System – Sistema de prevención de intrusos.
IPS: Internet Protocol Suite – conjunto de protocolos de internet, es un nombre con el que también se conoce al conjunto de protocolos TCP/IP.
IPSec: Protocolo de seguridad para datos en tránsito.
Iptables: Es el subsistema de firewalling de Linux 2.4.x/2.5.x. Ofrece la funcionalidad de filtrado de paquetes (ya sea *stateless* o *stateful*), todos los diferentes tipos de NAT (Network Address Translation), la manipulación de paquetes (modificar TOS -Type of Service- y encabezados) y también facilita el trabajo al subsistema de QoS (Quality of Service) de Linux.
ISN: Initial Sequence Number – Número inicial de secuencia empleado para establecer comunicaciones en el protocolo TCP).
ISO: Acrónimo de International Organization for Standardization - Organización Internacional de Estándares.

K

Kerberos: Protocolo de autenticación de redes de ordenador, que permite a dos computadoras en una red insegura demostrar su identidad mutuamente de manera segura.
Keylogger: Deriva del inglés Key (Tecla) y Logger (Registrador), en conjunto, un software o hardware registrador de teclas.

L

L2TP: Layer 2 Tunneling Protocol – Protocolo de túnel capa 2, protocolo VPN como alternativa y mejora de PPTP.
LAN: Acrónimo de Local Area Network- Red de área local, clasificación de la red según su tamaño.

LCC: Acrónimo de Logical Link Control- Control de enlace lógico, estándar para la transmisión de datos lógicos.
LM Hash: También conocido como LAN Manager hash, es uno de los formatos que se emplean en el almacenamiento de cuentas de usuario en los sistemas operativos anteriores a Windows Vista, con longitud de 16 caracteres.
Log: Hace referencia a un registro de algo.
LSA: Acrónimo de Level Service Agreement, es un acuerdo de nivel de servicio, contrato escrito entre un proveedor de servicio y su cliente con el objetivo de fijar el nivel de calidad del servicio, en aspectos como tiempo de respuesta, disponibilidad de horario, documentación disponible, personal asignado al servicio.

M

MAC_1: Media Access Control- Control de acceso al medio, en redes.

MAC_2: Message Authentication Code – código de autenticación de mensaje en criptografía.
Malware: Denominación que se le recibe cualquier tipo de software malicioso, el término malware incluye virus, gusanos, troyanos, rootkits.
MAN: Metropolitan Área Network-Redes de Área Metropolitana, clasificación de redes según su tamaño.
MBSA: Acrónimo de Microsoft Baseline Security Analyzer, herramienta para ayudar a determinar el estado de seguridad de un sistema de acuerdo con las recomendaciones de seguridad de Microsoft.
MD5: Abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits.
Mecanismo de seguridad: Es un control que se utiliza para implementar un servicio, diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.
MIB: Management Information Base – Base de información gestionada, tipo de base de datos que contiene información de los dispositivos gestionados en una red de comunicación.
MILNET: Military Network – Red militar, fue el nombre que se le dio a parte de la red de ARPANET, diseñada para tráfico clasificado por el departamento de defensa de los Estados Unidos.
Mirror: Del inglés Mirror – Espejo, en redes se refiere a la réplica del tráfico de red de un Puerto en otro.
MIT: Acrónimo de Massachusetts Institute of Technology – Instituto de tecnología de Massachusetts

N

NAS: Acrónimo de Network Attached Storage, brinda un lugar central de almacenamiento de datos, permitiendo acceso a clientes heterogéneos por diversos medios de conexión, estos dispositivos han ganado popularidad en medios virtuales por su rápido acceso a datos, facilidad, administración y configuración simple.

NAT: Acrónimo de Network Address Translation – Traducción de direcciones de red.
NetBios: Network Basic Input/Output System, especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.
NIC: Acrónimo de Network Interface Controller – controlador de interfaz de red, también llamada adaptador de red que permite la comunicación entre diversos dispositivos.
NIDS: Acrónimo de Network IDS – Sistema detector de intrusos de red.
NIST: Acrónimo de National Institute of Standards and Technology- Instituto Nacional de Normas y Tecnología.
No repudio: Servicio de seguridad que permite probar la irrenunciabilidad del envío o recepción de información.
NOC: Acrónimo de Network Operations Center – Centro de operaciones de Red, responsable del monitoreo del estado de la red y de la atención, resolución y análisis de incidentes a problemas que afecten a la disponibilidad y funcionalidad de la infraestructura de red.
NTFS: NT File System, sistema de archivos empleado por algunos sistemas operativos de la familia Microsoft, el cual incorpora principalmente la posibilidad de cifrado, permisos y compresión.

O

OECD: Acrónimo de Organization for Economic Co-operation and Development –Organización para la Cooperación y Desarrollo Económico.
OSI: Acrónimo de Open System Interconnection –Sistema de interconexión abierto, modelo para redes de datos.
Outsoursing: Es el contrato con alguna compañía o persona para realizar una función en particular.

P

Password: Secreto conocido sólo por el sistema y el usuario, utilizado para probar la identidad de un usuario.
PC: Acrónimo de Personal Computer - computadora de propósito general.
PDCA: Acrónimo de Plan-Do-Check-Act, modelo para aplicar a los procesos de Sistemas de Gestión de la Seguridad de la Información, definido en ISO 27001.
PDCA: Ciclo PDCA de mejora continua de la calidad (planear, hace, revisar, actuar).
PF: Packet Filter, sistema de filtrado TCP/IP y traducción de direcciones de red, normalización de paquetes TCP/IP, control de ancho de banda y priorización de paquetes. Parte genérica del sistema operativo OpenBSD a partir de su versión 3.
Pharming: Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta.

Phishing: Es una modalidad de estafa diseñada con la finalidad de robarle la identidad, el delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Plan de contingencia: Tipo de plan preventivo, predictivo y reactivo. Presenta una estructura y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias.

Política: Declaración general de los principios que representan la posición de la administración para un área de control definida.

PPTP: Point to Point Tunneling Protocol. Protocolo de túnel punto a punto, método para implementar VPN.

Print Server: Acrónimo de servidor de impresión que conecta una impresora a la red para que cualquier dispositivo pueda utilizarlo.

Protocolo: Es una regla formal o comportamiento, en relaciones internacionales, los protocolos minimizan el problema causado por diferencia cultural por acordar un conjunto común de reglas que son ampliamente conocidas e independientes de cualquier país.

En comunicaciones de datos, conjunto de reglas utilizadas por dispositivos, para comunicarse entre ellos, la naturaleza de los protocolos requieren procesos de estandarización abierta y documentación de los estándares disponible públicamente, los estándares de internet están desarrollados por Internet Engineering Task Force (IETF) dentro de presentaciones abiertas y públicas, los protocolos desarrollados en este proceso son publicados como Request for Comment(RFCs).

R

RADIUS: Remote Authentication Dial-In User Server – Servidor, protocolo centralizado de autenticación, autorización y auditoría para aplicaciones de acceso a la red.

RC5: Algoritmo simétrico de cifrado de bloques, diseñado por Ronald Rivest en 1994.

RFCs: Acrónimo de Request for Comments - petición de comentarios, serie de documentos que describe el conjunto de protocolos de internet.

RFID: Acrónimo de Radio Frequency IDentification – Identificador por radio frecuencias, sistema de almacenamiento y recuperación de datos por radio frecuencia.

Riesgo residual: El riesgo remanente después del tratamiento de los riesgos.

Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad, es la posibilidad de que suceda un evento.

RIPEMD: Acrónimo de RACE Integrity Primitives Evaluation Message Digest – Primitivas de integridad del resumen del mensaje, algoritmo de resumen, también conocido como función hash.

RMON: Remote Monitoring – Monitoreo remoto, protocolo empleado para el monitoreo de la red.

Robo de identidad: Hacerse pasar por otra entidad haciendo creer a un tercero que se es un usuario verdadero.

Rootkit: Colección de herramientas o utilerías que habilitan niveles de acceso de administrador a una computadora.

Router: Conmutador de paquetes que opera a nivel de red del modelo OSI.

RSA: "Rivest, Shamir y Adleman" - Algoritmo de cifrado asimétrico, desarrollado en 1977.

S

S/MIME: Secure / Multipurpose Internet Mail – Correo de propósito múltiple seguro, estándar de cifrado asimétrico y firma de correo.
SANS: Organización dedicada al entrenamiento en seguridad en cómputo.
Screened subnet: Arquitectura de firewall equivalente a una DMZ.
Seguridad convergente: Seguridad que contempla tanto la seguridad física como lógica, para asegurar un host.
Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la información, pueden estar involucradas otras propiedades como la autenticación, responsabilidad, no repudio y confiabilidad.
Seguridad: Consiste en mantener libre de peligro, daño o riesgo un activo.
Servicio de seguridad: Referido a ofrecer confidencialidad, integridad, no repudio, autenticación, control de acceso, disponibilidad.
Servicio no orientado a conexión: Servicio el cual utiliza el protocolo UDP para su transmisión.
Servicio orientado a conexión: Servicio el cual utiliza el protocolo TCP para su transmisión.
SET: Secure Electronic Transaction – Transacción electrónica segura, protocolo elaborado por iniciativa de VISA o Mastercard, protocolo asimétrico similar a PGP.
SGSI: Acrónimo de Sistema de Gestión de la Seguridad de la Información.
SHA1: Algoritmo de resumen criptográfico, genera cadenas de 128 y 256 bits.
Site: Lugar o sitio, en el cual se tiene el conjunto de dispositivos de telecomunicaciones y servidores con condiciones idóneas como clima, presión, monitoreo, control de acceso, corriente regulada, UPS, sistemas de tierra y obra civil, principalmente.
SLA: Service Level Agreement - acuerdo de nivel de servicio, contrato escrito entre un proveedor de servicios y su cliente con el objeto de fijar el nivel acordado para la calidad de dicho servicio.
SMB: Server Message Block, protocolo empleado para compartir acceso a recursos, impresoras, puertos, entre otros.
SMTP: Simple Message Transport Protocol – Protocolo de transporte de mensajes simple.
Sniffer: Programa de captura de las tramas de red, generalmente se usa para gestionar la red con una finalidad administrativa, aunque también puede ser utilizado con fines maliciosos.
SNMP: Simple Network Management Protocol - Protocolo simple de administración de red.
SPAM: Correo no solicitado enviado por internet.
Spoofing: Ataque que se caracteriza por la suplantación de identidad.
SQL injection: Es una técnica de inyección de código que explota una vulnerabilidad que ocurre en la base de datos o en la capa de aplicación.
SQL: Acrónimo de Structure Query Languaje - Lenguaje de consulta estructurado, aplicación para bases de datos.
SSH: Secure Shell -intérprete de órdenes seguro, protocolo seguro de administración remota.

SSL: Secure Socket Layer, protocolo de seguridad que permite cifrar la información en el transporte de la misma, desarrollado por Netscape Communications.
Switch: Es un dispositivo de red, que habilita a los dispositivos de red comunicarse uno con otro eficientemente, dentro de los diversos dispositivos que comunica se encuentran computadoras, puntos de acceso, servidores, print servers, móviles, entre otros.
Syskey: Sistema que añade una capa de seguridad en el almacenamiento de contraseñas en plataformas Microsoft.

T

TCP/ IP: Transmission Control Protocol – Internet Protocol (Protocolo de Control de Transmisión – Protocolo de Internet), es un conjunto de protocolos que forman la base de Internet.
TELNET: The Network Terminal Protocol – Protocolo de terminal para la red.
Texto en claro: Nombre empleado para definir a los datos que viajan sin cifrado.
TI: Acrónimo de Tecnologías de la información.
TKIP: Acrónimo de Temporal Key Integrity Protocol – Protocolo de integridad de clave temporal
TLS: Acrónimo Transport Layer Security – Seguridad en la capa de transporte, protocolo de seguridad de los datos en tránsito.
Trap: Para el protocolo SNMP, se refiere a un reporte de ciertas condiciones y cambios de estado a un proceso de administración.
TRIPLE DES: Algoritmo de cifrado simétrico con claves de 112 o 168 bits.

U

UDP: Acrónimo de User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas.
UPS: Acrónimo de Uninterruptible Power Supply–Entrega de alimentación ininterrumpida
USB: Acrónimo de Universal Serial Bus – bus serial universal, especificación para establecer comunicación entre dispositivos y un host.
UTP: Acrónimo de Unshielded Twisted Pair – Cable de par trenzado

V

Virus: Malware que tiene por objeto alterar el normal funcionamiento de la computadora
VoIP: Acrónimo de Voz sobre IP, es una de las familias de protocolos de comunicación enfocada a tecnología de transmisión de voz.
VPN: Acrónimo de Virtual Network Private - Red Privada Virtual.
Vulnerabilidad: Hace referencia a un punto débil dentro de un sistema

W

WAN: Wide Area Network- Redes de Área Amplia, clasificación de la red según su tamaño.
Wardriving: Búsqueda de redes inalámbricas desde un vehículo en movimiento.
WEP: Wireless Equivalent Privacity –Privacidad equivalente al cableado, protocolo de seguridad en redes inalámbricas.
WiFi: Wireless Fidelity – Fidelidad Inalámbrica, tecnología de comunicaciones inalámbricas.
Wireless hacking: Hackeo de redes inalámbricas.
Wireless: Tecnología de transmisión inalámbrica por medio de ondas magnéticas a diferentes frecuencias dependiendo el estándar.
WLAN: Wireless Local Area Network – Red Inalámbrica de Area Local.
WMAN: Wireless Metropolitan Area Network –Red Inalámbrica de Área Metropolitana.
WPA: Wi-Fi Protect Access – Acceso protegido Wi-Fi, protocolo de seguridad para redes inalámbricas, creado para corregir las deficiencias de WEP.
WPA2: Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2, sucesor de WPA, utilizando para garantizar confidencialidad AES.

Referencias

Bibliografía

Capítulo I

1) Programa de la academia Cisco Networking, material multimedia, 2006
2) Libor Dostálek, Undestanding TCP/IP, Packt publishing, 2006
3) Steven T. Karris, NETWORKS Design and Management, Orchard Publications 2002
4) Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001
5) Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004
6) Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005
7) Craig Hunt, TCP/IP Network Administration, 3rd Edition, O'Reilly 2002
8) Bryan Burns, SECURITY POWER TOOLS, O Reilly 2007

Capítulo II

1) Robert Richardson, CSI Computer Crime & Security Survey, 2008
2) Charles P. Pfleeger, Security in Computing, Fourth Edition, Prentice Hall 2006
3) Kimberly Graves, CEH ™ Official Certified Ethical Hacker Review Guide, Wiley Publishing 2007
4) William Stallings, Fundamentos de seguridad en redes aplicaciones y estándares, segunda edición, Pearson Educación 2005.
5) Matthew Strebe, Network Security Jumpstart, Sybex, 2002
6) Mike Horton, Clinton Mugge, Hacknotes™ Network Security Portable Reference, McGraw-Hill/Osborne 2003
7) Robert Richardson, CSI Computer Crime & Security Survey, 2008
8) Jordi Herrera Joancomartí, Aspectos avanzados de seguridad en redes, UOC Formación de Posgrado 2004
9) Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001
10) Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005
11) Daltabuit, La seguridad de la información, Limusa Noriega Editores 2007
12) Risk Management Guide for Information technology System, NIST SP800-30

Capítulo III

1) Matthew Strebe, Network Security Jumpstart, Sybex, 2002
2) Antonio Villalón Huerta, seguridad en unix y redes, GNU Free Documentation 2002
3) Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004
4) Jordi Herrera Joancomartí, Aspectos avanzados de seguridad en redes, UOC Formación de Posgrado 2004
5) Lawrence MillerandPeter Gregory, CISSP for Dummies, 2nd Edition, John Wiley & Sons 2007

6) **Mike Horton, Clinton Mugge, Hacknotes™ Network Security Portable Reference, McGraw-Hill/Osborne 2003**
7) **James Joshi, Network Security: Know It All, Morgan Kaufmann 2008**
8) **Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001**
9) **John E. Canavan, Fundamentals of Network Security, Artech House 2000**
10) **Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005, p346-348**
11) **Melissa M, Syngress, Designing a Windows server 2003 active Directory Infrastructure.**
12) **Módulo 3 fundamentos de seguridad en redes, aplicaciones y estándares, Diplomado Seguridad de la Información, CEM Polanco DGTIC 2008**
13) **William Stallings, Fundamentos de seguridad en redes aplicaciones y estándares, segunda edición, Pearson Educación 2005.**

Capítulo IV

1) **Matthew Strebe, Network Security Jumpstart, Sybex, 2002**
2) **ISO 27001 ed 2005**
3) **Daltabuit, La seguridad de la información, Limusa Noriega Editores 2007**
4) **Dr. Eric Cole, Network Security Bible, Wiley Publishing 2005, p346-348**
5) **Kimberly Graves, CEH ™ Official Certified Ethical Hacker Review Guide, Wiley Publishing 2007**
6) **Cliff Riggs, Network Perimeter Security: Building Defense In-Depth, Auerbach Publications 2004**
7) **MIKE HORTON, CLINTON MUGGE, HACKNOTES™ Network Security Portable Reference, McGraw-Hill/Osborne 2003**
8) **Joel Scambray, Hacking Exposed: Network Security Secrets & Solutions Second Edition, McGraw-Hill 2001**
9) **John E. Canavan, Fundamentals of Network Security, Artech House 2000**
10) **Bryan Burns, SECURITY POWER TOOLS, O Reilly 2007**

Capítulo V

1) **NIST 800-30.**
2) **Peter N.M. Hansteen, The Book of PF 2nd Edition, William Pollock 2011**
3) **Joel Scambray & Stuart McClure, Hacking exposed windows: windows Security Secrets & Solutions third edition, McGrawHill 2008**
4) **Andrew Williams, Nessus, Snort & Ethereal Power Tools, Syngress Publishing 2005**
5) **John R.Vacca, Firewalls Jumpstart for Network and Systems Administrators, Elsevier 2005**
6) **KerryJ. Cox, Christopher Gerg Managing Security with Snort and IDS Tools, O'Reilly 2004**
7) **Steve Andrés, Security Sage's guide to hardening the network infrastructure, Syngress Publishing 2004**

Páginas electrónicas

Capítulo I

1) **Carlos Vicente, Servicios de red Universidad de Oregon, Gestión de Traps SNMP (última revisión: 01-febrero-2011).**
   http://www.nsrc.org/workshops/2008/walc/presentaciones/gestion_traps.ppt
2) **Dirección física (última revisión: 01-febrero-2011).**
   http://standards.ieee.org/regauth/oui/index.shtml
3) **Definición de puerto (última revisión: 01-febrero-2011).**
   http://www.iana.org/assignments/port-numbers
4) **Protocolo ARP (última revisión: 01-febrero-2011).**
   http://www.rfc-es.org/rfc/rfc0826-es.txt
5) **Three-way handshake (última revisión: 01-febrero-2011).**
   http://www.telefonica.net/web2/marco2z/doc/tcp_ip.es.pdf
6) **RFC854 - Telnet Protocol Specification (última revisión: 01-febrero-2011).**
   http://www.faqs.org/rfcs/rfc854.html
7) **RFC959 - File Transfer Protocol (última revisión: 01-febrero-2011).**
   http://www.faqs.org/rfcs/rfc959.html
8) **Modos de conexión FTP (última revisión: 01-febrero-2011).**
   http://www.ignside.net/man/ftp/pasivo.php
9) **RFC 2616 - Hypertext Transfer Protocol (última revisión: 01-febrero-2011).**
   http://www.faqs.org/rfcs/rfc2616.html
10) **RFC 1939 - Post Office Protocol - Version 3 (última revisión: 01-febrero-2011).**
    http://www.faqs.org/rfcs/rfc1939.html(pop3)
11) **Domain Name Service (DNS) (última revisión: 01-febrero-2011).**
    http://technet.microsoft.com/en-us/library/bb726935.aspx
12) **Servidores DNS raíz (última revisión: 01-febrero-2011)**
    http://www.root-servers.org/
13) **Miguel Angel Hernández Vallejos, Riesgos en el sistema DNS, ESA Security S.A. (última revisión: 01-febrero-2011).**
    http://www.esa-security.com/pdf/SIC_68_Riesgos%20en%20el%20Sistema%20de%20DNS.pdf
14) **BOOTP y DHCP (última revisión: 01-febrero-2011).**
    http://technet.microsoft.com/es-es/library/cc781243.aspx
15) **María Gabriela Briseño, Protocolo básico de administración de red (snmp) versión 3. (última revisión: 01-febrero-2011)**
    http://neutron.ing.ucv.ve/revista-e/No6/Brice%C3%B1o%20Maria/SNMPv3.html

Capítulo II

1) **Amenazas lógicas, tipos de ataques (última revisión: 01-febrero-2011).**
http://www.segu-info.com.ar/ataques/ataques.htm
2) **Virus (última revisión: 01-febrero-2011).**
http://www.2privacy.com/www/viruses/virus-glossary.html
3) **IP Spoofing (última revisión: 01-febrero-2011).**
http://www.symantec.com/connect/articles/ip-spoofing-introduction
4) **Rule Set Based Access Control, (última revisión: 01-febrero-2011).**
http://www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx
5) **Envenenamiento ARP (última revisión: 01-febrero-2011).**
http://blackspiral.org/docs/arp_spoofing.html
6) **Ataque Man In the Middle (última revisión: 01-febrero-2011).**
http://casidiablo.net/man-in-the-middle/
7) **Fingerprintings Tools (última revisión: 01-febrero-2011).**
http://www.securityfocus.com/archive/112/323521
8) **Fingerprinting activo (última revisión: 01-febrero-2011).**
http://bpsmind.wordpress.com/2008/07/17/fingerprinting-activo-y-pasivo/
9) **Botnet (última revisión: 01-febrero-2011).**
http://eliax.com/index.php?/archives/4665-El-nuevo-Botnet-Kraken,-amenaza-contra-el-Internet.html
10) **Cuatro pasos para luchar contra los botnets (última revisión: 01-febrero-2011).**
http://www.idg.es/computerworld/articulo.asp?id=183857
11) **El super ordenador más potente del mundo (última revisión: 01-febrero-2011).**
http://www.elmundo.es/navegante/2008/06/10/tecnologia/1213080910.html
12) **Rendimiento de las computadoras (última revisión: 01-febrero-2011).**
http://www.tecnologiahechapalabra.com/datos/soluciones/implementacion/articulo.asp?i=3269
13) **Footprinting, escaneos, enumeración (última revisión: 01-febrero-2011).**
http://www.hacktimes.com/?q=taxonomy/term/24

Capítulo III

1) **DRP (última revisión: 01-febrero-2011)**
http://132.248.173.15/labsec/3semsi/filminas/Administracionderiesgos.pdf
2) **Active Directory (última revisión: 01-febrero-2011)**
http://ditec.um.es/aso/teoria/tema13.pdf
3) **Seguridad del terminal, HP (última revisión: 01-febrero-2011)**
http://docs.hp.com/es/5187-2217/ch07s02.html?btnPrev=%AB%A0anterior
4) **Beneficios, políticas de seguridad (última revisión: 01-febrero-2011)**
http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html
5) **Mecanismos de protección, servicios seguros (última revisión: 01-febrero-2011)**
http://sistemas.itlp.edu.mx/tutoriales/sistemasoperativos2/unidad3.htm
6) **Métodos de autenticación, algo que se es, (última revisión: 01-febrero-2011)**
http://www.biometriaaplicada.com/nosotros.html
7) **Planeación de la seguridad, (última revisión: 01-febrero-2011)**

http://www.cujae.edu.cu/eventos/convencion/cittel/Trabajos/CIT052.pdf
8) **Matriz de acceso, (última revisión: 01-febrero-2011)**
http://www.esdebian.org/articulos/23887/rule-set-based-access-control
9) **Gunnar Wolf, Herramienta "Logcheck", (última revisión: 01-febrero-2011)**
http://www.gwolf.org/files/logcheck/index.html
10) **Gunnar Wolf, Herramienta "PortSentry", (última revisión: 01-febrero-2011)**
http://www.gwolf.org/files/portsentry/index.html
11) **C. Allen, The TLS Protocol, Network Working Group (última revisión: 01-febrero-2011)**
http://www.ietf.org/rfc/rfc2246.txt
12) **CyberLocator and The van Dillen GroupAutenticación basada en localización física, (última revisión: 01-febrero-2011)**
http://www.lbszone.com/index2.php?option=com_content&do_pdf=1&id=1144
13) **Elena Pérez Gómez, La gestión de la seguridad de la información, Socia de la firma de abogados Sánchez-Crespo (última revisión: 01-febrero-2011)**
http://www.microsoft.com/business/smb/es-es/legal/gestion-seguridad.mspx
14) **Carlos Alberto Vicente, Seguridad perimetral, DGSCA 2005(última revisión: 01-febrero-2011)**
http://www.seguridad.unam.mx/eventos/admin-unam/Monitoreo.pdf
15) **Mecanismos básicos de seguridad para redes de cómputo, (última revisión: 01-febrero-2011)**
http://www.seguridad.unam.mx/eventos/admin-unam/politicas_seguridad.pdf
16) **Estrategias Básicas de Seguridad Informática: Defensa en Profundidad, (última revisión: 01-febrero-2011)**
http://www.sentineldr.com/post/estrategias-basicas-de-seguridad-informatica-defensa-en-profundidad
17) **Estrategias de seguridad, (última revisión: 01-febrero-2011)**
http://www.textoscientificos.com/redes/firewalls-distribuidos/estrategias-seguridad
18) NSA Suite B Cryptography, NSA, nov. 8 2010
http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml
19) Steven M. Bellovin, Access Control Matrix, Columbia University, sep 12 2005.
http://www1.cs.columbia.edu/~smb/classes/f05/l03.pdf
20) **Rule Set Based Access Control, Controles de acceso** (última revisión: 01-febrero-2011)
http://www.esdebian.org/articulos/23887/rule-set-based-access-control

Capítulo IV

1) **The 7 best for network security in 2007 (última revisión: 01-febrero-2011)**
http://www.networkworld.com/columnists/2007/011707miliefsky.html
2) **The 7 best for network security in 2007, (última revisión: 01-febrero-2011)**
http://www.networkworld.com/columnists/2007/011707miliefsky.html?page=3
3) **The Top Cyber Security Risk, SANS**
http://www.sans.org/top20/
4) **Seguridad en sistemas, (última revisión: 01-febrero-2011)**
http://technet.microsoft.com/es-es/library/ms143455(SQL.90).aspx
5) **Seguridad en sistemas, (última revisión: 01-febrero-2011)**

http://technet.microsoft.com/es-es/library/cc782569(WS.10).aspx
6) **Seguridad en sistemas, Windows IIS hardening(última revisión: 01-febrero-2011)**
http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1096044,00.html#general
7) **Hardening en sistemas operativos Windows, (última revisión: 01-febrero-2011)**
http://www.microsoft.com/spain/empresas/seguridad/articulos/plan_seguridad.mspx
8) Robert Comella, Computer Disaster Recovery Plan Policity, SANS
http://www.sans.org/security-resources/policies/disaster_recovery2.pdf
9) **Hardening en sistemas operativos Unix y Linux, (última revisión: 01-febrero-2011)**
http://www.seguridad-informatica.cl/web/content/hardening-de-servidores-linux-y-windows-
10) **Hardening en sistemas operativos Unix y Linux , Lynis (última revisión: 01-febrero-2011)**
http://www.rootkit.nl/projects/lynis.html
11) **Hardening, HowTos(última revisión: 01-febrero-2011)**
http://www.linux-sec.net/Harden/howto.gwif.html
12) **The First Ten Steps to Securing a UNIX Host, (última revisión: 01-febrero-2011)**
http://www.arsc.edu/~lforbes/cug/HHPaper.html
13) **The Bastille Hardening program, increased security for you OS (última revisión: 01-febrero-2011)**
http://bastille-linux.sourceforge.net/running_bastille_on.htm#top
14) **Buenas prácticas para evitar "hackeos" de servidores, (última revisión: 01-febrero-2011)**
http://www.cristalab.com/blog/buenas-practicas-para-evitar-hackeos-de-servidores-c68898l/
15) **Buenas prácticas de seguridad para servidores Windows, (última revisión: 01-febrero-2011)**
http://www.atencion.ula.ve/documentacion/seguridad/recomendaciones_adm_windows.pdf
16) **Buenas prácticas en seguridad, informática (última revisión: 01-febrero-2011)**
http://www.eset-la.com/press/informe/buenas_practicas_seguridad_informatica.pdf
17) **VOIP Security Series , (última revisión: 01-febrero-2011)**
http://blogs.sans.org/security-leadership/
18) **What are the 20 Critical Controls , (última revisión: 01-febrero-2011)**
https://blogs.sans.org/security-leadership/2009/08/01/what-are-the-20-critical-controls/
19) **Los 20 controles críticos según SANS Institute, (última revisión: 01-febrero-2011)**
http://symc.com.mx/index.php/2009/08/07/los-20-controles-criticos-segun-sans-institute/
20) **20 Critical Security Controls, (última revisión: 01-febrero-2011)**
http://www.sans.org/critical-security-controls/print.php

Capítulo V

1) **Filtrado de contenido, OpenDNS(última revisión: 01-febrero-2011)**
http://www.opendns.com/
2) **Sistema operativo OpenBSD, packet filter (última revisión: 01-febrero-2011)**
http://www.openbsd.org/faq/pf/shortcuts.html
3) **Sistema operativo OpenBSD, (última revisión: 01-febrero-2011)**
http://www.openbsd.org/

4) **IDS open source, (última revisión: 01-febrero-2011)**
http://www.snort.org/
5) **NTOP, análisis de tráfico de red (última revisión: 01-febrero-2011)**
http://www.ntop.org/news.php
6) **Portal cautivo ChilliSpot (última revisión: 01-febrero-2011)**
http://www.chillispot.info/
7) **ChilliSpot configuración, (última revisión: 01-febrero-2011)**
http://www.chillispot.info/chilliforum/viewtopic.php?id=18
8) **Task Secure Hardening, Microsoft (última revisión: 01-febrero-2011)**
http://msdn.microsoft.com/en-us/library/ee695875(VS.85).aspx
9) Switch hardening on your network, (última revisión: 01-febrero-2011).
http://isc.sans.edu/diary.html?storyid=6910
10) **White paper, IronShield best practices hardening Foundry router & switch, (última revisión: 01-febrero-2011)**
http://www.genesisglobalinc.com/PDF/foundry-hardening-routers-switches.pdf

Figuras

CAPÍTULO 1. Conceptos Básicos

CAPÍTULO 2. Conceptos Generales de Seguridad

CAPÍTULO 3. Mecanismos de seguridad en red

CAPÍTULO 4. Buenas Prácticas de Seguridad

CAPÍTULO 5. Propuesta de implementación, caso práctico

Apendice B.

Apéndice C.

Tablas