



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Manual de Prácticas para la asignatura
Seguridad Informática Avanzada

TESIS PROFESIONAL

para obtener el título de:

INGENIERO EN COMPUTACIÓN

ÁREA

Redes y Seguridad

PRESENTAN:

IGNACIO DAVID GONZÁLEZ CASTILLO

ISRAEL MONTES MEDINA

DIRECTORA DE TESIS:

M.C. Cintia Quezada Reyes

Ciudad Universitaria, México, Octubre 2014.





Universidad Nacional
Autónoma de México



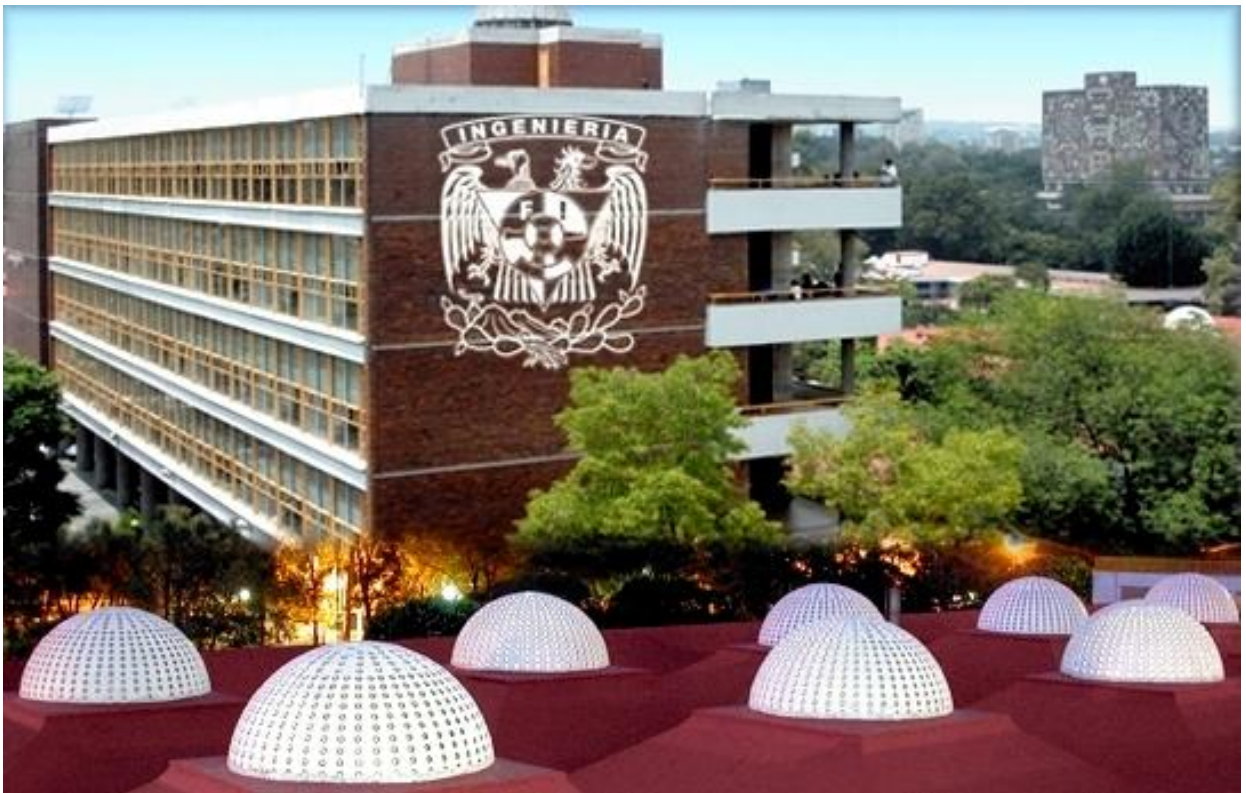
UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS



AGRADECIMIENTOS

IGNACIO DAVID GONZÁLEZ CASTILLO

AGRADEZCO A:

Mis Padres

Ignacio González Rodiles y María del Pilar Irma Castillo Lara que hicieron todo en la vida para que yo pudiera lograr mis metas, al motivarme y darme la mano o decirme las palabras correctas justo cuando sentía que el camino se cerraba, a ustedes los llevo siempre en mi corazón y sé que mi mamá siempre me estará guiando desde el cielo.

Mi Hermana

Irma Lizbeth González Castillo por estar conmigo en los momentos buenos y malos pero sobre todo por apoyarme siempre.

Mi novia

Yessika Guzmán López por tu paciencia, comprensión, apoyo, consejos y alentarme a continuar cuando todo parecía que estaba perdido, gracias por esas palabras, por llegar siempre con sonrisa de oreja a oreja, tu simpatía y tus buenos chistes. Tú me enseñaste a ver el lado positivo, en los malos momentos y sobretodo estuviste cuando más te necesité, me sigues inspirando a ser mejor para ti, ahora puedo decir que esta tesis lleva algo de ti, gracias por estar siempre a mi lado y ser una magnífica persona, ¡¡¡TE AMO!!!

Mi compañero de Tesis

Israel Montes Medina que sin su colaboración no hubiera sido posible terminar esta tesis ya que considero que hicimos un excelente equipo de trabajo al apoyarnos en los momentos difíciles y en los obstáculos que tuvimos que pasar para poder finalizarla pero principalmente quiero darte las gracias por ser un excelente amigo.

Mi asesora de tesis

M.C. Cintia Quezada Reyes por la dirección de este trabajo.

Todos mis amigos

Gracias a todos ustedes pues son importantes en mi vida y siempre estuvieron listos para brindarme toda su ayuda y aconsejarme, con todo mi cariño esta tesis se las dedico.

AGRADECIMIENTOS

Todos mis compañeros de trabajo

De la Coordinación de Procesos e Información de Consejo Técnico de la Facultad de Ingeniería por su amistad y colaboración. En especial a mi jefe M.A. Víctor Damián Pinilla Mora quien me apoyó y otorgó los permisos que necesitaba para realizar el proceso de Titulación y a la Ing. Gabriela Camacho Villaseñor que me apoyó, asesoró, orientó y alentó a terminar la tesis.

En general

En la presente Tesis hubo un esfuerzo directo o indirecto de varias personas que participaron leyendo, opinando, corrigiendo, dándome ánimo, acompañándome en los momentos de crisis y en los momentos de felicidad. Todos aquellos familiares y amigos que no tienen una mención particular al momento de escribir esto quiero decirles: ¡Gracias por todo!.

11000010 10100001 01000111 01110010 01100001 01100011 01101001 01100001
01110011 00100000 01110000 01101111 01110010 00100000 01110100 01101111
01100100 01101111 00100001 00101110

AGRADECIMIENTOS

ISRAEL MONTES MEDINA

A Dios, por darme su infinito amor, fe y esperanza en este recorrido que me permite concluir e iniciar otro. Además, de la oportunidad de vivir y por estar conmigo día a día, haciéndome una mejor persona con valores, aceptando mis defectos, fortaleciendo mi corazón y ayudándome en los momentos difíciles. Gracias por haber puesto en mi camino a aquellas personas que han sido mi luz, soporte y compañía durante la realización de la tesis. También por haberme dado salud ante todo para lograr mis objetivos.

A mis padres por ser el pilar fundamental de todo lo que soy ahora, en toda mi educación, tanto académica como de la vida. Gracias a su amor incondicional, esfuerzo y dedicación, no sería nada sin ustedes: A mi madre Norma Medina Gascón por darme la vida, por apoyarme y escucharme siempre, por sus consejos sabios, por impulsarme a lograr mis metas, por pulir mis habilidades, por darme los valores para ser una persona de bien y sobre todo por tu inmenso amor. A mi padre Adolfo Montes Galindo, por demostrarme tu gran amor y confianza que me ha ayudado a ser un buen hombre; en verdad, te agradezco que me conozcas, por darme las armas para salir adelante y por creer en mí. Sabiendo que jamás existirá una forma de agradecerles una vida de lucha, sacrificio y empeños constantes, solo deseo que comprendan que este logro obtenido es suyo, que mi trabajo está inspirado en ustedes y que son mi único ideal.

A mis hermanos, Mónica Montes Medina y Adolfo Christian Montes Medina, por estar conmigo, preocuparse, protegerme y apoyarme siempre, los amo con todo mi corazón. Agradezco a Dios y a mis padres tenerlos a mi lado, sin ustedes mi vida sería diferente.

A mis abuelos Graciela Gascón Ponce (QEPD), Jaime Medina Sosa (QEPD), Adolfo Montes Daza (QEPD) y Ofelia Galindo García por quererme, apoyarme siempre, darme consejos, ser un gran ejemplo de vida y sobre todo por luchar por los sueños, esto también se lo debo a ustedes.

A toda mi familia, entre mis tíos (Rebeca, Enrique, Beatriz Medina, Gerardo, Adriana Ruiz de Chávez [QEPD], Martha, Joel, Alma, Antonio, Lucila, Gustavo, Blanca, Luis y Beatriz), mis primos (Guadalupe, Margarita, Miguel, Karina, Diego, Gustavito, Marcos, Fernando, Cesar Hiram y Perla) y a todos aquellos que participaron directa o indirectamente en la elaboración de esta tesis.

A mis mascotas, que nunca piden nada a cambio y que siempre están ahí incondicionalmente para alegrarte en los buenos y malos momentos (Max, Morris, Ivy, Hermiona, Pulina, Toña, Pepe, Fito, mis peces y a mi tortuga) y a los que ya no están pero siguen estando en mi corazón (Doc, Dief, Dark, Rocco, Nicky y mis cuyos).

A mi colega Ignacio David González Castillo por apoyarme a realizar juntos este gran proyecto para titularnos, eres como un gran hermano para mí porque crecimos,

AGRADECIMIENTOS

aprendimos uno del otro y sobretodo nos apoyamos en las buenas y en las malas que la vida misma nos ponía en el camino. Te lo agradezco de antemano.

A mis amigos, por todas las palabras de aliento, apoyo, solidaridad y aprecio en estos años de trayectoria escolar, de trabajo, de amistad y de fraternidad: Sinhue, Viridiana, Doña Bety, Don Moisés, Jorge, a la familia Karasiak (Jakob, Josef, Amanda, Jonatan, Kjell y Eva), Niklas Persson, Daniel Undegård, Mayra, Ana Lilia, Jenny, Sandy, Carolina, Angélica, Rocio, Brenda, Gabriela, Edna Alejandra, Karina López, Diego Guespan, Doriceli, Landy, Abelardo, Eduardo, Gina, Ornella, Leticia, Gustavo Miramontes, Alex Arias, Adry, Dana, Pablo Ramírez, Patricia, Arlin Vergara, Ishe Reyes, Luis Alan, Martin Tristán, Alejandra Montserrat, Ben CG, Yolitzí Saldívar, Ivonne, Alma Sánchez, Belevelo Venegas, Esteban, Alberto Montes, Alejandro Osorio, Ariel López, Sandibel Armendáriz, Eloísa Lemus, Priscila Avalos, Héctor Iturbide, Pedro Arenas, Bruno, Pablo Martínez, Zirce, entre muchos otros.

A los clubes oficiales de música en inglés por parte de las disqueras SONY MUSIC MÉXICO, UNIVERSAL MUSIC MÉXICO y WARNER MUSIC MÉXICO, a los que he pertenecido a través de los años, muchas gracias por ayudarme a hacer más amena la lucha por los sueños: Westlife Latinoamérica, Coldplay México, Keane México (The Lotus Mex Dreamers), Maroon 5 México, Tiziano Ferro México, The Wanted México, entre otros.

También quiero dar las infinitas gracias a nuestra directora de tesis de Licenciatura, a la honorable M.C Cintia Quezada Reyes por su gran trabajo en cada detalle, participación activa, motivación, paciencia, disponibilidad y tiempo compartido en el desarrollo de esta tesis; además, por impulsar el desarrollo de nuestra formación profesional. Su apoyo y confianza en mi trabajo y su capacidad para guiar mis ideas ha sido un aporte invaluable, no solamente en el desarrollo de esta tesis, sino también en mi formación como investigador. Las ideas propias, siempre enmarcadas en su orientación y rigurosidad, han sido la clave del buen trabajo que hemos realizado juntos, el cual no se puede concebir sin su siempre oportuna participación.

Finalmente a los maestros de la Facultad de Ingeniería, aquellos que marcaron cada etapa de nuestro camino universitario, y que me ayudaron en asesorías y dudas presentadas en la elaboración de la tesis (M.E Evelyn Salazar Guerrero). Muchas gracias a mi alma mater la Universidad Nacional Autónoma de México. Te extrañaré por siempre porque pasé uno de los mejores momentos en mi vida y espero llenarte de orgullo a futuro como profesionista. Por mi raza hablará el espíritu.

Hay tantas personas (maestros, familiares y amigos) a quien agradecer que no me bastaría la vida para decirles GRACIAS de todo corazón a los que me apoyaron en la realización de este trabajo de tesis y creyeron en mí.

DIOS LOS BENDIGA.

Le grá godeo.

ÍNDICE

	Página
INTRODUCCIÓN	1
CAPÍTULO 1 CONCEPTOS FUNDAMENTALES	7
1.1 CLASIFICACIÓN DE LAS REDES	10
1.1.I TOPOLOGÍA	10
1.1.II TECNOLOGÍA DE TRANSMISIÓN	12
1.1.III ÁREA GEOGRÁFICA	12
1.2 ORGANIZACIONES DE ESTÁNDARES PARA REDES	14
1.3 CAPAS DEL MODELO OSI	17
1.4 MODELO TCP/IP	19
1.5 FAMILIA DE PROTOCOLOS DE INTERNET	21
1.5.I TELNET (TELECOMMUNICATION NETWORK - RED DE TELECOMUNICACIONES)	21
1.5.II SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL, PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED)	23
1.5.III FTP (FILE TRANSFER PROTOCOL, PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)	25
1.5.IV HTTP (HYPERTEXT TRANSFER PROTOCOL, PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO)	27
1.5.V SMTP (SIMPLE MAIL TRANSFER PROTOCOL, PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO)	29
1.5.VI DNS (DOMAIN NAME SERVICE, SISTEMA DE NOMBRES DE DOMINIO)	31
1.5.VII NAT (NETWORK ADDRESS TRANSLATION, TRADUCCIÓN DE DIRECCIÓN DE RED)	32
1.5.VIII ARP (ADDRESS RESOLUTION PROTOCOL, PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN)	35
1.5.IX IP (INTERNET PROTOCOL, PROTOCOLO DE INTERNET)	37
1.5.X TCP (TRANSMISSION CONTROL PROTOCOL, PROTOCOLO DE CONTROL DE TRANSMISIÓN)	39
1.5.XI UDP (USER DATAGRAM PROTOCOL, PROTOCOLO DE DATAGRAMA DE USUARIO)	41
1.6 MEDIOS DE TRANSMISIÓN	43
1.6.I TERRESTRES	43
1.6.II AERÉOS	46
1.7 REDES INALÁMBRICAS (WIRELESS NETWORK)	48
1.7.I LAN INALÁMBRICA	49
1.7.II INTERFAZ DE RED INALÁMBRICA	51

CAPÍTULO 2	COMPONENTES Y MONITOREO DE RED	57
2.1	COMPONENTES DE UNA RED	60
2.1.I	ROUTER	60
2.1.II	HUB (CONCENTRADOR	64
2.1.III	SWITCH	67
2.1.IV	SERVIDORES	69
2.1.V	PANEL DE PARCHEO	72
2.1.VI	RACK	73
2.1.VII	GATEWAY (PUERTA DE ENLACE)	75
2.2	MONITOREO DE RED	77
2.2.I	ENFOQUES	78
2.2. II	CONEXIONES	80
2.2. III	ANÁLISIS DE PAQUETES	81
2.2. IV	ENCADENAMIENTO DE PAQUETES	84
2.2. V	FRAGMENTACIÓN DE PAQUETES IP	85
2.2. VI	PATRONES NORMALES	88
2.2. VII	PATRONES ANORMALES	92
2.2. VIII	TRÁFICO DE RELLENO	93
CAPÍTULO 3	INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA	97
3.1	FUNDAMENTOS TEÓRICOS	100
3.1.I	CONCEPTO DE SEGURIDAD INFORMÁTICA	100
3.1.II	VULNERABILIDAD	102
3.1.III	AMENAZAS	105
3.1.IV	ATAQUES	109
3.2	SERVICIOS DE SEGURIDAD	111
3.3	POLÍTICAS DE SEGURIDAD	115
3.4	MECANISMOS DE SEGURIDAD	118
3.5	SEGURIDAD FÍSICA	120
3.6	SEGURIDAD LÓGICA	122
3.7	HERRAMIENTAS DE MONITOREO	127

CAPÍTULO 4	MÉTODO DE CIFRADO	131
4.1	INTRODUCCIÓN A LA CRIPTOGRAFÍA	134
4.1.I	CRIPTOLOGÍA	134
4.1.II	CRIPTOANÁLISIS	136
4.1.III	CRIPTOGRAFÍA	137
4.2	ALGORITMOS DE CRIPTOGRAFÍA	140
4.2.I	SIMÉTRICOS	140
4.2.II	ASIMÉTRICOS	147
CAPÍTULO 5	INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR	157
5.1	INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR	160
CAPÍTULO 6	DEFENSA EN REDES	177
6.1	SEGURIDAD EN REDES INALÁMBRICAS	180
6.1.I	ACCESS POINT (PUNTO DE ACCESO)	181
6.1. II	SSID (SERVICE SET IDENTIFIER, IDENTIFICADOR DE CONJUNTO DE SERVICIOS)	182
6.1. III	WEP (WIRED EQUIVALENT PRIVACY, PRIVACIDAD EQUIVALENTE AL CABLE)	183
6.1.IV	RADIUS AUTHENTICATION (REMOTE AUTHENTICATION DIAL IN USER SERVICE, AUTENTICACIÓN REMOTA TELEFÓNICA DE SERVICIO DE USUARIO)	184
6.1.V	802.11(X)	185
6.1.VI	NUEVAS TECNOLOGÍAS DE SEGURIDAD	186
6.2	DETECCIÓN DE INTRUSOS	190
6.2.I	SISTEMAS DETECTORES DE INTRUSOS (IDS)	190
6.2.II	FALSOS POSITIVOS	191
6.2. III	FALSOS NEGATIVOS	192
6.2.IV	MÉTODOS DE DETECCIÓN DE INTRUSOS	192
6.2.V	IDENTIFICACIÓN DE ATAQUES	193
6.2.VI	ANÁLISIS DEL TIEMPO DE RESPUESTA DE LOS IDS	194
6.3	AUDITORÍA DE RED	195
6.3.I	CONCEPTO	195
6.3.II	HERRAMIENTAS DE AUDITORÍA	197
6.3.III	MAPEO DE LA RED	198
6.3.IV	MONITORES DE RED	199
6.3.V	AUDITORÍA A FIREWALLS	199

6.3.VI	PRUEBAS DE PENETRACIÓN SOBRE REDES	201
6.3.VII	ANÁLISIS DE LA INFORMACIÓN Y RESULTADOS	202
6.3. VIII	DOCUMENTACIÓN REFERIDA DEL CASO	203
6.3.IX	LOG DE SEGURIDAD	203
6.4	ANÁLISIS FORENSE	204
6.4.I	INTRODUCCIÓN	205
6.4.II	OBTENCIÓN Y PROTECCIÓN DE LA EVIDENCIA	207
6.4.III	ANÁLISIS SOBRE EL SISTEMA	209
6.4.IV	HERRAMIENTAS PARA OBTENER INFORMACIÓN DE LA RED	210
6.4.V	ANÁLISIS DE LA INFORMACIÓN Y RESULTADOS	211
6.5	ENTORNO SOCIAL E IMPACTO ECONÓMICO DE LA SEGURIDAD INFORMÁTICA	212
6.6	NUEVAS TENDENCIAS Y TECNOLOGÍAS	214
6.6.I	CULTURA DE LA SEGURIDAD INFORMÁTICA	214
6.6.II	TECNOLOGÍAS DE PROTECCIÓN	215
6.6.III	TENDENCIA EN ATAQUES	218
CAPÍTULO 7	MANUAL DE PRÁCTICAS	221
7.1	MANUAL DE PRÁCTICAS	224
	CONCLUSIONES	237
	FIGURAS	243
	TABLAS	249
	GLOSARIO DE TÉRMINOS	253
	APÉNDICE A	269
	APÉNDICE B	285
	APÉNDICE C	313
	APÉNDICE D	321
	APÉNDICE E	333
	APÉNDICE F	345
	APÉNDICE G MANUAL DE PRÁCTICAS (VÉASE CD ANEXO)	
	REFERENCIAS	363

INTRODUCCIÓN

INTRODUCCIÓN

Al estar inscrito en la Facultad de Ingeniería cursando la carrera de Ingeniero en Computación y terminar el módulo de Redes y Seguridad, un profesor de la misma área explicó que quieren renovar el plan de estudios del año 2005 y una de esas modificaciones es unir las asignaturas de Seguridad Informática I y II, en el nuevo plan que está en construcción nombrando a la nueva asignatura como Seguridad Informática Avanzada. Además, incluiría un laboratorio para poner en práctica lo que se aprende en teoría pero aún no se tiene planeado que temas abarcaría y mucho menos existe un diseño del programa; por tal motivo, se decidió diseñar un conjunto de prácticas que complementen el aprendizaje de la nueva asignatura así como del programa de laboratorio. En las prácticas se le mostrará al lector los diferentes métodos de hackeo que existen y las herramientas que dan mejores resultados al momento de defenderse de un ataque informático o en su caso de realizar el ataque; además, las prácticas se diseñaron para ser realizadas en un máximo de dos horas que corresponde al tiempo que dura el laboratorio. También, se incluye la tabla de costos, especificaciones del equipo, dispositivos de red, software libre y con licencia para poderlo llevar a futuro como proyecto en la Facultad de Ingeniería.

Se les invita a los alumnos y a los profesores de la Facultad de Ingeniería a leer el *Manual de Prácticas para el laboratorio de la asignatura Seguridad Informática Avanzada* y a los que estén interesados en las redes y seguridad para contar con una noción básica de cómo un perpetrador puede atentar contra la información de terceras personas. Si el alumno está por concluir o ya concluyó la carrera de Ingeniería en Computación con este manual podrá aplicar los diferentes casos en contra de la seguridad que pueden suceder.

El objetivo principal de este trabajo es:

- **Diseñar un conjunto de prácticas para complementar el aprendizaje del laboratorio de la asignatura de Seguridad Informática Avanzada.**
 - a) Mostrar a los participantes los diferentes métodos de hackeo que existen para defenderse de un ataque informático.
 - b) Identificar las posibles vulnerabilidades y amenazas en la seguridad física y lógica para identificar y corregir los problemas más habituales.
 - c) Determinar que herramientas son mejores al momento de proteger los diferentes activos para obtener los mejores resultados al analizar el equipo que fue atacado.

A continuación se da una breve descripción del contenido de cada capítulo:

INTRODUCCIÓN

Capítulo 1 - Conceptos Fundamentales

Se toman en cuenta las clasificaciones de las redes, organizaciones de estándares para redes, capas del modelo OSI, modelo TCP/IP, familia de protocolos de Internet, medios de transmisión y las redes inalámbricas; al unir todos los elementos anteriores aumentan la eficiencia al compartir los datos de forma rápida y reduce los costos de una empresa u organización.

Capítulo 2 - Componentes y Monitoreo de Red

Se ven los componentes de una red como es el router, switch, servidores entre otros elementos que existen además del monitoreo de red en donde se ven las conexiones, análisis de paquetes, tráfico de relleno, encadenamiento de paquetes, patrones normales y anormales.

Capítulo 3 - Introducción a la Seguridad Informática

Se definen los conceptos de vulnerabilidades, amenazas, ataques, herramientas de monitoreo, seguridad física y lógica, mecanismos de seguridad, los servicios y políticas de seguridad.

Capítulo 4 - Método de Cifrado

Se analizan las técnicas que tratan de proteger la información como es la criptología, criptoanálisis, criptografía así como los algoritmos de criptografía simétricos y asimétricos que se encargan de transformar un mensaje inteligible en otro que no lo es usando una clave que solo el emisor y el destinatario conocen, para que después puedan devolverlo a su forma original.

Capítulo 5 - Introducción a la Arquitectura Cliente/Servidor

Se contempla el procesamiento cooperativo de la información por medio de un conjunto de procesadores, en el cual múltiples clientes, distribuidos geográficamente, solicitan requerimientos a uno o más servidores centrales. Siendo ésta una arquitectura distribuida, permite a los usuarios finales obtener acceso a la información de forma transparente aun en entornos multiplataforma.

INTRODUCCIÓN

Capítulo 6 - Defensa en Redes

Se estudia la seguridad en redes inalámbricas, detección de intrusos, auditoría de red, análisis forense, entorno social e impacto económico de la seguridad informática, nuevas tendencias y tecnologías como las interconexiones que se hacen a nivel mundial a la nube donde se guarda información sensible.

Capítulo 7 - Manual de Prácticas

Correspondiente al trabajo de tesis, se realizan las prácticas del laboratorio de la asignatura de Seguridad Informática Avanzada donde se explican los métodos y elementos que le permitan planificar, identificar y analizar las amenazas, vulnerabilidades y ataques en sistemas y redes de cómputo, además, aplicará las estrategias de monitoreo y herramientas que le ayuden a implementar la seguridad informática dentro de una organización u empresa.

CAPÍTULO 1

CONCEPTOS FUNDAMENTALES



Una *red de comunicación*, es un conjunto de equipos y facilidades que proporcionan un servicio consistente en la transferencia de información entre usuarios situados en puntos geográficos distantes.

En su nivel más elemental, una red de equipos consiste en dos equipos conectados entre sí con un cable que les permite compartir datos. Todas las redes de equipos, independientemente de su nivel de sofisticación, surgen de este sistema tan simple.

Las redes de equipos surgen como respuesta a la necesidad de compartir datos de forma rápida. Los equipos personales son herramientas potentes que pueden procesar y manipular rápidamente grandes cantidades de datos, pero no permiten que los usuarios compartan los datos de forma eficiente.

Se le llama *dispositivo* a cualquier entidad que está conectada a una red. Existen 2 tipos:

- a) *Dispositivo local (transmisor)*
Origina la comunicación a través de una red.

- b) *Dispositivo remoto (receptor)*
Aquel al que se tiene acceso desde el dispositivo local.

El *medio* es el *ambiente* físico usado para conectar miembros (computadoras, dispositivos, etcétera.). Entonces, una *red de computadoras*, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos *que* envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos.

Una *red de computadoras* es un conjunto de terminales, nodos, servidores y elementos de propósito especial que interaccionan entre sí al estar conectados por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de intercambiar información, compartir recursos y ofrecer servicios.

Una red de equipos se emplea porque ésta aumenta la eficiencia y reduce los costos. Las redes de equipos alcanzan estos objetivos de tres formas principales:

- ✓ Compartiendo información (o datos).
- ✓ Compartiendo hardware y software.
- ✓ Centralizando la administración y el soporte.

1.1 CLASIFICACIÓN DE LAS REDES

1.1.1 TOPOLOGÍA

La *topología* es la forma como se interconectan los diferentes nodos y computadoras en una red (físicamente) que se muestra en la figura 1.1.

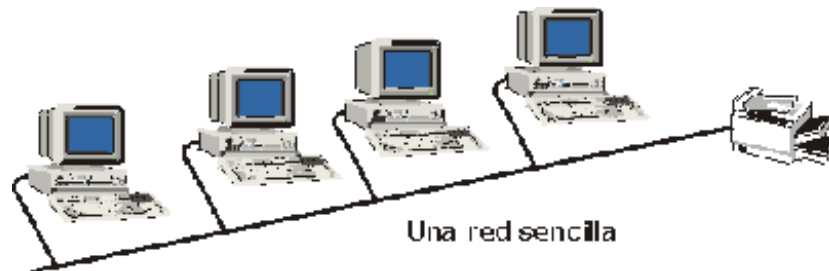
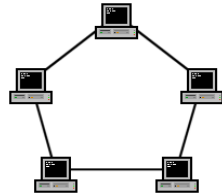


Figura 1.1 Red sencilla

En la tabla 1.1 se muestran los diferentes tipos de topología en las redes.

<p><i>Estrella:</i> Los equipos se interconectan a un miembro central.</p> <p>Red en topología de estrella</p>	<p><i>Bus:</i> Comparten el mismo canal de comunicaciones.</p> <p>Red en topología de bus</p>
<p><i>Árbol:</i> Interconexión de miembros con miembros en forma jerárquica.</p> <p>Red en topología de árbol</p>	<p><i>Malla:</i> Interconexión de cada uno de los miembros con el resto.</p> <p>Red con topología de malla</p>

Anillo: Todas las conexiones están conectadas entre sí formando un anillo.

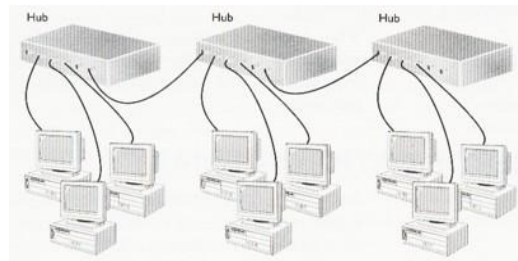
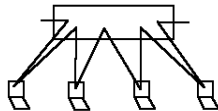


Red con topología de anillo

Mixtas: Se da cualquier combinación de las anteriores. Las más comunes son:

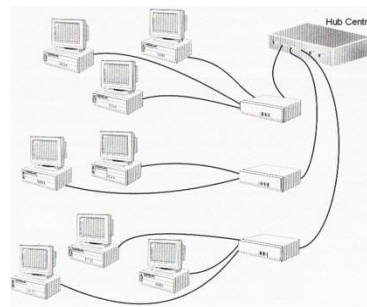
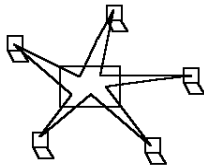
- ✓ Bus-Estrella
- ✓ Anillo-Estrella

Bus-Estrella: La red es un bus que se cablea físicamente como una estrella por medio de concentradores.



Topología Bus Estrella. Se reemplazan las computadoras miembro de una topología bus con los hubs de una topología estrella.

Anillo-Estrella: Físicamente la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo. Usada para facilitar la administración de la red.



Topología Anillo Estrella. Los hubs más pequeños están internamente interconectados como en un anillo y conectados al mismo tiempo con el hub principal como en una topología en estrella.

1.1.II TECNOLOGÍA DE TRANSMISIÓN

Al crear una red se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen dicha transmisión de datos. Al primer factor se le llama nivel físico y al segundo protocolo.

El protocolo es un conjunto de normas que regulan la comunicación al establecer, mantener y cancelar la conexión entre los distintos componentes de una red informática.

En el nivel físico generalmente hay señales de voltaje que tienen un significado predefinido. Esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma como se accede a esos paquetes determina la tecnología de transmisión. Se divide en dos grandes rubros:

a) Redes de difusión (broadcast)

Tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos que envía una máquina son recibidos por todos los demás.

b) Redes punto a punto (point-to-point)

Consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino un paquete puede tener que visitar primero una o más máquinas intermedias y puede haber múltiples rutas diferentes.

1.1.III ÁREA GEOGRÁFICA

Las redes de computadoras se clasifican según su tamaño, es decir, por la extensión física en la que se ubican sus componentes, desde una red hogareña hasta una empresa, un campus, una ciudad, un país o, incluso, el mundo entero. La clasificación determina los medios de conexión, los dispositivos y los protocolos requeridos para operarlas.

En la tabla 1.2 se muestra la clasificación de las redes por área geográfica.

Tabla 1.2 Clasificación de las redes por área geográfica

Distancia entre procesadores	Procesadores ubicados en (la) mismo (a)	
0.1 [m]	Tarjeta de circuitos	Máquina de flujo de datos
1 [m]	Sistema	Multicomputadora
10 [m]	Cuarto	Red de área local
100 [m]	Edificio	
1 [km]	Campus	
10 [km]	Ciudad	Red de área metropolitana
100 [km]	País	Red de área amplia
1000 [km]	Continente	

De acuerdo con el área geográfica que ocupa la red, se cuenta con los siguientes tipos de redes:

- a) LAN (Local Area Network, Red de área local): Interconecta miembros dentro de un área geográfica de tamaño moderado. Ejemplos de redes LAN:
 - ✓ Ethernet
 - ✓ Token Ring
 - ✓ Fiber Distributed Data Interface (FDDI)

- b) WAN (Wide Area Network, Red de área amplia): Interconecta miembros que están ampliamente separados geográficamente. Algunas modalidades son:
 - ✓ Red de datos de servicios integrados (ISDN)
 - ✓ Frame relay
 - ✓ Servicio de datos conmutados multimegabit (SMDS)
 - ✓ Redes de modo de transferencia asíncrona (ATM)

- c) MAN (Metropolitan Area Network, Red de área metropolitana): Interconecta miembros que cubren un área metropolitana. Tienen variadas aplicaciones, las principales son:
 - ✓ Puede ser pública o privada
 - ✓ Soporta voz y datos
 - ✓ DQDB (Distributed Queue Dual Bus, Bus Dual de Cola Distribuida)

- d) PAN (Personal Area Network, Red de área personal): Pequeñas redes de computadoras que se encuentran en casas privadas.

- e) GAN (Global Area Network, Red de área global): Colección de WAN que cubre el globo.

1.2 ORGANIZACIONES DE ESTÁNDARES PARA REDES

Se ha desarrollado una gran cantidad de estándares de redes que definen:

- ✓ Interfaces de hardware
- ✓ Protocolos de comunicación
- ✓ Arquitectura de redes

Los estándares de redes establecen reglas o regulaciones específicas que deben ser observadas.

Para que un producto o industria sea económica y técnicamente estable, es necesario tener un grado de estandarización cuyo marco de normalización es complementado a través de un nivel físico y un nivel conceptual.

1. El nivel físico especifica cosas como tipo de cables, conectores, etc.
2. El nivel conceptual son correspondencias lógicas y detalles de organización que no son evidentes de un examen físico del producto o sistema.

Sus principales ventajas son:

1. Un estándar asegura que haya un gran mercado para un equipo y programa en particular.
2. Un estándar permite que los productos de muchos vendedores se comuniquen, lo que le da a los usuarios más flexibilidad en la selección y usos en equipos.

La principal desventaja de los estándares es que congelan las tecnologías.

Las organizaciones de estandarización son organismos encargados de establecer los diferentes estándares utilizados en diferentes áreas: telecomunicaciones, redes, sistemas móviles, etcétera, a nivel mundial. Existe una variedad muy grande de organizaciones de estandarización en el mundo, aquí se presentan algunas de ellas.

- a) ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION – ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN)

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos.

Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional; por lo tanto, no tiene autoridad para imponer sus normas a ningún país.

b) ITU (INTERNATIONAL TELECOMMUNICATION UNION - UNIÓN INTERNACIONAL DE TELECOMUNICACIONES)

Es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. En general, la normativa generada por la ITU está contenida en un amplio conjunto de documentos denominados Recomendaciones, agrupados por Series.

Cada serie está compuesta por las Recomendaciones correspondientes a un mismo tema. Aunque en las Recomendaciones nunca se ordena, solo se recomienda su contenido, a nivel de relaciones internacionales es considerado como mandatorio por las Administraciones y Empresas Operadoras.

c) IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS - INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS CAPACITADOS)

Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías. Promueven la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información electrónica y ciencias en general.

d) ANSI (AMERICAN NATIONAL STANDARDS INSTITUTE, INSTITUTO NACIONAL ESTADOUNIDENSE DE ESTÁNDARES)

Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. Coordina estándares del país estadounidense con estándares internacionales, de tal modo que los productos de dicho país puedan usarse en todo el mundo.

e) NOM (NORMA OFICIAL MEXICANA)

Sirve para describir, de manera detallada, la forma, el formato y la documentación con que deben cumplir (basados en la Constitución Política de los Estados Unidos Mexicanos de 1917) y los reglamentos en México. Una NOM tiene el mismo poder que una ley.

f) EIA (ELECTRONIC INDUSTRIES ALLIANCE - ALIANZA DE INDUSTRIAS ELECTRÓNICAS)

Es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos, cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

g) EL FÓRUM ATM (ASYNCHRONOUS TRANSFER MODE - MODO DE TRANSFERENCIA ASÍNCRONA)

Se inició en octubre de 1991 por un conjunto de 4 empresas de ordenadores y telecomunicaciones. Desde su comienzo, ha visto un crecimiento sin precedentes, hasta junio de 1994 tenía alrededor de 500 miembros. Los actuales miembros están agrupados en proveedores del equipo, los que fabrican los conductores, los proveedores de servicio, los transportadores y los usuarios finales.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Éste último estructura cada red en 7 capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a 4 capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

1.3 CAPAS DEL MODELO OSI

El modelo OSI (Open System Interconnection - interconexión de sistema abierto), es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones, separa la compleja operación de una red en elementos más simples y proporciona una forma de entender cómo operan los dispositivos en una red; consta de 7 capas (figura 1.2) en las cuales se detalla cómo se hace una conexión entre computadoras; fue creado por la Organización Internacional para la Estandarización en el año 1984.



Figura 1.2 Modelo OSI conformado por 7 capas

1. Capa Física (Physical)

Controla la transmisión de la cadena de bits sobre el medio físico definiendo parámetros como voltaje a utilizar y duración del voltaje, solo trabaja con bits. Los bits son transformados en pulsos eléctricos, en luz o en radio frecuencia para ser enviados según sea el medio en que se propaguen.

2. Capa de Enlace de datos (Data Link)

Responsable de la confiabilidad en el envío de información por parte de la capa física, se encarga de iniciar, mantener y terminar una comunicación punto a punto, detecta y elimina errores. Transforma los voltios en tramas y las tramas en voltios.

3. *Capa de Red (Network)*

Lleva a cabo el direccionamiento lógico que tiene carácter jerárquico. Establece la ruta necesaria a seguir para enviar la información entre dos nodos locales o remotos sobre una red.

4. *Capa de Transporte (Transport)*

Garantizar la confiabilidad del enlace en la red al proveer la corrección de errores y el control del flujo entre los dos puntos finales conectados en la red. Los datos son divididos en segmentos identificados con un encabezado y con un número de puerto que identifica la aplicación de origen.

5. *Capa de Sesión (Session)*

Establece, administra y termina la conexión a nivel usuario y administra la interacción entre los sistemas finales estableciendo el tipo de comunicación ya sea simple, half o full duplex.

6. *Capa de Presentación (Presentation)*

Transforma datos para proveer una interfaz común con el usuario. Los datos formateados se proveen de diversas funciones de conversión y codificación que se aplican a los datos provenientes de la capa de aplicación.

7. *Capa de Aplicación (Application)*

Es la única capa que no presta servicio a otro puesto ya que es la capa de nivel superior del modelo OSI directamente relacionado con el usuario (envío de archivos, conexión remota, etc.).

1.4 MODELO TCP/IP

Es la base de Internet con la cual se comunica todo tipo de dispositivos, computadoras con diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

El modelo TCP/IP consta de 4 capas, las cuales se encargan de determinados aspectos de la comunicación y a su vez brindar un servicio específico (figura 1.3).



Figura 1.3 Modelo TCP/IP conformado por 4 capas

1. Capa de Acceso a red

Asignación de direcciones IP a las direcciones físicas, el encapsulamiento de los paquetes IP en tramas; basándose en el tipo de hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

2. Capa de Internet

Seleccionar la mejor ruta para enviar paquetes por la red; los principales protocolos que operan en esta capa son IP (enrutamiento de paquetes), ICMP (control y envío de mensajes), ARP (determina la dirección de la capa de enlace de datos) y RARP (determina las direcciones IP cuando se conoce la dirección MAC).

3. Capa de Transporte

Transporte desde el host origen hacia el host destino; forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor.

4. Capa de Aplicación

Maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo combinando todas las aplicaciones en una sola capa y asegurando que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente; los principales protocolos son:

- a. FTP (File Transfer Protocol - Protocolo de transferencia de archivos)
- b. TFTP (Trivial File Transfer Protocol - Protocolo trivial de transferencia de archivos)
- c. NFS (Network File System - Sistema de archivos de red)
- d. SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo)
- e. TELNET (Telecommunication Network - Red de Telecomunicaciones)
- f. SNMP (Simple Network Management Protocol - Protocolo Simple de Administración de Red)
- g. DNS (Domain Name System - Sistema de denominación de dominio)

Todos los protocolos que pertenecen al conjunto de protocolos TCP/IP se encuentran en los tres niveles superiores de este modelo, tal como se muestra en la figura 1.4.

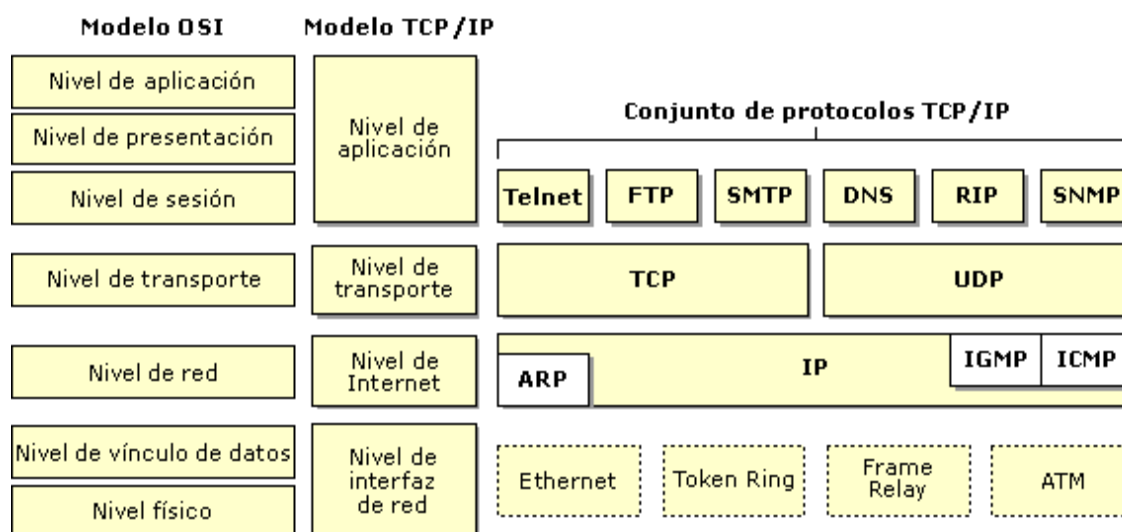


Figura 1.4 Conjunto de protocolos del modelo TCP/IP junto a la comparativa del modelo OSI

1.5 FAMILIA DE PROTOCOLOS DE INTERNET

Es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

Se denomina TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse y son los más utilizados.

Está diseñado para cumplir una cierta cantidad de criterios, entre ellos:

1. Dividir mensajes en paquetes
2. Usar un sistema de direcciones
3. Enrutar datos por la red
4. Detectar errores en las transmisiones de datos

1.5.1 TELNET (TELECOMMUNICATION NETWORK -RED DE TELECOMUNICACIONES)

Es un protocolo que permite conectar terminales y aplicaciones en Internet proporcionando las reglas básicas para vincular a un cliente con un intérprete de comandos.

Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits; brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

Telnet tiene tres conceptos principales: NVT (Virtual Network Terminal - Terminal Virtual de Red), opciones negociadas y reglas de negociación.

a) NVT

Con el surgimiento de internet cada sesión de terminal tenía su propia manera de controlar el flujo de datos entrantes y salientes. Comenzaron a desarrollar adaptadores para cada tipo de terminal con el fin de tener interoperabilidad entre sistemas, pero con el tiempo decidieron programar una interfaz estándar denominada NVT para que cualquier host ya sea cliente o servidor se comuniquen con otro host sin conocer sus características.

b) Opciones negociadas

Permite el uso de funciones avanzadas denominadas opciones, donde el cliente y el servidor inician solicitudes de autorización desde el sistema remoto, donde cada parte puede negociar las siguientes opciones (véase tabla 1.3):

Tabla 1.3 Opciones negociadas de Telnet

Opciones negociadas de Telnet		
Solicitud	Respuesta	Interpretación
DO	WILL	El remitente comienza utilizando la opción
	WON'T	El remitente no debe utilizar la opción
WILL	DO	El remitente comienza utilizando la opción después de enviar <i>DO</i>
	DON'T	El remitente no debe utilizar la opción
DON'T	WON'T	El remitente indica que ha desactivado la opción
WON'T	DON'T	El remitente indica que el remitente debe desactivar la opción

Así cada parte puede enviar una solicitud para utilizar una opción y la otra parte debe responder si acepta o no el uso de la opción.

c) Reglas de negociación

Permiten evitar situaciones de enrollo automático que es cuando una de las partes envía solicitudes de negociación de opciones a cada confirmación de la otra parte. Las reglas para la negociación son las siguientes:

- ✓ Las solicitudes solo deben enviarse cuando se cambia de modo.
- ✓ Si una de las partes recibe solicitud de cambio de modo, solo debe confirmar su recepción si todavía no se encuentra en el modo apropiado.
- ✓ Solo debe insertarse una solicitud en el flujo de datos en el lugar en el que surte efecto.

Las ventajas y desventajas de telnet se muestran a continuación:

1. *Ventajas de telnet*

- ✓ La transmisión de datos consiste solo en enviar bytes en el flujo TCP.
- ✓ Especifica los datos que deben agruparse de manera predeterminada.
- ✓ Los datos se envían línea por línea para prevenir fallas.
- ✓ Al transmitir el byte 255, el siguiente byte se interpreta como un comando.

2. *Desventajas de telnet:*

- ✓ No utiliza la autenticación ya que se encuentra separado de las aplicaciones que lo utilizan.
- ✓ No es un protocolo de transferencia de datos seguro ya que transmite en la red como texto sin codificar.
- ✓ Cuando se conecta un host remoto a un equipo que funciona como servidor solo se le puede asignar el puerto 23.

1.5.II **SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL, PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED)**

Permite a los administradores de la red monitorear y controlar el status de dispositivos conectados a internet para diagnosticar posibles problemas.

El sistema de administración se basa en dos elementos: un supervisor y un agente (figura 1.5).

- a) Supervisor: es la terminal que permite al administrador de red realizar solicitudes de administración; los elementos de la red pueden ser: puentes, concentradores, routers o servidores.
- b) Agente: es aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local.

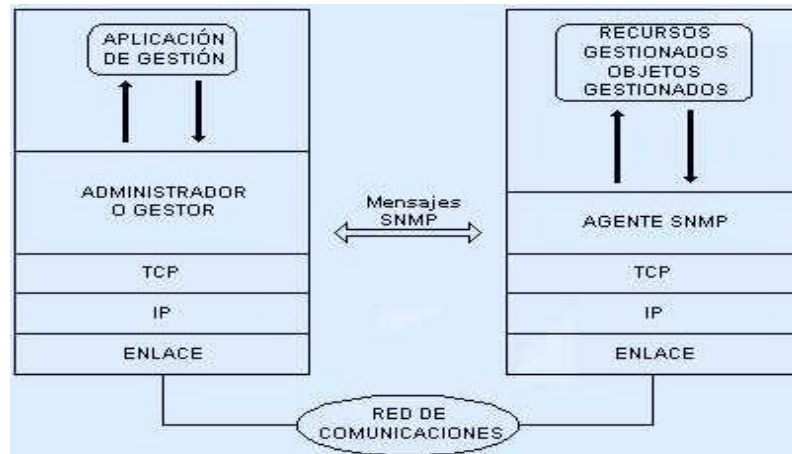


Figura 1.5 Estructura del protocolo SNMP

Existen 3 tipos de versiones de SNMP, éstas y sus características se muestran a continuación:

a) SNMPv1:

- ✓ Utiliza UTP como medio de envío.
- ✓ Es un protocolo de nivel de aplicación (tiene por objetivo *La gestión de red*).
- ✓ Utiliza el puerto 162 para el gestor y el puerto 161 para el agente.
- ✓ Tiene dos tipos de solicitudes de información: petición (encuesta o Poll) de gestor a agente y notificación no solicitada (Traps) de agente a gestor.

b) SNMPv2:

- ✓ Se mejoran los tipos de datos (contadores de 64bits).
- ✓ Se mejora la documentación de cada objeto (Se añade la Cláusula Units)
- ✓ Se crean nuevas convenciones para crear y eliminar filas en una tabla
- ✓ Se implementan dos tipos de MIB's (Management Information Base, Base de Información Gestionada):
 - MIB SNMP v2: Información de agentes, protocolos, configuración, agentes y gestores
 - M2M (Manager To Manager) Para sistemas de gestión distribuidos

c) SNMPv3:

- ✓ Protección con enmascaramiento de datos
- ✓ Modificación de flujo de mensajes
- ✓ Revelación de contenidos
- ✓ Modificación de mensajes.
- ✓ No incluye protección a ataque DoS (Denegación de servicio) o el análisis del tráfico.
- ✓ Modelo de seguridad orientado a usuarios (USM User-Based Security Model)
- ✓ Modelo de configuración orientado en vistas (VACM View-Based Access Control Model)

1.5.III FTP (FILE TRANSFER PROTOCOL, PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)

El protocolo FTP como su nombre lo indica sirve para transferir archivos; inicia en 1971 cuando se desarrolló un sistema de transferencia de archivos entre equipos del Instituto Tecnológico de Massachusetts.

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP, teniendo como objetivo el siguiente: permitir a los equipos remotos que puedan compartir archivos, permitir una transferencia de datos eficaz y permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor; utiliza habitualmente el puerto de red 20 y el 21.

El modelo FTP (figura 1.6) está incluido dentro del modelo cliente-servidor, un equipo envía órdenes (cliente) y el otro espera solicitudes para llevar a cabo acciones (servidor).

Durante una conexión FTP se abren dos canales de transmisión:

1. Un canal de comandos.
2. Un canal de datos.

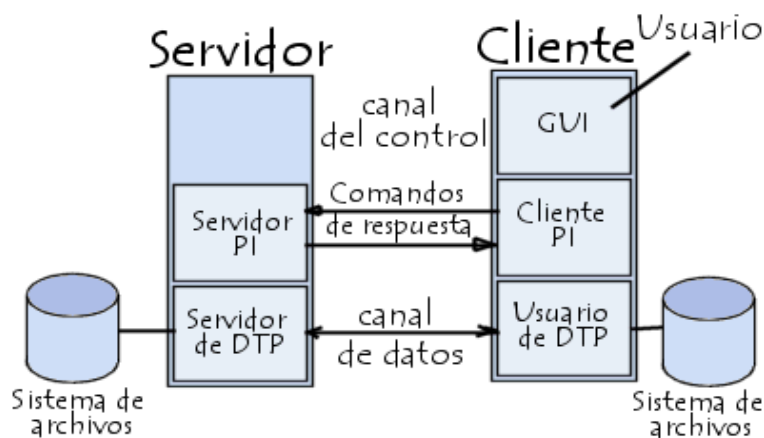


Figura 1.6 Estructura del protocolo FTP

El cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- a) DTP (Proceso de transferencia de datos): proceso encargado de establecer la conexión y de administrar el canal de datos.

- b) PI (Intérprete de protocolo): interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de comandos. Es diferente en el cliente y el servidor:
- ✓ *SERVIDOR PI*: es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal, establece la conexión y recibe los comandos FTP del USUARIO PI para responderle y ejecuta el SERVIDOR de DTP.
 - ✓ *USUARIO PI*: es responsable de establecer la conexión con el servidor FTP, enviar los comandos FTP, recibir respuestas del SERVIDOR PI y de controlar al USUARIO de DTP si es necesario.

El protocolo indica que los canales deben permanecer abiertos durante la transferencia de datos para que el servidor pueda detener una transmisión si el canal de control es interrumpido durante la transmisión.

Existen diferentes formas de acceso al servidor FTP, las cuales son:

a) Modo usuario

En este modo se tienen privilegios y acceso a todo el sistema de archivo del servidor FTP, se pueden modificar los archivos ya existentes y subir nuestros propios ficheros; con el uso de una cuenta de usuario en la cual debe autenticarse para tener el acceso; el servidor guarda la información de las distintas cuentas para que puedan acceder a él.

b) Modo anónimo

Brindan el servicio libremente a todos los usuarios permitiéndoles acceder a los archivos sin necesidad de tener una cuenta de usuario.

Al tener un servidor en modo anónimo no se necesita ninguna contraseña preestablecida pero se tendrá que teclear la palabra *anonymous* solo para ese momento a un que normalmente se suele utilizar la propia dirección de correo electrónico. Al estar conectado se tiene acceso a los archivos del servidor FTP donde solo se puede leer y copiar los documentos que sean públicos o los que indique el administrador del servidor sin tener los privilegios que un usuario normal posee.

Un servidor FTP anónimo sirve para depositar archivos muy grandes que no tienen mucha utilidad si no son transferidos a la máquina del usuario.

1.5.IV HTTP (HYPERTEXT TRANSFER PROTOCOL, PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO)

HTTP es un protocolo orientado a objetos genéricos y sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse.

Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor (figura 1.7). Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como *user agent* (agente del usuario).

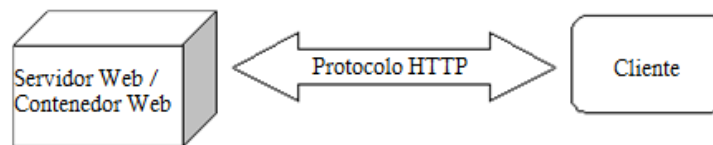


Figura 1.7 Arquitectura 2-capas (Cliente/Servidor)

A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etcétera.

Una transacción HTTP (figura 1.8) consiste básicamente en:

- a) Conexión: El establecimiento de una conexión del cliente con el servidor. El puerto TCP/IP 80 es el puerto bien conocido.
- b) Solicitud: El envío por parte del cliente de un mensaje de solicitud al servidor.
- c) Respuesta: El envío por parte del servidor de una respuesta al cliente.
- d) Cierre: El cierre de la conexión por parte del cliente y el servidor.

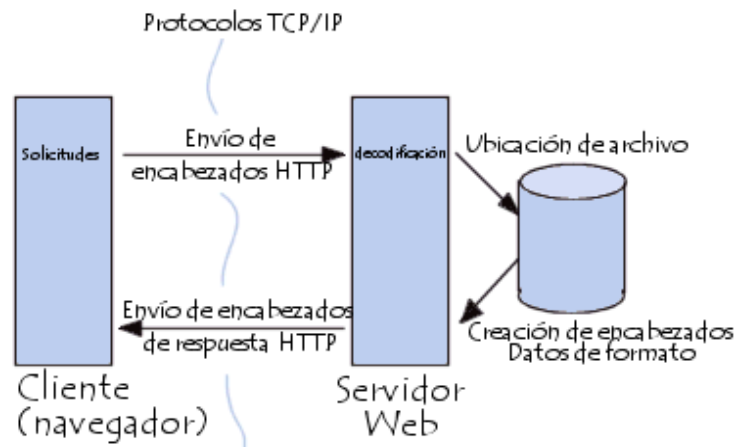


Figura 1.8 Comunicación entre el navegador y el servidor por el puerto 80/TCP

El desarrollo de aplicaciones web necesita frecuentemente mantener un estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de *sesión*, y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

HTTP ha pasado por múltiples versiones del protocolo, muchas de las cuales son compatibles con las anteriores. El RFC 2145 describe el uso de los números de versión de HTTP. El cliente le dice al servidor al principio de la petición la versión que usa, y el servidor usa la misma o una anterior en su respuesta.

HTTP define 8 métodos (o comandos) que indican la acción que desea que se efectúe sobre el recurso identificado, éstos se listan a continuación.

- a) **HEAD**: Solicita el encabezado del recurso ubicado en la URL especificada
- b) **GET**: Solicita el recurso ubicado en la URL especificada
- c) **POST**: Envía datos al programa ubicado en la URL especificada
- d) **PUT**: Envía datos a la URL especificada
- e) **DELETE**: Borra el recurso especificado.
- f) **TRACE**: Solicita al servidor que envíe de vuelta en un mensaje de respuesta, en la sección del cuerpo de entidad, toda la data que reciba del mensaje de solicitud.
- g) **OPTIONS**: Devuelve los métodos HTTP que el servidor soporta para un URL específico.
- h) **CONNECT**: Este método se reserva para uso con proxys. Permite que un proxy pueda dinámicamente convertirse en un túnel.

El código de estado es un número de 3 dígitos que indica si la petición ha sido atendida satisfactoriamente o no, y en caso de no haber sido atendida, indica la causa. Los códigos se dividen en cinco clases definidas por el primer dígito del código de estado (tabla 1.4).

Tabla 1.4 Ejemplos de códigos de estado

100, continuar.	404, no encontrado.
101, cambio de protocolo.	405, método no permitido.
200, éxito.	406, no se puede aceptar.
201, creado.	407, se requiere autenticación proxy.
202, aceptado.	408, límite de tiempo de la petición.
203, información no autoritativa.	409, conflicto.
204, sin contenido.	410, gone.
205, contenido restablecido.	411, tamaño requerido.
206, contenido parcial.	412, falla una precondition.
300, múltiples elecciones.	413, contenido de la petición muy largo.
301, movido permanentemente.	414, URL de la petición muy largo.
302, movido temporalmente.	415, campo media typerequerido.
303, ver otros.	500, error interno del servidor.
304, no modificado.	501, no implementado.
305, usar proxy.	502, puerta de enlace errónea.
400, petición errónea.	503, servicio no disponible.
401, no autorizado.	504, tiempo límite de la puerta de enlace.
402, pago requerido.	505, versión de protocolo HTTP no soportada.
403, prohibido.	

1.5.V SMTP (SIMPLE MAIL TRANSFER PROTOCOL, PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO)

Es un protocolo de la capa de aplicación basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos. Está definido en el RFC 2821 y es un estándar oficial de Internet.

Este protocolo es el estándar de Internet para el intercambio de correo electrónico. El objetivo de SMTP es transferir correo electrónico fiable y eficiente.

En 1982 se diseñó el primer sistema para intercambiar correos electrónicos en ARPANET, definido en los *Request for comments* RFC 821 y RFC 822. La primera de ellas define este protocolo y la segunda el formato del mensaje que este protocolo debía transportar.

Con el tiempo se ha convertido en uno de los protocolos más usados en internet.

Las características de SMTP son:

- ✓ SMTP está basado en el modelo cliente-servidor.
- ✓ Las respuestas del servidor constan de un código numérico de tres dígitos, seguido de un texto explicativo.
- ✓ SMTP utiliza *órdenes*, réplicas o datos son líneas de texto, delimitadas por el carácter <CR><LF>. Las réplicas tienen un código numérico al comienzo de la línea.
- ✓ Los comandos y las respuestas no son sensibles a mayúsculas y minúsculas. Sin embargo, algunos argumentos utilizan paréntesis angulares literalmente.
- ✓ En el conjunto de protocolos TCP/IP, el SMTP usa normalmente el puerto 25 en el servidor para establecer la conexión.

Cuando un servidor de SMTP requiere transmitir un mensaje a otro servidor SMTP, el emisor establece una conexión con el receptor. Esta conexión es unidireccional, es decir, el emisor puede enviar correo al receptor, pero durante esa conexión, el receptor no puede enviar correo al emisor. Si el receptor tiene que enviar correo al emisor, tiene que esperar a que finalice la conexión establecida y establecer otra en sentido contrario, cambiando los papeles de emisor y receptor.

Los mensajes pueden tener como destino el receptor o un intermediario para llegar a un destino más lejano. Una vez que el servidor recibe el mensaje finalizado con un punto puede almacenarlo si es para un destinatario que pertenece a su dominio, o bien retransmitirlo a otro servidor para que finalmente llegue a un servidor del dominio del receptor.

El funcionamiento de SMTP:

1. Cuando un cliente establece una conexión con el servidor SMTP, espera a que éste envíe un mensaje.
2. Se envía un HELO desde el cliente. Con ello el servidor se identifica. Esto puede usarse para comprobar si se conectó con el servidor SMTP correcto.
3. El cliente comienza la transacción del correo con la orden MAIL FROM. Como argumento de esta orden se puede pasar la dirección de correo al cual el servidor notificará cualquier fallo en el envío del correo.
4. Ya se le ha dicho al servidor que se desea mandar un correo, ahora hay que decirle a quién, para esto es RCPT TO:<destino@host>. Se pueden mandar tantas órdenes RCPT como destinatarios del correo se quiera.
5. Una vez enviados todos los RCPT, el cliente envía una orden DATA para indicar que a continuación se envían los contenidos del mensaje.
6. Ahora el cliente envía el cuerpo del mensaje, línea a línea. Una vez finalizado, se termina con <CRLF>.<CRLF> (última línea será un punto).
7. Tras el envío, el cliente, si no tiene que enviar más correos, con la orden QUIT corta la conexión.

1.5.VI DNS (DOMAIN NAME SERVICE, SISTEMA DE NOMBRES DE DOMINIO)

Permite traducir el nombre de dominio a dirección IP y viceversa. Pero internet solo funciona con direcciones IP, por lo cual el DNS permite que las personas usen nombres de dominio bastante más simples de recordar aunque pueden causar conflictos, puesto que dichos nombres son activos valiosos en algunos casos y pueden ser marcas o nombres ya registrados ante la Ley con lo cual pueden causar demandas si no se elige un nombre de dominio adecuado.

DNS en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Se basa en un árbol que define la jerarquía entre los dominios y los sub-dominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda.

Los componentes del dominio tienen un servidor primario y varios secundarios con la misma autoridad para responder por ese dominio; el servidor primario es el único con derecho para hacer modificaciones ya que tiene la copia maestra y los secundarios copian la información desde él. Cuando el DNS primario no está disponible entra el DNS secundario para responder la petición.

Para que el sistema DNS funcione adecuadamente se utilizan tres componentes principales (figura 1.9):

1. Clientes DNS: El programa cliente DNS se ejecuta en la computadora del usuario y genera peticiones DNS de resolución de nombres a un servidor DNS
2. Servidores DNS: Contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.
3. Zonas de autoridad: porciones del espacio de nombres de dominio que almacenan los datos.



Figura 1.9 Sistema DNS

Existen 3 tipos de servidores DNS:

- a) Preferidos: Guardan los datos de un espacio de nombres en sus ficheros.
- b) Alternativos: Obtienen los datos de los servidores primarios a través de una transferencia de zona.
- c) Locales o caché: Funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres; ya que consultan a los servidores secundarios para dar la solución al problema.

Al conectarse a Internet, el proveedor asigna una IP que habitualmente cambia cada vez que se conecta de nuevo a esto se le llama IP dinámica; a menos que se tenga contratado un servicio de IP estática en cuyo caso siempre se asignaría la misma IP.

Un DNS dinámico usa un subdominio para que siempre se dirija al servidor en casa; sea cual sea la IP actual, permitiendo la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres. El software que usa es el de un servidor en una computadora con dirección IP dinámica, el cual lo dan los proveedores con el que se contrata el servicio.

1.5.VII NAT (NETWORK ADDRESS TRANSLATION, TRADUCCIÓN DE DIRECCIÓN DE RED)

Traduce las IP privadas de una red casera en una IP pública para que pueda enviar paquetes al exterior y después de recibir el paquete pueda traducir esa IP pública de nuevo a una IP privada para que el paquete vaya de regreso a la computadora que lo envió, como se muestra en la figura 1.10. El mecanismo que utiliza NAT para las asociaciones entre IP pública e IP privada es una tabla (tabla de NAT) en la que guarda una entrada por cada conexión.

Cuando una computadora de la red local quiere enviar un paquete a Internet se lo envía al router o a la puerta de enlace y éste hace el SNAT (Source-NAT) que cambia la dirección de origen por la IP pública. Cuando llega una respuesta o un paquete perteneciente a esa conexión, llega primero al router y éste traduce la dirección IP de destino y la cambia por la dirección privada del host que corresponde para hacer la entrega del paquete a la red local.

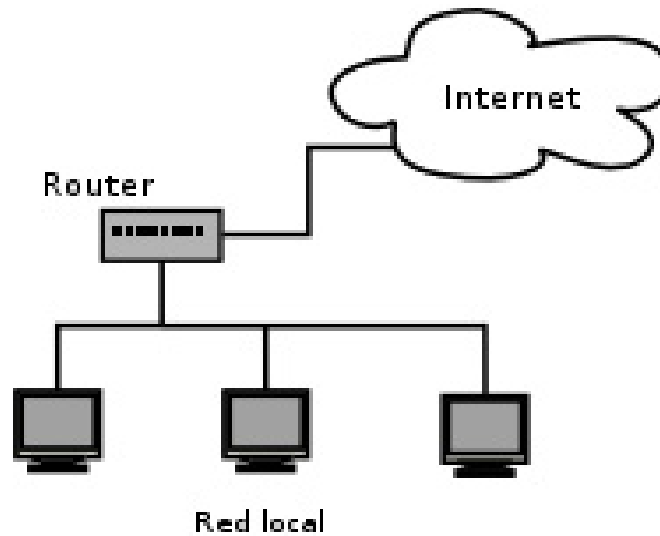


Figura 1.10 Funcionamiento de NAT

Las diferentes variantes del NAT comparten las siguientes características:

- ✓ Asignación transparente de direcciones.
- ✓ Encaminamiento transparente mediante la traducción de direcciones, donde el encaminamiento se refiere al reenvío de paquetes y no al intercambio de información de encaminamiento.
- ✓ Traducción de la carga útil de los paquetes de error ICMP (Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet).

Para que una red privada tenga acceso a Internet, el acceso debe ser por medio de un dispositivo ubicado en la frontera de las dos redes que tenga configurado NAT para la traducción de direcciones, en estos casos lo más conveniente es poner a un router para que los paquetes sean enviados hacia él. Existen dos tipos de asignación de direcciones:

- a) Asignación estática de direcciones: Existe un mapeo uno a uno de direcciones para las máquinas entre una dirección privada de red y una dirección externa de red durante el tiempo en funcionamiento del NAT. La asignación estática de direcciones asegura que NAT no tiene que administrar la gestión de direcciones con los flujos de sesión, tal como se muestra gráficamente en la figura 1.11.

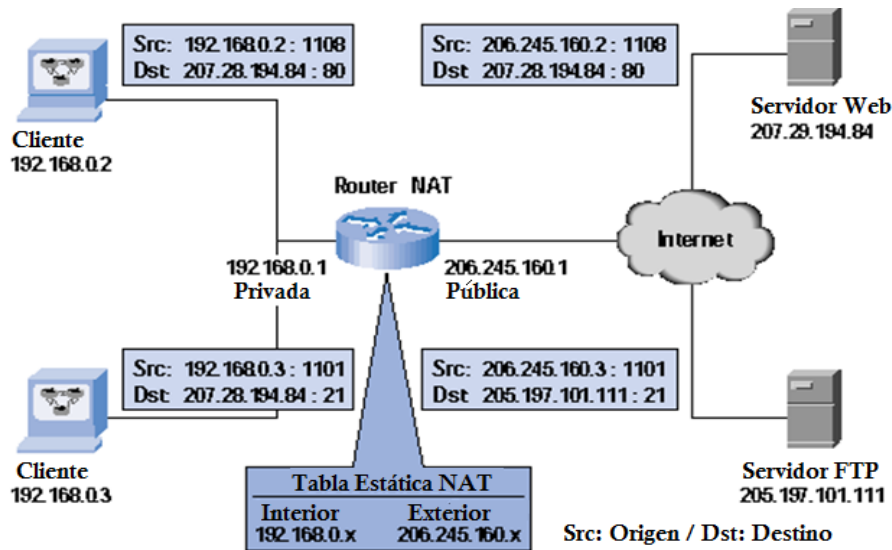


Figura 1.11 NAT estático: cuando el host 192.168.0.2 envía un paquete al servidor 207.28.194.84 tiene en la cabecera de sus paquetes los datos mostrados en A, al pasar estos paquetes por el router NAT, los datos son modificados y llegan al servidor con los datos mostrados en B. Las relaciones de direcciones de la tabla del router son puestas estáticamente.

- b) Asignación dinámica de direcciones: En este caso, las direcciones externas son asignadas a las máquinas de la red privada, o viceversa, de manera dinámica, basándose en los requisitos de uso y el flujo de sesión que el NAT determine heurísticamente. Cuando la última de las sesiones que use una dirección asociada termine, NAT liberará la asociación para que la dirección global pueda ser reciclada para su posterior uso. La naturaleza exacta de la asignación de direcciones es específica de cada implementación de NAT (figura 1.12).

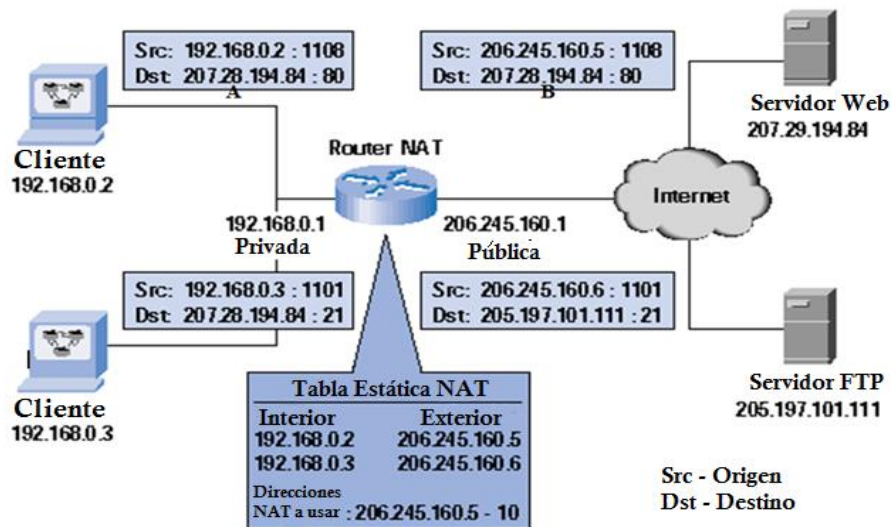


Figura 1.12 NAT dinámico: en este caso sucede lo mismo que en el anterior con las cabeceras de los paquetes que salen de A, en este caso la tabla muestra una lista con las direcciones válidas disponibles para ser usadas, estas direcciones son asignadas dinámicamente a los hosts.

Las principales versiones del NAT:

a) NAT tradicional

Las sesiones son unidireccionales y salientes de la red privada. Las sesiones en la dirección opuesta pueden ser permitidas en una base excepcional usando mapeos de dirección estáticos para hosts preseleccionados.

b) NAT Básico

Es una zona con un conjunto de direcciones de red privadas que pueden ser habilitadas para comunicarse con una red externa mapeando dinámicamente el conjunto de direcciones privadas a un conjunto de direcciones de red válidas globalmente donde cada dirección tiene garantizada una dirección global para ser mapeada a ella.

c) NAT con múltiples direcciones

Usa al NAPT (Network Address Port Translation - Traducción de Direcciones de Red por Puerto) con el cual un grupo de hosts en una red privada pueden tener salida a redes externas con una sola dirección global mediante la asociación de direcciones IP y puertos.

d) DNAT: Destination-NAT

Son conexiones del exterior a una computadora de red local donde se añade una entrada fija en la tabla del NAT en la que se indica que todo el tráfico proveniente de un determinado puerto sea dirigido a la computadora en cuestión. El puerto es el único elemento que hay para distinguir las diferentes conexiones; ya que, todo llega directo a la IP del router.

1.5.VIII ARP (ADDRESS RESOLUTION PROTOCOL, PROTOCOLO DE RESOLUCIÓN DE DIRECCIÓN)

Los equipos que se conectan a la red tienen un número de identificación de 48 bits, el cual es único y se establece en la fábrica en el momento de armar la tarjeta; en Internet no se utiliza directamente el número de identificación ya que los equipos utilizan una dirección IP.

Para que una dirección física se conecte con las direcciones lógicas se utiliza el protocolo ARP que asocia la dirección IP a la dirección MAC (Media Access Control, Control de

Acceso al Medio) que tiene cada computadora; el protocolo utiliza la memoria caché que es donde crea una tabla en la que almacena las asignaciones entre nivel de enlace de datos y las direcciones IP del nivel de red. El nivel de enlace de datos se encarga de gestionar las direcciones MAC y el nivel de red de las direcciones IP. ARP tiene la utilidad para supervisar y modificar la tabla de asignación de direcciones IP y direcciones MAC.

Si un equipo quiere comunicarse con otro consulta la tabla de búsqueda pero si la dirección que se requiere no se encuentra en la tabla el protocolo ARP envía una solicitud a la red indicándole a todos los equipos que necesita comparar la dirección lógica con la suya para poder identificarla, así el ARP almacenará el par de direcciones en la tabla de búsqueda y podrá establecerse la comunicación. ARP se emplea en redes IEEE 802 aunque también se usó en las redes DIX Ethernet para mapear direcciones IP a dirección hardware.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

1. Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
2. Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
3. Cuando un router necesita enviar un paquete a un host a través de otro router.
4. Cuando un router necesita enviar un paquete a un host de la misma red.

Protocolo RARP

RARP (Reverse Address Resolution Protocol, Protocolo de Resolución de Direcciones Inverso) se usa esencialmente para las estaciones de trabajo que no tienen discos duros y desean conocer su IP; funciona desde la tabla de búsqueda entre las direcciones MAC y las direcciones IP alojadas en el router que está en la red de área local (LAN).

El protocolo tiene muchas limitaciones:

- ✓ Necesita mucho tiempo de administración para mantener las tablas importantes en los servidores.
- ✓ Necesita muchas personas para el mantenimiento de las tablas de búsqueda y de capacidad por parte del hardware que aloja al servidor del protocolo RARP.
- ✓ Permite que varios servidores respondan a solicitudes, pero no tiene mecanismos que garanticen la respuesta en forma idéntica.
- ✓ Un servidor solo puede servir para una LAN.

I.5.IX IP (INTERNET PROTOCOL, PROTOCOLO DE INTERNET)

Es la base fundamental de Internet. Es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable (no garantiza la recepción del paquete) y de mejor entrega posible sin garantías. Esto significa que los paquetes de información, que serán emitidos a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino.

El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Las principales características de este protocolo son:

- ✓ Direccionamiento mediante direcciones lógicas IP de 32 bits.
- ✓ Si un paquete no es recibido, éste permanecerá en la red durante un tiempo finito.
- ✓ Realiza el *mejor esfuerzo* para la distribución de paquetes.
- ✓ Tamaño máximo del paquete de 65635 bytes.
- ✓ Solo se realiza verificación por suma al encabezado del paquete, no a los datos que éste que contiene.

La unidad de información intercambiada por IP es denominada datagrama. Tomando como analogía los marcos intercambiados por una red física los datagramas contienen un encabezado y un área de datos. IP no especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte.

Para que en una red de dos computadoras puedan comunicarse entre sí, deben estar identificadas con precisión. Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) dependiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bites. La dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.

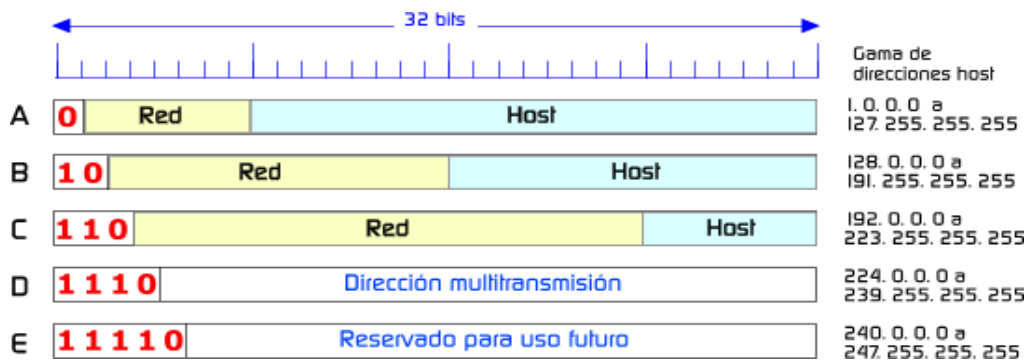


Figura 1.13 Clases de direcciones IP

Tomando en cuenta como está definida una dirección IP, podría surgir la duda de cómo identificar qué parte de la dirección identifica a la red y qué parte al nodo en dicha red. Lo anterior se resuelve mediante la definición de las *Clases de direcciones IP*; lo cual, se observa que una red con dirección clase A queda precisamente definida con el primer octeto de la dirección, la clase B con los dos primeros y la C con los tres primeros octetos. Los octetos restantes definen los nodos en la red específica. Se puede observar en la figura 1.13.

Existen dos maneras de obtener una dirección IP por medio del proveedor de acceso a Internet (ISP), el cual puede asignar siempre la misma dirección IP (IP fija) o dar una diferente (IP dinámica) cada vez que se quiera conectarse:

1. Dirección IP fija

Es una IP asignada por el usuario o bien dada por el proveedor ISP en la primera conexión.

Permite al usuario montar servidores web, correo, FTP, entre otros y dirigir un dominio a esta IP sin tener que mantener actualizado el servidor DNS cada vez que cambie la IP como ocurre con las IP dinámicas.

Ventajas:

- ✓ Es más fácil identificar al usuario que está utilizando esa IP.
- ✓ Permite tener servicios dirigidos directamente a la IP.
- ✓ Nunca cambia.

Desventajas:

- ✓ Son más vulnerables al ataque puesto que el usuario no puede conseguir otra IP.
- ✓ Es más caro para los ISP puesto que esa IP puede no estar usándose las 24h. del día.

2. Dirección IP dinámica

Es una IP asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica de Host) al usuario. La IP tiene una duración determinada ya que cambia cada vez que el usuario se reconecta por cualquier causa. Estas IP dinámicas son ofrecidas por la mayoría de los operadores sin gasto adicional.

Ventajas:

- ✓ Es más difícil identificar al usuario que está utilizando esa IP.
- ✓ Reduce los costos de operación a los proveedores de servicios internet.
- ✓ Para los ISP los equipos son más simples

Desventajas:

- ✓ Obliga a depender de servicios que redirigen un host a una IP.
- ✓ Es ilocalizable porque en unas horas pueden haber varios cambios de IP.

1.5.X TCP (TRANSMISSION CONTROL PROTOCOL, PROTOCOLO DE CONTROL DE TRANSMISIÓN)

Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación permite la administración de datos que vienen del nivel más bajo del modelo o van hacia él (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) solo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que se dice que se está en un entorno Cliente-Servidor (figura 1.14).

Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

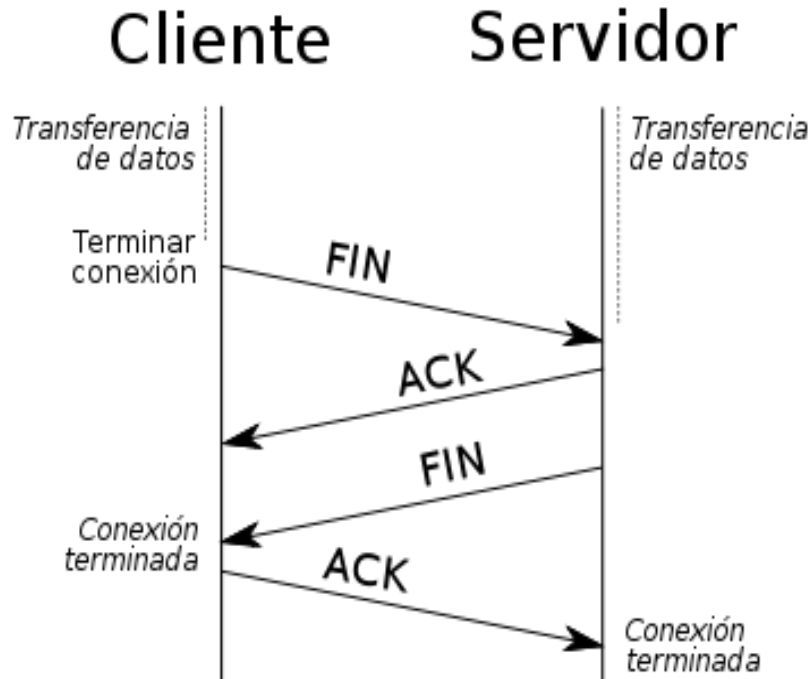


Figura 1.14 Cierre de una conexión según el estándar

Las principales características del protocolo TCP son las siguientes:

- ✓ Orientado a conexión
- ✓ Permitir una transferencia confiable y transparente de datos entre los puntos terminales de la red
- ✓ Monitorea el flujo de los datos para evitar la saturación de la red
- ✓ Reensambla los mensajes en la estación destino y a partir de segmentos entrantes.
- ✓ Vuelve a enviar lo que no se ha recibido
- ✓ Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP
- ✓ Proporciona a los datos que se formen en segmentos de longitud variada para entregarlos al protocolo IP
- ✓ Admite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente
- ✓ Acepta comenzar y finalizar la comunicación amablemente.

Los puertos TCP utilizan un puerto de programa específico para la entrega de datos enviados mediante el TCP. Los puertos TCP son más complejos y funcionan de manera distinta que los puertos UDP.

Mientras que un puerto UDP funciona como una única cola de mensajes y el extremo de red para la comunicación basada en UDP, el extremo final para toda la comunicación TCP es una conexión única. Cada conexión TCP se identifica de forma exclusiva mediante extremos dobles.

Cada puerto de servidor TCP puede ofrecer acceso compartido a varias conexiones, ya que todas las conexiones TCP se identifican de forma exclusiva mediante dos parejas de direcciones IP y puertos TCP (una pareja de dirección y puerto para cada host conectado).

Los programas TCP utilizan números de puerto reservados o conocidos. El lado del servidor de cada programa que utiliza puertos TCP atiende los mensajes que llegan a su número de puerto conocido. Todos los números de puerto de servidor TCP inferiores a 1,024 (y algunos números superiores) están reservados y registrados por la Autoridad de números asignados de Internet (IANA - Internet Assigned Numbers Authority). Identifica las aplicaciones emisoras y receptoras; dependiendo de la conexión TCP tiene asociado un número de puerto (de 16 bits, y existen 65536 puertos posibles), los más comunes son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80).

1.5.XI UDP (USER DATAGRAM PROTOCOL, PROTOCOLO DE DATAGRAMA DE USUARIO)

Es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión. Además, es muy simple ya que no proporciona detección de errores.

UDP tiene los siguientes propósitos:

1. Envío de mensajes sin espera de ack de confirmación. Los mensajes pueden ser perdidos, duplicados o llegar en desorden.
2. Sin control de flujo, los mensajes pueden llegar más rápido de lo que pueden ser procesados.
3. Este protocolo utiliza el mismo esquema de numeración de puertos que usa TCP para los protocolos de capas superiores.

Sus características son:

- ✓ Poco confiable.
- ✓ No utiliza acuses de recibo.
- ✓ Transmite mensajes (llamados datagramas del usuario).
- ✓ No ofrece verificación de software para la entrega de segmentos (poco confiable).
- ✓ No reensambla los mensajes entrantes.

Se utiliza cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

El puerto UDP es una dirección de 16 bits que existe solo para el propósito de pasar determinados tipos de información de datagrama a la ubicación correcta por encima de la capa de transporte de la pila del protocolo.

UDP utiliza puertos para permitir la comunicación entre aplicaciones. Estos puertos no son los mismos como los puertos TCP, aunque TCP y UDP pueden utilizar el mismo número de puerto en determinados casos. Los puertos UDP pueden recibir más de un mensaje a la vez y se identifican mediante números de puerto bien conocidos.

1.6 MEDIOS DE TRANSMISIÓN

1.6.1 TERRESTRES¹

a) Cable coaxial (coaxial cable)

El cable coaxial está formado por un alambre de cobre rígido como núcleo que transporta señales electrónicas para formar datos; este núcleo puede ser sólido (normalmente de cobre) o de hilos. Está rodeado por un material aislante dieléctrico que lo separa de la malla. El aislante está forrado con un conductor cilíndrico que con frecuencia es una malla de tejido fuertemente trenzado para proteger los datos transmitidos absorbiendo las señales electrónicas llamadas ruido, de forma que no pasan por el cable y no distorsionan los datos. El conductor externo se cubre de una envoltura protectora plástica no conductora que normalmente está hecha de goma, teflón o plástico que rodea todo el cable y cubre la malla de hilos de metal, mostrado en la figura 1.15.

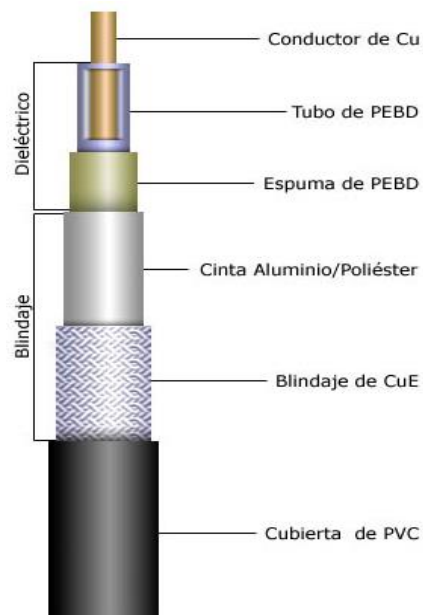


Figura 1.15 Partes del cable coaxial

El cable coaxial puede abarcar tramos grandes sin necesidad de repetidores a velocidades mayores. Existen dos tipos de cable coaxial (figura 1.16).

¹ Para mayor información véase el apéndice A

- ✓ Cable de 50 ohms (RG-58/U) para comunicación BaseBand (transmisión digital). Generalmente para redes LAN, existen dos tipos de cables: *coaxial grueso (thick)* y *coaxial fino (thin)*.
- ✓ Cable de 75 ohms (RG-59/U) para comunicación BroadBand (transmisión analógica), utilizado comúnmente en sistemas de televisión por cable.

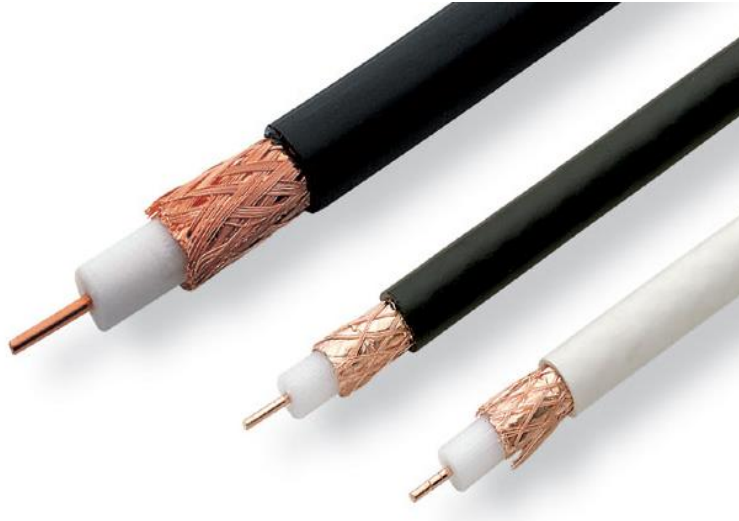


Figura 1.16 Tipos de cables coaxial. Tenemos de izquierda a derecha al cable coaxial BaseBand dividido en grueso y fino; finalizando con el cable coaxial BroadBand

El cable coaxial, sea cual sea el tipo, no puede ser utilizado para redes Token Ring, FDDI (Fiber Distributed Data Interface, Interfaz de Datos Distribuida por Fibra), teléfono o ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados). El cable coaxial puede ser utilizado para redes Ethernet.

b) Par trenzado (twister-pair cabling)

Consiste en dos alambres de cobre aislados de 1mm de grosor trenzados en forma helicoidal para reducir la interferencia eléctrica de pares similares cercanos; con la característica de que dos alambres paralelos funcionan como antena. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipar de pares trenzados en 2, 4, 8 o hasta 300 pares. Debajo de la aislación de PVC existe otra capa de aislación también de polietileno, la contiene una sustancia antioxidante para evitar la corrosión del cable. Generalmente el par trenzado es utilizado en la línea telefónica.

Este tipo de cable no se maneja por unidades ya que siempre es por pares o grupos de pares que se conoce como cable multipar; el cual siempre está trenzado entre sí para mejorar la resistencia de todo el grupo en diferentes niveles de interferencia electromagnética externa. Con el tiempo se definen colores que permitan visualizar el inicio y el final de cada grupo de cables, como se aprecia en la figura 1.17. Los colores del aislante están normalizados a fin de tener una mejor manipulación al instalar grandes cantidades. En las redes locales los colores son:

- ✓ Naranja/Blanco – Naranja
- ✓ Verde/Blanco – Verde
- ✓ Blanco/Azul – Azul
- ✓ Blanco/Marrón - Marrón



Figura 1.17 Colores del par trenzado

Existen tres tipos de par trenzado los cuales son divididos de acuerdo a sus características físicas, teniendo así, diferentes características de alcance.

1. UTP (Unshielded Twister Pair - Par Trenzado Sin Blindaje)

Únicamente depende de trenzar los cables sin necesidad de un recubrimiento externo a ellos.

2. STP (Shielded Twister Pair - Par Trenzado Blindado)

Cable de par trenzado de 150 ohm en donde existe un recubrimiento de aluminio alrededor, de tal manera que impide interferencias eléctricas sobre los cables logrando así una inmunidad hacia el ruido

3. FTP (Foiled Twisted Pair, Par trenzado con pantalla global)

Es como el cable UTP pero sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas.

c) Fibra óptica (optical fiber)

Consiste en un medio de vidrio (filamento) con grosor aproximado de 0.1 mm, forrado por un aislante plástico; en el cual, la información viaja en forma de luz. La ventaja que tiene es su alta inmunidad al ruido, baja pérdida de información y la confiabilidad de la misma a velocidades luz.

La fibra óptica está formada por los siguientes componentes:

- ✓ La fuente de luz: LED o láser.
- ✓ Medio transmisor: fibra óptica.
- ✓ Detector de luz: fotodiodo.

Un pulso de luz indica un bit 1 y la ausencia de luz indica un bit 0. El medio transmisor es una fibra de vidrio muy delgada en la cual se genera un pulso eléctrico cuando la luz incide en él.

Los tipos básicos de fibra óptica son:

- ✓ Multimodo
- ✓ Multimodo con índice graduado
- ✓ Multimodo con índice escalonado
- ✓ Monomodo

1.6.II AERÉOS

Los medios inalámbricos transportan señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos.

Como medio de red, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre.

Las especificaciones de la capa física se aplican a áreas que incluyen datos para la codificación de señales de radio, frecuencia y poder de transmisión, recepción de señales y requisitos de codificación y diseño y construcción de la antena.

Según el rango de frecuencias utilizado para transmitir, el medio de transmisión puede ser las ondas de radio, las microondas terrestres o por satélite, y los infrarrojos.

Dependiendo del medio, la red inalámbrica tendrá unas características u otras:

- a) Ondas de radio: Las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de los 300 a los 3000 MHz en el espectro radioeléctrico.
- b) Microondas terrestres: Se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.
- c) Microondas por satélite: Se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal (denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas.
- d) Infrarrojos: Enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

1.7 REDES INALÁMBRICAS (WIRELESS NETWORK)

Los estándares de IEEE y de la industria de las telecomunicaciones sobre las comunicaciones inalámbricas de datos abarcan las capas física y de enlace de datos.

Los cuatros estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son:

- a) IEEE estándar 802.11: Comúnmente denominada Wi-Fi, se trata de una tecnología LAN (Red de área local inalámbrica, WLAN) que utiliza una contención o sistema no determinista con un proceso de acceso a los medios de acceso múltiple con detección de portadora/prevención de colisiones (CSMA/CA).
- b) IEEE estándar 802.15: Red de área personal inalámbrica (WPAN) estándar, comúnmente denominada *Bluetooth*, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de una distancia de 1 a 100 metros.
- c) IEEE estándar 802.16: Conocida como WiMAX (Interoperabilidad mundial para el acceso por microondas), utiliza una topología punto a multipunto para proporcionar un acceso de ancho de banda inalámbrico.
- d) Sistema global para comunicaciones móviles (GSM): Incluye las especificaciones de la capa física que habilitan la implementación del protocolo Servicio general de radio por paquetes (GPRS) de capa 2 para proporcionar la transferencia de datos a través de redes de telefonía celular móvil.
- e) Otros tipos de tecnologías inalámbricas como las comunicaciones satelitales, ofrecen una conectividad de red de datos para ubicaciones sin contar con otros medios de conexión. Los protocolos, incluso GPRS, permiten la transferencia de datos entre estaciones terrestres y enlaces satelitales.

En la figura 1.18 se detalla el posicionamiento de los estándares para Wireless.

Posicionamiento de Estándares Wireless

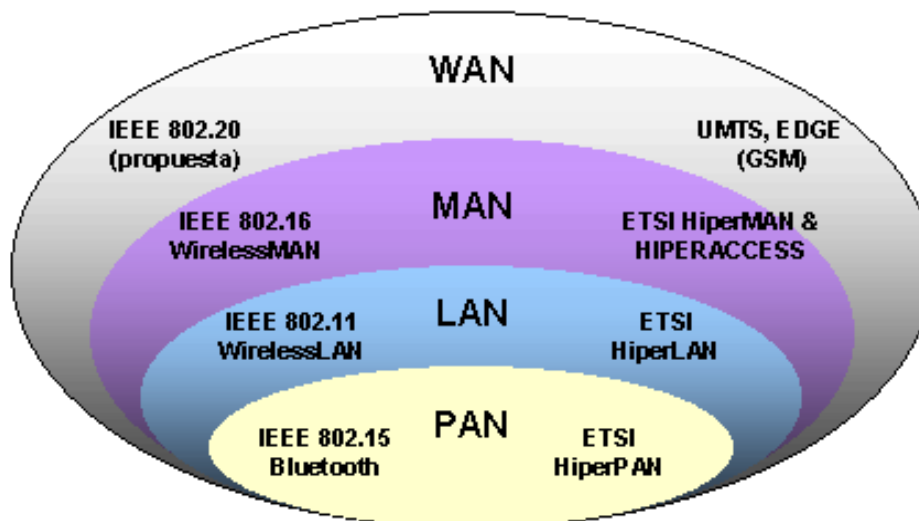


Figura 1.18 Posicionamiento de estándares Wireless

1.7.1 LAN INALÁMBRICA

Una WLAN (Wireless Local Area Network, *red de área local inalámbrica*) es una red que cubre un área equivalente a la red local de una organización, con un alcance aproximado de cien metros. Permite que las terminales que se encuentran dentro del área de cobertura puedan conectarse entre sí. Utiliza tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

Una LAN inalámbrica requiere los siguientes dispositivos de red:

- a) Punto de acceso inalámbrico (AP): Concentra las señales inalámbricas de los usuarios y se conecta, generalmente a través de un cable de cobre, a la infraestructura de red existente basada en cobre, como Ethernet (véase figura 1.19).
- b) Adaptadores NIC inalámbricos: Proporcionan capacidad de comunicación inalámbrica a cada host de la red (véase figura 1.19).



Figura 1.19 Adaptadores y puntos de acceso de una WLAN

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (capa física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. Es el primer estándar que permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad.

Los estándares incluyen:

- a) **IEEE 802.11a**: Opera en una banda de frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbps. Posee un área de cobertura menor y es menos efectivo al penetrar estructuras edilicias ya que opera en frecuencias superiores. Los dispositivos que operan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g.
- b) **IEEE 802.11b**: Opera en una banda de frecuencia de 2.4 GHz y ofrece velocidades de hasta 11 Mbps. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11a.

- c) IEEE 802.11g: Opera en una frecuencia de banda de 2.4 GHz y ofrece velocidades de hasta 54 Mbps. Por lo tanto, los dispositivos que implementan este estándar operan en la misma radiofrecuencia y tienen un alcance de hasta 802.11b pero con un ancho de banda de 802.11a.
- d) IEEE 802.11n: El estándar IEEE 802.11n se encuentra actualmente en desarrollo. El estándar propuesto define la frecuencia de 2.4 GHz o 5 GHz. La velocidad típica de transmisión de datos que se espera es de 100 Mbps a 210 Mbps con un alcance de distancia de hasta 70 metros.

1.7.II INTERFAZ DE RED INALÁMBRICA

Hace referencia a la capa de enlace de datos del modelo OSI que proporciona un medio para intercambiar datos a través de medios locales y realiza dos servicios básicos:

1. Permite a las capas superiores acceder a los medios usando técnicas, como tramas.
2. Controla cómo los datos se ubican en los medios y son recibidos usando técnicas como control de acceso a los medios y detección de errores.

Para sostener una gran variedad de funciones de red, la capa de enlace de datos se divide en dos subcapas: una superior y otra inferior.

- a) Subcapa superior: define los procesos de software que proveen servicios a los protocolos de capa de red.
- b) Subcapa inferior: define los procesos de acceso a los medios realizados por el hardware.

Al separar la capa de enlace de datos en subcapas permite a un tipo de trama definida por la capa superior acceder a diferentes tipos de medios definidos por la capa inferior. Tal es el caso en muchas tecnologías LAN, incluidas Ethernet. Las dos subcapas comunes de LAN son:

1) Control de enlace lógico llc (logical link control)

LLC es la superior de la capa 2 del modelo OSI que se encarga de la lógica de la comunicación como es el control de flujo, control de errores, entramado, direccionamiento de la subcapa MAC y el SAP (Source Access Point, punto de acceso a la fuente) que es el identificador que determina el protocolo usado en la capa 3 del modelo OSI.

En la figura 1.20, se muestran las subcapas que tiene la capa de enlace de datos del modelo OSI.

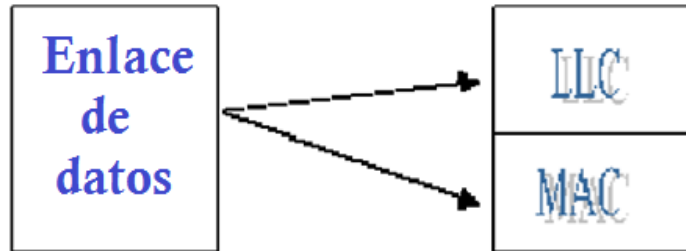


Figura 1.20 Subcapas de la capa 2 del modelo OSI

Es responsable del control de enlace lógico. El protocolo LLC más generalizado es IEEE 802.3, que incluye variantes como no orientado a conexión y orientadas a conexión.

Los servicios que ofrece en la capa de red, son los siguientes:

a) Servicio en modo conexión (cons, connection oriented network service).

- ✓ Es un servicio que establece una conexión entre las estaciones del enlace.
- ✓ Garantiza la entrega de las unidades de datos que fluyen a través de dicha conexión (servicio confiable).
- ✓ El servicio de conexión le garantiza al receptor la entrega en secuencia de las unidades de datos y la protección contra pérdidas y duplicados.
- ✓ Con ese fin dispone de los mecanismos necesarios para controlar el flujo y corregir los errores.

b) Servicio no orientado a conexión (clns, connection less network service)

- ✓ No establece una conexión previa entre las estaciones, por lo que cada trama intercambiada es independiente de todas las demás.
- ✓ Cada trama es individualmente autónoma y autosuficiente ante el receptor.
- ✓ Es un servicio que tiene utilidad cuando el establecimiento de una conexión implica retrasos que son inaceptables para el funcionamiento del sistema (control distribuido).
- ✓ El servicio de enlace sin conexión puede ser con o sin confirmación.

En la subcapa LLC se contemplan dos aspectos bien diferenciados:

- 1) Protocolos: Para la comunicación entre entidades de la propia subcapa LLC, definen los procedimientos para el intercambio de tramas de información y de control entre cualquier par de puntos de acceso al servicio del nivel de enlace LSAP (Link Source Access Point, Enlace del punto de acceso a la fuente).
- 2) Interfaces: con la subcapa inferior MAC y con la capa superior (de Red).
 - a) Interfaz LLC – MAC: Especifica los servicios que la subcapa de LLC requiere de la subcapa MAC, independientemente de la topología de la subred y del tipo de acceso al medio.
 - b) Interfaz LLC – Capa de red modelo OSI: Especifica los servicios que la capa de red del modelo OSI obtiene de la capa de enlace del mismo modelo, independientemente de su configuración.

2) Mac (medium access control, control de acceso al medio)

No está definida en ningún estándar IEEE 802 ya que depende más que nada de la tecnología o protocolo usado (por ejemplo, Ethernet usa el método CSMA/CD, Token Ring el método Token Passing, las redes inalámbricas el método CSMA/CA, etcétera).

El MAC es el mecanismo encargado del control de acceso de cada estación al medio; donde puede realizarlo de forma distribuida cuando todas las estaciones cooperan para determinar cuál es y cuándo debe acceder a la red. También se puede realizar de forma centralizada utilizando un controlador.

El esquema centralizado tiene las siguientes ventajas:

1. Puede proporcionar prioridades, rechazos y capacidad garantizada.
2. La lógica de acceso es sencilla.
3. Resuelve conflictos entre estaciones de igual prioridad.

Los principales inconvenientes son:

1. Si el nodo central falla, falla toda la red.
2. El nodo central puede ser un cuello de botella.

Las técnicas de control de acceso al medio pueden ser síncronas o asíncronas:

- a) Síncronas: hacen que la red se comporte como de conmutación de circuitos, lo cual no es recomendable para LAN y WAN.
- b) Asíncronas: son más aceptables ya que las LAN actúan de forma impredecible y por tanto no es conveniente el mantenimiento de accesos fijos.

De esta forma, la subcapa MAC define una dirección física para cada nodo, que generalmente se le conoce como *dirección MAC*.

La dirección MAC es un identificador único en el mundo representado en notación hexadecimal para cada dispositivo y conformado por 48 bits; 24 bits que definen el proveedor de dicha tarjeta y 24 bits que el proveedor coloca a esa tarjeta. Se conoce también como dirección física o hardware.

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet, usándose ésta solo a niveles internos de la red. Sin embargo, es posible añadir un control de hardware en un conmutador o un punto de acceso inalámbrico, para permitir solo a unas MAC concretas el acceso a la red. En este caso, deberá saberse la MAC de los dispositivos para añadirlos a la lista. Dicho medio de seguridad se puede considerar un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

- Ethernet
- 802.3 CSMA/CD
- 802.5 o redes en anillo a 4 Mbps o 16 Mbps
- 802.11 redes inalámbricas (Wi-Fi).
- Asynchronous Transfer Mode.

CAPÍTULO 2

COMPONENTES Y MONITOREO DE RED



Una red es un conjunto de conexiones físicas y programas informáticos empleados para conectar dos o más computadoras. Los usuarios de una red pueden compartir archivos, impresoras y otros recursos, así como enviar mensajes electrónicos y ejecutar programas en otras computadoras.

Una red tiene tres niveles de componentes principales:

1. Software de aplicaciones: Programas informáticos que se comunican con los usuarios de la red y permiten compartir información (archivos de bases de datos, documentos, gráficos o vídeos) y recursos (impresoras o unidades de disco). Un tipo de software de aplicación es el de cliente-servidor al cual la computadora cliente envía peticiones de información o de uso de recursos a otras computadoras o a servidores que controlan el flujo de datos y la ejecución de las aplicaciones a través de la red. Otro tipo de software de aplicación es el de igual a igual (peer to peer) en el cual las computadoras envían mensajes entre sí y peticiones directamente sin utilizar un servidor como intermediario
2. Software de red: Son programas informáticos que establecen protocolos o normas para que las computadoras se comuniquen entre sí. Estos protocolos envían y reciben grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigen el movimiento de paquetes a través de la red física y minimizan las posibilidades de colisión entre paquetes enviados simultáneamente.
3. Hardware de red: Componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de éstas (cable UTP o fibra óptica) y el adaptador de red el cual permite acceder al medio material que las conecta, recibir paquetes desde el software de red, transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios que pueden ser procesados por los circuitos electrónicos de ellas.

2.1 COMPONENTES DE UNA RED

Los componentes de una red tienen funciones específicas y se utilizan dependiendo de las características físicas (hardware) que tienen.

Para elegirlos se requieren considerar las necesidades y los recursos económicos de quien se desea conectar a la red, por eso deben conocerse las características técnicas de cada componente de red.

A continuación se mencionan los principales componentes que integran un modelo básico de red.

2.1.1 ROUTER

La palabra router es un término en inglés que puede traducirse como enrutador, ruteador o direccionador lo que se puede interpretar como simplemente guía. El router permite la interconexión de redes LAN y su función es la de guiar los paquetes de datos para que fluyan hacia la red correcta e ir determinando qué caminos debe seguir para llegar a su destino, básicamente para los servicios de Internet, los cuales recibe de otro dispositivo como un módem del proveedor de Internet de banda ancha.

El router que se utiliza dentro de los hogares se conoce como SOHO (Small Office/Home Office, Oficinas pequeñas/Oficinas de casa). Este dispositivo permite que varias computadoras se conecten a un servicio de banda ancha a través de una red privada virtual segura. Técnicamente, el router residencial se encarga de traducir las direcciones de red en lugar de concretar el enrutamiento (no conecta a todas las computadoras locales a la red de forma directa, sino que hace que funcionen como un solo equipo).

Dentro de las empresas puede encontrarse el router de acceso (incluyendo el SOHO), el router de distribución (suman tráfico a partir de otros enrutadores o de la obtención de los flujos de datos) y el router de núcleo o core router (que administra diversos niveles del router).

Existe, por otra parte, el router inalámbrico, que funciona como una interfaz entre las redes fijas y las redes móviles (como WiFi, WiMAX y otras). El router inalámbrico comparte los mismos principios que el router tradicional, aunque admite la conexión sin cables a la red en cuestión (véase la figura 2.1).



Figura 2.1 Router inalámbrico

Características generales

- a) Permiten la conexión a la LAN desde otras redes, así como de las computadoras que así lo soliciten, principalmente para proveer servicios de Internet.
- b) Se puede interconectar con redes WLAN, por medio de dispositivos inalámbricos como Access Point o Routers Wi-Fi (Wireless Fidelity, Fidelidad inalámbrica).
- c) Permiten la conexión ADSL (Asymmetric Digital Subscriber Line, Línea de Suscripción Digital Asimétrica), la cual permite el manejo de Internet de banda ancha y distribuirlo hacia otras computadoras por medio de cables UTP.

Funcionamiento

En la figura 2.2 se muestra el funcionamiento de un router al interconectar redes LAN y proveer servicios de Internet a las mismas:

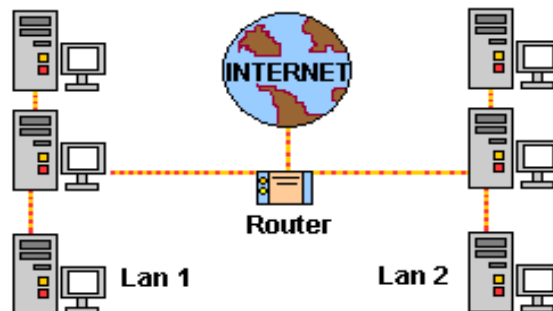


Figura 2.2 Funcionamiento de un router

1. El router puede estar conectado a la red telefónica y recibir servicio de Internet.
2. El router interconecta redes cableadas (LAN) y permite proveer servicios a los equipos que hagan la petición.
3. También permite determinar caminos alternos para que los datos fluyan de manera más eficiente.

El router tiene que ser capaz de:

- Construir tablas de enrutamiento.
- Ejecutar comandos.
- Enrutar paquetes por las interfaces de red mediante el uso de protocolos de enrutamiento, por lo que integran un microprocesador.

Tecnología ADSL y el router

La tecnología ADSL tiene la capacidad de utilizar la línea telefónica convencional y subdividir en frecuencias, esto para incorporar varios servicios a la vez (telefonía, internet y televisión de paga). En el caso de la telefonía solo hace falta muy poco ancho de banda para las conversaciones, mientras que para el envío de datos se incorpora una banda media y para recibir datos se utiliza un ancho muy alto, de allí el nombre de Asymmetric, como puede observarse en la figura 2.3. Con estas características anteriores es posible que se tenga Internet de alta velocidad, ya que el recibir los datos es mucho más veloz que el envío de los mismos.



Figura 2.3 División de frecuencias en telefonía e Internet

Las velocidades promedio de descarga de datos o *Downstream* es de 24 Mbps mientras que el envío de datos *Upstream* es de solamente 1 Mbps, esto marca una diferencia de velocidad superior al recibir que al enviar, por ello es tan veloz la conexión a Internet.

Estándares

Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para enviar el paquete hacia su destino.

- Cada red a la que se conecta un router requiere una interfaz separada.

- b) La principal responsabilidad de un router es dirigir los paquetes:
- Determinar la mejor ruta para enviar paquetes
 - Enviar paquetes hacia su destino
- c) El router usa su tabla de enrutamiento para determinar la mejor ruta para reenviar el paquete.

El router determina la mejor ruta.

Proceso

- 1) El router recibe un paquete.
- 2) Examina su dirección IP de destino.
- 3) Busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del router.
- 4) La tabla de enrutamiento también incluye la interfaz que se utilizará para enviar el paquete.
- 5) Cuando se encuentra una coincidencia, el router encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida.
- 6) El paquete se envía hacia su destino.

El router se encuentra diseñado para funcionar con ciertos estándares o protocolos (reglas de comunicación establecidas) para redes (véase tabla 2.1):

Tabla 2.1 Estándares definidos para el router

Estándar	Norma	Velocidad (Megabits por segundo)	Método de acceso a la red
Fast Ethernet	IEEE 802.3u	10 / 100 / 1000 Mbps	Acceso múltiple con detección de portadora y detección de colisiones, actualmente es el más utilizado.
Ethernet	IEEE 802.3	10 Mbps	Acceso múltiple con detección de portadora y detección de colisiones.

Usos específicos

Se utilizan cuando se necesita un alto grado de precisión en la ruta que debe llevar la información, así como para interconectar redes y compartir Internet de banda ancha mientras cuenta con la función para ello.

2.1.II HUB (CONCENTRADOR)

Es un dispositivo activo que actúa como elemento central y como un repetidor mediante dos enlaces: transmisión y recepción; ya que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

También puede tener la función de un servidor debido a su capacidad para gestionar los recursos compartidos de la red hacia los clientes, son la base de la creación de redes tipo estrella. Como alternativa existen los sistemas en los que las computadoras están conectados en serie a una línea que une varias o a todas entre sí, antes de llegar a la computadora central.

Existen 3 clases de hubs:

- 1) Pasivo: No necesita energía eléctrica y solo interconecta dispositivos.
- 2) Activo: Necesita alimentación y regenera la señal recibida, como si fuera un repetidor, de ahí la denominación de repetidor multipuerto.
- 3) Inteligente: También llamados smart hubs, son hubs activos que incluyen microprocesador. Permite a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporciona una estructura de crecimiento ordenado de la red.

El hub extiende la funcionalidad de la red para que el cableado pueda ser extendido a mayor distancia, por eso su nombre de repetidor. El problema es que el hub transmite los broadcasts a todos los puertos que contenga. Si tiene 8 puertos todos los nodos que estén conectados recibirán la misma información, siendo innecesario y excesivo.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

En la figura 2.4 se observa un hub conectado a múltiples dispositivos.



Figura 2.4 Esquema del funcionamiento de un hub

Características generales

- a) Permiten concentrar todas las estaciones de trabajo (equipos clientes).
- b) También pueden gestionar los recursos compartidos hacia los equipos clientes.
- c) Cuentan con varios puertos RJ45 integrados, desde 4, 8, 16 y hasta 32.
- d) Son necesarios para crear las redes tipo estrella (todas las conexiones de las computadoras se concentran en un solo dispositivo).
- e) Permiten la repetición de la señal y son compatibles con la mayoría de los sistemas operativos de red.
- f) Tiene una función en la cual pueden ser interconectados entre sí, pudiéndose conectar a otros hubs y permitir la salida de datos (conexión en cascada), por medio del último puerto RJ45.

Estándares del hub

El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

Los hubs se encuentran diseñados para funcionar con ciertos estándares (véase tabla 2.2) o protocolos (reglas de comunicación establecidas):

Tabla 2.2 Estándares del hub

Nombre	Estándar	Velocidad (Megabits por segundo)	Características
Ethernet	IEEE 802.3 (10BASET)	10 / 100 Mbps	Se utilizan en todo tipo de redes basadas en cable en escuelas, hospitales, hogares, etc.
Ethernet	IEEE 802.3u (10BASETX)	100 Mbps	Alta velocidad, soporta cableado de hasta 100 m, para cable UTP, soporta Half Duplex (envía o recibe datos, una acción a la vez)

Ventajas

Un concentrador es un dispositivo simple, esto influye en dos características:

- 1) El precio es barato.
- 2) Un concentrador casi no añade ningún retardo a los mensajes.

Desventajas

- a) El concentrador envía información a ordenadores que no están interesados. A este nivel solo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todas las computadoras que están conectadas a él, así seguro que acierta.
- b) Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando una computadora quiere enviar información y emite de forma simultánea con otra que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añaden computadoras a la red también aumentan las probabilidades de colisión.
- c) Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si se observa cómo funciona el concentrador no tiene capacidad de almacenar nada. Por lo tanto si una computadora que emite a 100 megabits/segundo le trasmitiese a otro de 10 megabits/segundo algo se perdería del mensaje. En el caso del ADSL el router suele funcionar a 10 megabits/segundo, si se conecta a la red casera, toda la red funcionará a 10 megabits/segundo, aunque las tarjetas sean 10/100 megabits/segundo.

Actualmente compiten en el mercado contra dispositivos switch y contra dispositivos router pero han dejado de utilizarse por la gran cantidad de colisiones y tráfico de red que producen.

2.1.III SWITCH

Opera en el nivel de enlace de datos del modelo OSI y tiene como función la interconexión de dos o más segmentos de red, de tal manera que se puede hacer un puente (bridge) entre los dispositivos.

El switch transmite los datos de un segmento a otro basándose en la dirección MAC del destino que tienen las tramas en la red. Esta tarea permite conectar distintas redes y fusionarlas entre sí. Una de las principales ventajas que posee el switch es que actúa como un filtro y mejora el rendimiento de las redes locales. Además, tiene la ventaja de almacenar la dirección MAC de todos los dispositivos a los que puede llegar desde cada uno de sus puertos, así la información viaja directa desde el puerto origen hasta el puerto destino (figura 2.5).

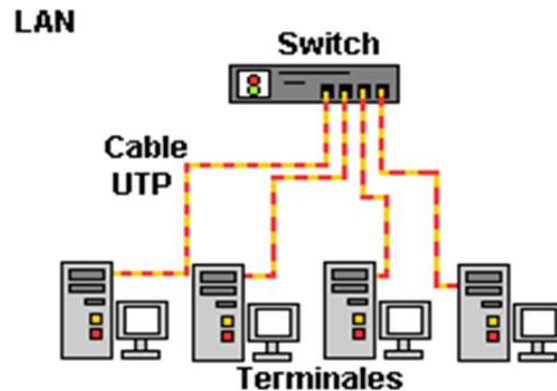


Figura 2.5 Funcionamiento de un switch

Al conectarse dos switches cada uno almacena la dirección MAC de todos los dispositivos que están conectados a sus puertos; siendo el puerto de interconexión donde se alojarán las direcciones MAC de los dispositivos del otro switch.

Características generales del switch

- a) Permite la conexión de distintas redes de área local (LAN).
- b) Se encarga solamente de determinar el destino de los datos *Cut-Through*.

- c) Tienen la función de bridge integrado, utilizan el modo *Store-And-Forward* y por lo tanto se encarga de actuar como filtro analizando los datos.
- d) Interconectan las redes por medio de cables.
- e) Cuentan con varios puertos RJ45 integrados, desde 4, 8, 16, 32 y hasta 52.
- f) Permite la regeneración de la señal y son compatibles con la mayoría de los sistemas operativos de red.

Actualmente compite contra dispositivos hub, router y switch inalámbricos.

El puerto 1 y el que se encuentre debajo de él, regularmente se utiliza para recibir el cable con la señal de red o para interconectarse entre sí con otros switches (figura 2.6).

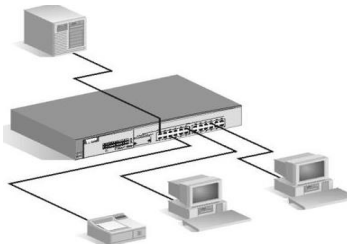


Figura 2.6 Esquema básico de un switch conectado a dos computadoras y una impresora, en la cual los elementos están compartiendo los recursos en red

Estándares

Se diseñaron para funcionar con ciertos estándares o protocolos (reglas de comunicación establecidas), las más comunes son las siguientes (véase tabla 2.3):

Tabla 2.3 Estándares del switch

Nombre	Estándar	Velocidad (Megabits por segundo)	Características
Ethernet	IEEE 802.3 (10BASET)	10 / 100 Mbps	Se utilizan en todo tipo de redes basadas en cable en escuelas, hospitales, hogares, etc.
Ethernet	IEEE 802.3u (10BASETX)	100 Mbps / 1000 Gigabit	Alta velocidad, soporta cableado de hasta 100 m, para cable UTP, soporta Half Duplex (envía o recibe datos, una acción a la vez, utilizando modo hub) o Full Duplex (envía y recibe datos de manera simultánea utilizando modo switch)

Uso específico del switch

Se utiliza para la rápida interconexión de redes; sin embargo, si cuentan con la función de bridge disminuye su funcionamiento debido a que se dedica a buscar errores en la información, pero en cuestiones de seguridad es mejor que se utilice en tal modo.

2.1.IV SERVIDORES

En Internet, un servidor es un ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras y son los proveedores de todos sus servicios, incluyendo la WWW (World Wide Web, las páginas web), FTP, correo electrónico, grupos de noticias, etc.

En redes locales se entiende como el software que configura una PC como servidor para facilitar el acceso a la red y sus recursos.

Los servidores almacenan información en forma de páginas web y a través del protocolo HTTP lo entregan a petición de los clientes (navegadores web) en formato HTML.

Funcionamiento

Básicamente, una computadora conectada a Internet emplea una dirección (dirección web, dirección IP, dirección FTP, etc.) para poder comunicarse con el servidor al que le corresponde. La computadora envía (utilizando el protocolo adecuado) las distintas solicitudes al servidor, y éste responde (empleando el protocolo adecuado) las solicitudes. El servidor también puede solicitar datos de la computadora, y ésta le responde.

Las solicitudes pueden ser de diferentes tipos, por ejemplo, en la figura 2.7 se observa que la PC 1 (Personal Computer, Computadora Personal) solicita una página web (www.alegsa.com.ar) específica al servidor del sitio web. El servidor web responde con el archivo HTML que corresponde. Si el servidor no encuentra el recurso, devuelve un mensaje (puede ser un mensaje de error 404 u otro).

En el ejemplo (figura 2.7), las PC 1, 2 y 3 se llaman clientes. La PC 1 emplea un programa llamado cliente web o navegador que está preparado para enviar y recibir este tipo de recursos (las páginas web). La PC 2 emplea un programa cliente e-mail, preparado para enviar y recibir e-mails. La PC 3 emplea un programa cliente FTP, con la capacidad y características para comunicarse con servidores FTP.

Los ejemplos de la figura 2.7 están simplificados, en la práctica existen muchos mensajes intercambiados (peticiones) entre el cliente y el servidor cuando se presta algún servicio. A cualquier computadora conectada a una red se le pueden instalar los programas y configuraciones adecuadas para ser un servidor.

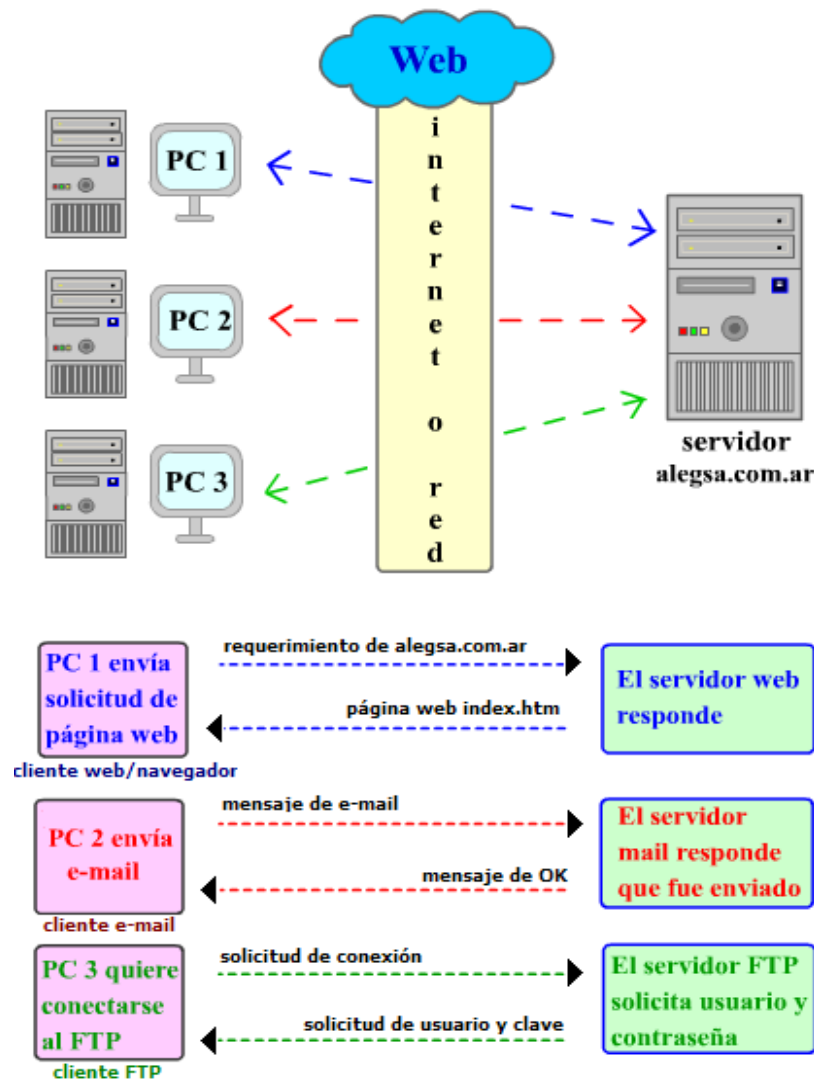


Figura 2.7 Gráfico esquemático simplificado del funcionamiento de las computadoras servidores en Internet.

Sin embargo, de acuerdo con el rol que asumen dentro de una red se dividen en:

1. Servidor dedicado: Son aquellos que le dedican toda su potencia a administrar los recursos de la red, es decir, atender las solicitudes de procesamiento de los clientes.

2. Servidor no dedicado: Son aquellos que no dedican toda su potencia a los clientes, sino también pueden jugar el rol de estaciones de trabajo al procesar solicitudes de un usuario local.

Para el caso de seguridad informática, se enfocará al estudio de los servidores web:

Servidores Web

Ofrece contenido estático al navegador, carga un archivo y lo brinda a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP (figura 2.8).

Se pueden utilizar varias tecnologías en el servidor para aumentar su potencia más allá de su capacidad de entregar páginas HTML; éstas incluyen scripts CGI, seguridad SSL y páginas activas del servidor (ASP).



Figura 2.8 Servidor web

En el servicio web clásico se dispone de aplicaciones web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- a) Aplicaciones en el lado del cliente: El cliente web es el encargado de ejecutarlas en la máquina del usuario. Son aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje JavaScript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.
- b) Aplicaciones en el lado del servidor: El servidor web ejecuta la aplicación, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como ocurre en el caso de querer ejecutar aplicaciones JavaScript o java. Cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

2.1.V PANEL DE PARCHEO

Se concentran todos los cables de las cajas de contacto que hay en el edificio; de manera que existe una conexión para cada caja de contacto en el panel de parcheo, para proporcionarle o suspenderle el servicio a un determinado departamento u oficina (figura 2.9). A este cableado se le conoce como cableado horizontal.

El cableado horizontal debe tener un medio por el cual distribuir el cable y el mejor conducto es la canaleta que permite de una forma flexible trazar los recorridos adecuados desde el espacio de trabajo hasta el panel de parcheo.



Figura 2.9 Panel de parcheo

Los paneles de parcheo se utilizan en bastidores y armarios de telecomunicaciones para el montaje de cable, con el fin de garantizar una conmutación de alta calidad (figura 2.10). Cada línea tiene asignado un puerto aparte del que tiene en el panel de parcheo. El panel de parcheo consiste en un bloque de puertos (RJ-45 End-Plug), la cantidad corresponde al número de puertos.

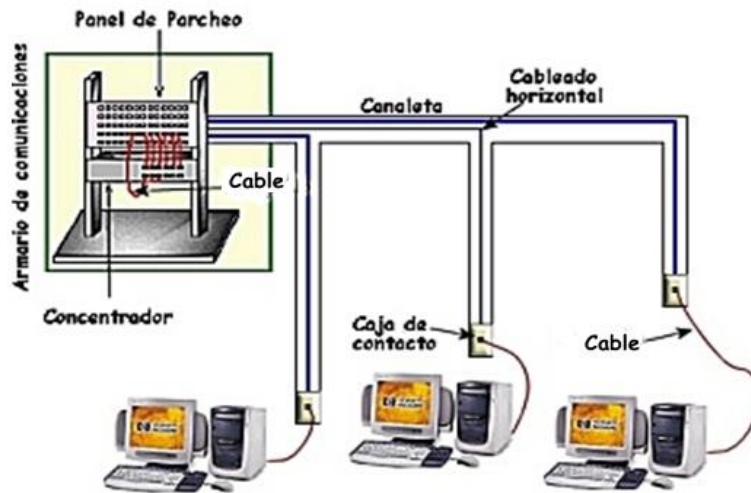


Figura 2.10 Componentes que integran al panel de parcheo

En la parte frontal del panel los puertos están señalados con marcaje numérico. En la parte inversa del panel, los contactos tienen marcaje numérico y de colores. El panel tiene porta etiquetas para completar el marcaje (figura 2.11).



Figura 2.11 Contactos con marcaje numérico

2.1.VI RACK

Es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante.

Los racks tienen armazón metálico con un ancho normalizado de 19 pulgadas (48.26 cm), mientras que el alto y el fondo son variables para adaptarse a las distintas necesidades. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón (figura 2.12).



Figura 2.12 Fotografía de un rack

La distancia entre cada guía horizontal está normalizada y se denomina altura o simplemente por la letra U. Todos los equipos deben adaptar su altura a un múltiplo de dicha unidad. Por ejemplo, un equipo 2U ocupará dos estantes de altura. Los bastidores se fabrican en diferentes alturas, el estándar es de 42U.

Funcionamiento

Los racks son muy útiles en un centro de proceso de datos, donde el espacio es escaso y se necesita alojar un gran número de dispositivos. Estos dispositivos suelen ser:

- a) Servidores cuya carcasa ha sido diseñada para adaptarse al bastidor. Existen servidores de 1U, 2U y 4U, recientemente se han popularizado los servidores blade que permiten compactar más de veinte servidores en una altura de 4U, compartiendo fuentes de alimentación y cableado.
- b) Conmutadores y enrutadores de comunicaciones.
- c) Cortafuegos.
- d) Sistemas de audio y video.

El equipamiento simplemente se desliza sobre un riel horizontal y se fija con tornillos. También existen bandejas que permiten apoyar equipamiento no normalizado. Por ejemplo, un monitor y un teclado.

2.1.VII GATEWAY (PUERTA DE ENLACE)

Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red destino. Además es un nodo de la red equipado para hacer de interfaz con otra red que usa un protocolo y arquitectura diferente a todos los niveles de comunicación (figura 2.13). El gateway usa los siguientes elementos:

- a) **Hardware:** Puede contener dispositivos como traductores de protocolos, dispositivos de adaptación de impedancias, conversores de razón, aisladores de errores o traductores de señales, necesarios para proveer de interoperabilidad al sistema. También es requerido un establecimiento de aceptación mutua entre ambas redes.
- b) **Software:** Un protocolo gateway de traducción/mapeo que interconecte redes con diferentes protocolos de red, realizando las conversiones de protocolos requerida.

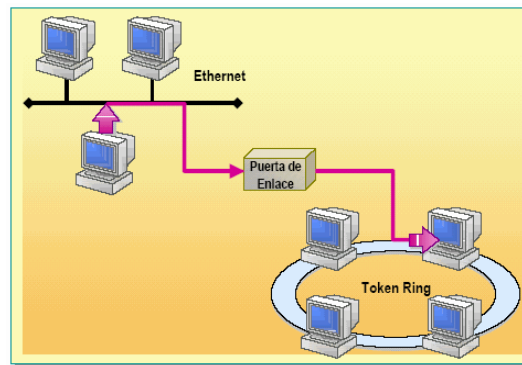


Figura 2.13 Puerta de enlace entre diferentes arquitecturas de red

La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local conectadas a él desde un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones.

Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP, usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet y una sola dirección IP externa.

La dirección IP de una puerta de enlace normalmente se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos como son: 127.x.x.x, 10.x.x.x, 172.16.x.x a 172.31.x.x, 192.168.x.x, que engloban o se reservan a las redes locales. Además se debe notar que necesariamente un equipo que cumpla el rol de puerta de enlace en una red, debe tener 2 tarjetas de red.

Una computadora gateway está configurada para tener 2 tarjetas de red y así realizar tareas en cualquier nodo que va a permitir conectar dos redes diferentes y que actúe como un conversor entre protocolos.

Funcionamiento

En las redes, los dispositivos finales se interconectan entre ellos mediante concentradores o conmutadores. Cuando se quiere agrupar esos últimos dispositivos, se pueden conectar esos concentradores a enrutadores. Estos últimos lo que hacen es conectar redes que utilicen distinto protocolo (por ejemplo, IP, NetBIOS, AppleTalk). Pero un enrutador solo puede conectar redes que utilicen el mismo protocolo. Cuando lo que se quiere es conectar redes con distintos protocolos, se utiliza una pasarela, ya que este dispositivo sí traduce las direcciones y formatos de los mensajes entre diferentes redes.

Default Gateway (puerta de enlace predeterminada)

Desempeñan una función importante en las redes TCP/IP. Proporcionan una ruta predeterminada que pueden utilizar los hosts TCP/IP para la comunicación con otros hosts en redes remotas.

La siguiente figura 2.14 muestra la función que desempeñan dos puertas de enlace predeterminadas (enrutadores IP) para dos redes: red 1 y red 2.

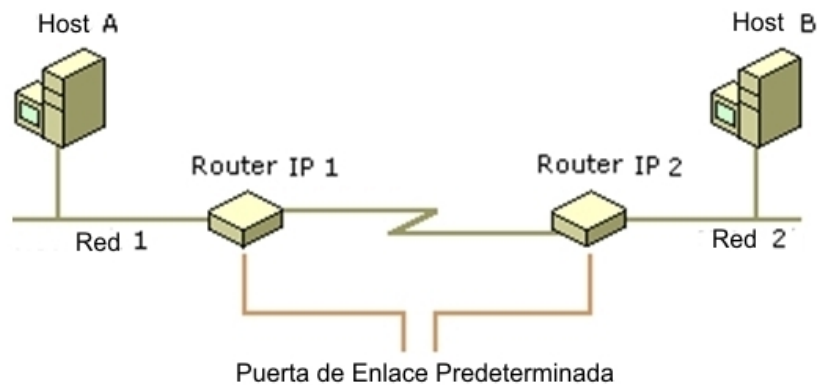


Figura 2.14 Función de dos puertas de enlace predeterminadas

Para que el host A (figura 2.14) de la red 1 pueda comunicarse con el host B de la red 2, el host A comprueba primero en su tabla de enrutamiento si existe una ruta específica al host B. Si no hay una ruta específica al host B, el host A reenvía el tráfico TCP/IP del host B a su propia puerta de enlace predeterminada, el enrutador IP 1.

El mismo principio se aplica si el host B (figura 2.14) envía tráfico al host A. Sin una ruta específica al host A, el host B reenvía el tráfico TCP/IP destinado al host A su propia puerta de enlace predeterminada, el enrutador IP 2.

Las puertas de enlace predeterminadas son importantes para que el enrutamiento IP funcione correctamente. En la mayor parte de los casos, el enrutador que actúa como puerta de enlace predeterminada para hosts TCP/IP, ya sea un enrutador dedicado o un equipo que conecta dos o más segmentos de red, mantiene información sobre otras redes de la red más grande y cómo llegar a ellas.

Los hosts TCP/IP se basan en puertas de enlace predeterminadas para la mayor parte de sus necesidades de comunicación con hosts de segmentos de red remotos. De esta forma, los hosts individuales están liberados de la carga de tener que mantener amplia información continuamente actualizada sobre segmentos de red IP remotos individuales. Solo el enrutador que actúa como la puerta de enlace predeterminada necesita mantener este nivel de información de enrutamiento para llegar a otros segmentos de red remotos del conjunto de redes más grande.

Si se produce un error en la puerta de enlace predeterminada, puede verse afectada la comunicación a partir del segmento de red local. La puerta de enlace predeterminada, al conectar dos redes de IP, poseerá:

- a) Una dirección IP privada: que servirá para identificarse dentro de la red local.
- b) Una dirección IP pública: que servirá para identificarse dentro de la red exterior.

2.2 MONITOREO DE RED

Es un sistema que constantemente revisa los signos vitales de la red en tiempo real para detectar sistemas lentos, en mal funcionamiento, fuera de servicio o con problemas como pueden ser las conexiones de red u otros dispositivos sobrecargados, notificando al administrador de la red en caso de falla vía correo electrónico u otras alarmas que dispongan. También es un proceso continuo de recolección y análisis de datos cualitativos y cuantitativos, con base en los objetivos planteados en las políticas de seguridad.

Entre las principales actividades del monitoreo se encuentran las dedicadas al desarrollo de tareas de supervisión, capaces de controlar resultados de operaciones diversas, así como programas que permitan la observación de variables seleccionadas.

Existen dos fundamentos para monitorear la red:

1. Mediante un historial de comportamiento de la red se pueden diagnosticar los cambios hacia el crecimiento a futuro.
2. Detectar los cambios inesperados en el estado de la red.

La detección oportuna de fallas y la predicción de cambios son actividades que permiten proporcionar un buen servicio a los usuarios.

2.2.1 ENFOQUES

En el monitoreo existen dos puntos de vista muy diferentes pero ambos se complementan.

1) Monitoreo Activo

Se realiza inyectando paquetes de prueba en la red o enviando paquetes a determinadas aplicaciones para medir sus tiempos de respuesta. Este monitoreo tiene la característica de agregar tráfico en la red pero también es utilizado para medir el rendimiento en la misma.

Métodos de monitoreo activo

a) Basado en ICMP

- ✓ Diagnosticar problemas en la red
- ✓ Detectar retardo y pérdida de paquetes.
- ✓ RTT (Round-Trip delay Time, Tiempo Aproximado de Viaje)
- ✓ Disponibilidad de host y redes.

b) Basado en TCP

- ✓ Tasa de transferencia
- ✓ Diagnosticar problemas a nivel aplicación

c) Basado en UDP

- ✓ Pérdida de paquetes en un sentido (one-way)
- ✓ RTT (traceroute, traza de la ruta)

2) Monitoreo Pasivo

Consiste en la obtención de datos a partir de la recolecta y análisis del tráfico que circula por la red al emplearse diversos dispositivos como pueden ser los sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para SNMP, RMON (Remote MONitoring, Protocolo de Monitoreo Remoto) y Netflow. Este monitoreo no agrega tráfico en la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y contabilizar su uso.

Métodos de monitoreo pasivo

a) Solicitudes remotas

- ✓ Usando SNMP se obtienen estadísticas del uso del ancho de banda en los dispositivos de red, para ello se requiere tener acceso a los mismos. Este protocolo genera paquetes llamados *traps* (alarmas) que indican que un evento inusual se ha producido.
- ✓ Realizando scripts que tengan acceso a los dispositivos remotos para obtener información importante. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública.

b) Captura de tráfico

- ✓ Hay dos maneras:
 - I. Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en el puerto hacia otro donde estará conectado el equipo que realizará la captura.
 - II. Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica contabiliza el tráfico que circula por la red.

c) Análisis de Tráfico

- ✓ Identifica el tipo de aplicaciones que son más utilizadas. Se puede usar un dispositivo llamado *probe* que envía información mediante RMON a través de un dispositivo intermedio que clasifica el tráfico de direcciones IP origen y destino, al igual que los puertos origen y destino.

d) Flujos

- ✓ Identifica el tipo de tráfico utilizado en la red. El flujo es un conjunto de paquetes con la misma IP origen y destino, el mismo puerto TCP origen y destino así como el mismo tipo de aplicación. Los flujos se obtienen de ruteadores mediante dispositivos que son capaces de capturar tráfico y transformarlo en flujos.

2.2. II CONEXIONES

El objetivo principal del monitoreo es descubrir las fortalezas y/o debilidades para establecer las diferentes líneas de acción que permite hacer las correcciones y reorientaciones necesarias en las técnicas de ejecución. Éstas técnicas hacen referencia a los diferentes tipos de conexiones que se pueden dar ya sea que provenga de un servidor a otro servidor, de una computadora a un servidor o simplemente de una red local. Estas conexiones se pueden dividir en los siguientes subprocesos:

- a) Monitoreo de la conexión: Mediante el inicio de sesión que los usuarios realizan para poderse conectar a la red pueden tener algunos problemas o fallas como son las de peticiones de estado (la conexión no pudo ser establecida), tiempo de espera agotado, etcétera. Usualmente produce una acción al sistema de monitoreo como puede ser una alarma enviada al administrador o una ejecución automática de mecanismos de controles de fallas.
- b) Monitoreo del tráfico: Comprende la identificación de aquellas situaciones en donde el tráfico no cumple con las políticas específicas o cuando éste excede los límites bien definidos. Algunas características incluyen:
 - ✓ Detectar fallas en la red y controlar su estado
 - ✓ Buscar el flujo de paquetes y detectar duplicados de direcciones IP
 - ✓ Identificación de hosts locales en modo promiscuo
 - ✓ Configuraciones erróneas en el software a través del análisis de los protocolos implicados
 - ✓ Identificación de hosts que están usando protocolos innecesarios
 - ✓ Identificación de estaciones de trabajo mal configuradas actuando como enrutadores
 - ✓ Uso excesivo del ancho de banda disponible

- c) Monitoreo remoto: Se realiza mediante agentes que recogen información y la trasladan a una consola central. Existe un agente para cada uno de los segmentos de la red monitorizada que pueden ser un host dedicado, dispositivo de red, etcétera. Las principales consolas de administración remota proporcionan dos ventajas en los procesos de red:
1. Puede existir más de un administrador en diferentes ubicaciones para monitorear y administrar la misma red.
 2. Entre más consolas administrativas mejor, porque si una falla, la otra podrá tomar su lugar.
- d) Monitoreo de aplicaciones: Supervisa la ejecución de las aplicaciones para controlar el uso debido a las licencias, determina la existencia de situaciones de carga extrema o saturación de los servicios de red que pudieran estar degradando el servicio ofrecido por la aplicación y verifica el número de clientes que acceden simultáneamente usando opciones de bloqueo.

2.2. III ANÁLISIS DE PAQUETES

Una de las tareas principales de un administrador de red es monitorear el tráfico de sus redes para que no tenga pérdida de paquetes, no se pierda la conectividad, no se desconecten los equipos sin motivo aparente y se logre obtener el máximo rendimiento posible en la red que gestiona.

La causa principal de los problemas en la red se da por tener una mala configuración en broadcast, spanning-tree, enlaces redundantes, aunque en algunas ocasiones puede tratarse de ataques inducidos por terceros al intentar dejar fuera un servidor web mediante ataque DoS (Denial of Service, Denegación de Servicio), husmear tráfico mediante un envenenamiento de ARP o simplemente infectar los equipos con código malicioso para que formen parte de una red zombi (botnet).

Para solucionar los casos anteriores primero se debe conocer el origen del incidente para poder tomar las contramedidas necesarias y conseguir una correcta protección.

En el mercado del software hay varios programas muy útiles para el análisis de paquetes en la red; captura de los paquetes que se generan, correlación del tráfico identificando las amenazas para que posteriormente se pueda limitar su impacto y mostrar el contenido de forma muy sencilla. En general los programas pueden hacer lo que a continuación de menciona:

- a) Si se tiene una red con distintas subredes y diferentes enrutamientos, se puede analizar si un paquete no llega correctamente a su destino. Esto se logra al ir monitorizando en los distintos nodos si el paquete va pasando por ellos y con qué datos (dirección IP origen y destino).
- b) Si la red tiene NAT se puede comprobar si el paquete hace el NAT correctamente o no (dirección IP privada se sustituye o se mantiene).
- c) Si hay broadcasts en la red, verifica que el equipo monitor reciba el paquete.
- d) Se puede usar para hacer una auditoría, al dejar un rato funcionando el programa y después se comprueba el tráfico habitual de la red.
- e) Captura automática de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por crackers para atacar sistemas posteriores.
- f) Conversión del tráfico de red en un formato inteligible por los humanos.
- g) Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?
- h) Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- i) Detección de intrusos, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados IDS (Intrusion Detection System, Sistema de Detección de intrusos), éstos son prácticamente analizadores con funcionalidades específicas.
- j) Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.
- k) Desarrollar aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red.

Con base en lo anterior, se hará un enfoque en los paquetes IP y TCP en la red para el análisis de paquetes.

1. *Paquete IP*

La información es cortada en pequeños bloques de datos y enviados de forma independiente a la dirección destino, luego el receptor pega cada bloque, a esto se le conoce como paquete *IP*.

Cada paquete transporta la dirección IP origen y destino así como el número de bloques en que se partió el paquete, también llevan los datos de los protocolos que Internet utiliza (TCP/IP). Cada paquete contiene parte del cuerpo del mensaje y suelen llevar unos 1500 bytes, al momento de ser enviado el paquete, éste se irá por la mejor ruta disponible aunque no todos los bloques se irán por la misma ruta.

Si hubiera algún problema con uno o varios equipos al momento de transferir el mensaje, los paquetes pueden ser encaminados por sitios alternativos, asegurando la entrega total del mensaje.

2. Paquete TCP

Con el protocolo TCP las aplicaciones pueden comunicarse en forma segura (sistema de acuse de recibo) independientemente de las capas inferiores. Los routers que funcionan en la capa de Internet solo envían los datos en forma de datagramas sin preocuparse por el monitoreo de datos ya que esta función la cumple la capa de transporte (protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora es la que solicita la conexión y se le llama cliente, a la máquina receptora se le llama servidor. Por eso se dice que se está en un entorno cliente-servidor. Las máquinas de dicho entorno se comunican en línea por lo que la comunicación se realiza en ambas direcciones (bidireccional).

Para adecuar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan y se le agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción. TCP es capaz de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman segmentos (figura 2.15).

URG ACK PSH RST SYN FIN																																			
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
Puerto de origen																Puerto de destino																			
Número de secuencia																																			
Número de acuse de recibo																																			
Margen de datos				Reservado				URG ACK PSH RST SYN FIN				Ventana																							
Suma de control																Puntero urgente																			
Opciones																								Relleno											
Datos																																			

Figura 2.15 Segmento TCP

2.2. IV ENCADENAMIENTO DE PAQUETES

El encaminamiento es una función necesaria en todas las redes excepto en las LAN ya que proporciona una conexión directa entre todos los pares de hosts conectados.

La función principal de la capa de red es enrutar la máquina origen al destino. En la mayor parte de las subredes los paquetes requieren hacer varias escalas antes de lograr completar su trayecto.

El algoritmo de enrutamiento se encarga de decidir la línea de salida por la que se transmitirá un paquete. Los algoritmos de encadenamiento se pueden agrupar en dos clases principales:

1) No Adaptativos

No basa su encaminamiento en mediciones, estimaciones del tráfico o topología actuales; elige la ruta que determina anticipadamente fuera de línea y se carga en los IMP (Interface Message Processor, Procesador de Mensajes Interfaz) cuando la red inicia, aunque el encaminamiento sea estático no habrá cambios.

2) Adaptivos

Cambia la decisión de encaminamiento para reflejar los cambios de topología del tráfico actual. La entrega de los paquetes a su destino es responsabilidad de los routers situados en los puntos de conexión. El paquete deberá ser transmitido en una serie de saltos, pasando a través de los routers. La determinación de las rutas a seguir para que un paquete llegue a su destino es responsabilidad del algoritmo de encaminamiento y por un programa en la capa de red de cada nodo (figura 2.16).

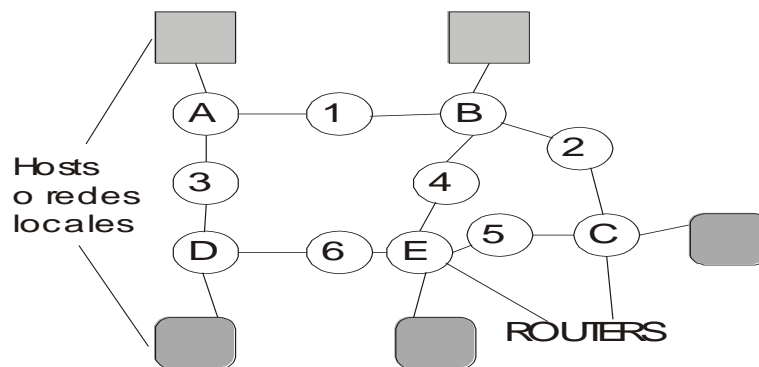


Figura 2.16 Ejemplo de varias redes LAN conectadas a varios routers

Hay tres algoritmos que se diferencian de acuerdo con la información que se utiliza:

- Globales*: utiliza información recogida en toda la subred para tomar decisiones óptimas. También se le conoce como encaminamiento centralizado.
- Locales*: opera en forma separada sobre cada IMP, solo utiliza la información que se encuentra disponible como la longitud de las colas de espera. También se les conoce como algoritmo aislado.
- Combinación de información global y local*: se conoce como algoritmo distribuido.

2.2. V FRAGMENTACIÓN DE PAQUETES IP

Se ha visto que las tramas físicas tienen un campo de datos y es aquí donde se transportan los datagramas IP. En este campo los datos no pueden tener una longitud indefinida debido a que está limitado por el diseño de la red. El MTU (Maximum Transmission Unit, Unidad Máxima de Transmisión) de una red es la mayor cantidad de datos que puede transportar su trama física. El MTU de las redes Ethernet es 1500 bytes y el de las redes Token-Ring, 8192 bytes. Esto significa que una red Ethernet nunca podrá transportar un datagrama de más de 1500 bytes sin fragmentarlo.

El router fragmenta un datagrama en varias partes si el siguiente tramo de la red por el que viaja tiene un MTU inferior a la longitud del mismo. Se observa con el siguiente ejemplo cómo se produce la fragmentación de un datagrama:

Se desea transmitir un datagrama IP de 1420 bytes de datos desde el ordenador A que se encuentra en la Red 1 hasta el ordenador B de la Red 2 (figura 2.17).



Figura 2.17 Se transmite un datagrama de 1420 bytes que sale del ordenador A y atraviesa la red 1 sin ningún problema ya que el MTU es de una red Ethernet y es menor a 1500



Figura 2.18 El siguiente paso que realiza el datagrama es que llega al router 1 y verifica su tamaño para que pueda atravesar la red 2 pero al ver que su MTU es de 620 bytes, entonces fragmenta el datagrama

Cada uno de estos fragmentos es un nuevo datagrama con el mismo identificador pero distinta información en los campos de desplazamiento de fragmentación y MF (More Fragments, Más Fragmentos) (figura 2.18).

- Fragmento 1: Long. Total = 620 bytes; Campo de desplazamiento = 0; MF=1
- Fragmento 2: Long. Total = 620 bytes; Campo de desplazamiento = 600; MF=1
- Fragmento 3: Long. Total = 620 bytes; Campo de desplazamiento = 1200; MF=0



Figura 2.19 Ahora el datagrama original se divide en tres fragmentos que se convierten en un nuevo datagrama con el mismo identificador pero distinta información en los campos de desplazamiento de fragmentación y MF la cual es encaminada en el router 2.

En la figura 2.19 se hace el ensamble de los tres paquetes para convertirlo en el datagrama original (figura 2.20).



Figura 2.20 El router 2 manda los fragmentos a la red 2, el ordenador B recibe y ensambla los fragmentos para tener el datagrama original

La fragmentación IP denota la distribución de un paquete IP entre varios bloques de datos, si su tamaño sobrepasa la MTU del canal.

El objetivo de la fragmentación IP es ocultar la infraestructura IP de las capas más altas para implantar protocolos independientes de hardware.

Proceso de fragmentación

El tamaño máximo de un datagrama es de 65,536 bytes. Este valor nunca es alcanzado porque las redes no tienen suficiente capacidad para enviar paquetes tan grandes. Las redes en internet utilizan diferentes tecnologías; por lo tanto, el tamaño máximo de un datagrama varía según el tipo de red (tabla 2.4). El datagrama se fragmentará si es más grande que la de la red.

Tabla 2.4 MTU en diferentes redes

Tipo de red MTU (en bytes)	
Arpanet	1000
Ethernet	1500
FDDI	4470

La fragmentación del datagrama se lleva a cabo a nivel de router, es decir, durante la transición de una red con una MTU grande a una red con una MTU más pequeña. Si el datagrama es demasiado grande para pasar por la red, el router lo fragmentará, es decir, lo dividirá en fragmentos más pequeños que la MTU de la red, de manera tal que el tamaño del fragmento sea un múltiplo de 8 bytes.

El router enviará estos fragmentos de manera independiente y los volverá a encapsular (agregar un encabezado a cada fragmento) para tener en cuenta el nuevo tamaño del fragmento. Además, el router agrega información para que el equipo receptor pueda rearmar los fragmentos en el orden correcto. Sin embargo, no hay nada que indique que los fragmentos llegarán en el orden correcto, ya que se enrutan de manera independiente.

Para tener en cuenta la fragmentación, cada datagrama cuenta con diversos campos que permiten su rearmado:

- a) Campo margen del fragmento (13 bits): Brinda la posición del comienzo del fragmento en el datagrama inicial. La unidad de medida para este campo es 8 bytes (el primer fragmento tiene un valor cero).
- b) Campo Identificación (16 bits): Número asignado a cada fragmento para permitir el rearmado.

- c) Campo Longitud total (16 bits): Esto se vuelve a calcular para cada fragmento.
- d) Campo Indicador (3 bits): Está compuesto de tres bits:
 - 1) El primero no se utiliza.
 - 2) *El segundo (denominado DF - No fragmentar)*: Indica si se puede fragmentar el datagrama o no. Si el datagrama tiene este bit en uno y el router no puede enrutarlo sin fragmentarlo, el datagrama se rechaza con un mensaje de error.
 - 3) *El tercero (denominado MF - Más fragmentos)*: Indica si el datagrama es un fragmento de datos (1). Si el indicador se encuentra en cero, esto indica que el fragmento es el último (entonces el router ya debe contar con todos los fragmentos anteriores) o que el datagrama no se ha fragmentado.

Efectos

Aunque el objetivo es una implementación para capas más altas (por ejemplo TCP/UDP) éste no está consentido en dos puntos:

- 1) La fragmentación puede tener una gran influencia negativa en la actuación y en el flujo de datos.
- 2) Si se pierde un pedazo fragmentado del paquete original, hay que transmitir completamente el paquete original otra vez. Sin embargo, IP no tiene mecanismos de seguridad o de timeout y es dependiente de las funciones de seguridad de las capas más altas como TCP.

Por las razones arriba mencionadas se intenta evitar la fragmentación siempre que sea posible.

2.2. VI PATRONES NORMALES

Al instalar una red de computadoras en un edificio se tiene contemplado un número posible de equipos, teniendo en cuenta que este número se pueda incrementar a futuro; al momento de planear la red se calcula un posible incremento en la misma, por tal motivo se usa una gráfica de comportamiento en la cual se estudian los datos de procesos en cuanto a las tendencias o los patrones a lo largo del tiempo.

Al registrar los puntos de datos en el orden en el cual ocurren, la gráfica de comportamiento ofrece información visual de los cambios en el proceso. Estos puntos de datos pueden o no revelar una tendencia o patrón en el proceso.

La media del proceso es calculada y presentada como una línea horizontal sólida en la gráfica. En una gráfica de comportamiento, se espera que los puntos de datos varíen aleatoriamente hacia abajo y arriba de la línea media como se muestra en la figura 2.21.

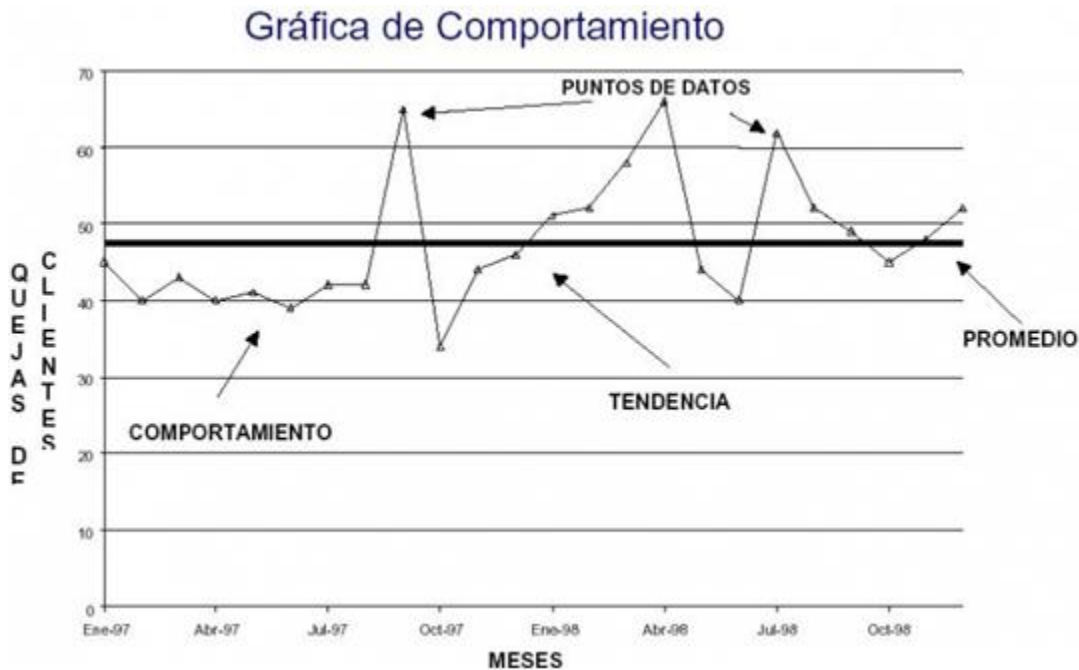


Figura 2.21 Ejemplo de una gráfica de comportamiento donde se indican los principales datos a tomar en cuenta

A continuación se explica brevemente cada uno de los datos a tomar en cuenta en una gráfica de comportamiento.

Características

1) Promedio

- a) Establecer una línea base (promedio): Permite comparar el desempeño inicial con el desempeño mejorado.
- b) Realizar un seguimiento de las mediciones consecutivas: Los resultados de varios procesos en una gráfica de comportamiento se obtiene una representación de cómo los resultados varían en el tiempo.

- c) Análisis de un proceso: Se tiene que ignorar el comportamiento aceptable y normal del proceso y enfocar únicamente los cambios que alteran el proceso significativamente. Una gráfica de comportamiento permite rastrear rápidamente los patrones anormales tales como los comportamientos y las tendencias; lo cual, es poco probable que sean causados por patrones aleatorios.
- d) Realizar cambios a un proceso: Es importante observar y entender cómo el resultado ha sido afectado por los cambios que se han efectuado. Al realizar una gráfica de comportamiento se puede comparar el antes y el después para saber si el cambio tuvo el comportamiento adecuado.

2) Comportamiento

- a) ¿Qué se va a medir?: Seleccionar el proceso y/o los resultados apropiados.
- b) Establecer un marco de tiempo a medir: Determinar el período de tiempo a medir (cada hora, diariamente, semanalmente, etcétera).
- c) Trazar un eje vertical a la izquierda: Representa el valor medido. Indica el número de ocurrencias esperadas, utilizando intervalos apropiados desde 0 hasta los valores más altos a la izquierda del eje vertical.
- d) Trazar un eje horizontal en la base: Representa el tiempo o la secuencia. Indica los límites de tiempo a lo ancho de la parte inferior del eje horizontal.
- e) Marcar cada punto: Los datos que se obtienen se van a marcar en una gráfica a medida que ocurren y posteriormente se conectarán los puntos.
- f) Calcular el promedio aritmético: Es conocido como la media. En algunos casos se tendrá que calcular la mediana en vez de la media.
- g) Marcar y presentar la gráfica.
- h) Analizar los resultados: Buscar tendencias y comportamientos. Buscar una distribución uniforme de los puntos de datos alrededor de la línea central (media). Buscar cualquier punto de datos exageradamente altos o bajos que pueden indicar un problema anormal en el proceso.

Para calcular la mediana existen dos formas:

1. Para un número impar de puntos de datos:
 - a) Ordenar los puntos de los datos del más bajo al más alto.
 - b) Encontrar el valor que separa los datos en dos partes. Este valor será la mediana.
2. Para un número par de puntos de datos:
 - a) Ordenar los datos de los puntos del más bajo al más alto.
 - b) Dividir el número de puntos de datos en dos para encontrar el punto medio.
 - c) Localizar el número que esté encima del punto medio.

- d) Sumar los dos valores que se localizaron en el inciso b y c.
- e) Dividir la suma del inciso anterior entre 2, el valor obtenido será la mediana.

Interpretación de la gráfica de comportamiento

- a) Es una representación de puntos de datos a través del tiempo. Esta representación puede o no corresponder un patrón o tendencia.
- b) El comportamiento puede ser un punto de datos individuales o una serie de puntos de datos consecutivos al mismo lado de la línea media (promedio). Conociendo el número de comportamientos en una gráfica puede ayudar a determinar si el proceso está siendo influenciado por causas especiales. El número de puntos de datos en la muestra determina el número de puntos consecutivos que constituye un comportamiento.
- c) La tendencia es una serie de aumentos o disminuciones consecutivas. En una gráfica de comportamiento no debería haber ninguna tendencia exageradamente larga. Si la tiene, el proceso deberá ser investigado para determinar qué ha cambiado para que cause la tendencia. El número de puntos de datos en su muestra determina el número de puntos consecutivos que constituyen una tendencia.
- d) Los datos reunidos deberán permanecer y presentarse en el orden en el cual fueron reunidos.

Una gráfica de comportamiento generalmente se relaciona con:

- a) Hoja de verificación
- b) Checklist para la reunión de datos
- c) Gráficas de control

Testeo Estadístico

- a) Duración del comportamiento: Un punto de datos individual o una serie consecutiva de puntos de datos en un mismo lado de la media.
- b) Número de comportamientos: Un proceso que no está influenciado por causas especiales no tendrá demasiados comportamientos o muy pocos comportamientos. El número de comportamientos es hallado por simple conteo.
- c) Tendencia(s): Aumentos o disminuciones consecutivos. La gráfica de comportamiento no deberá tener ninguna serie exageradamente larga de aumentos o disminuciones consecutivos.

2.2. VII PATRONES ANORMALES

Se entiende por comportamiento anómalo a la conducta que presentan las máquinas involucradas en el análisis de una red. Estos comportamientos pueden deberse a diversos factores entre los cuales podemos mencionar el mal funcionamiento de la interfaz de red de una computadora, virus informáticos o la presencia de intrusos entre otras cosas.

El tráfico anómalo se puede dividir en 4 partes:

- 1) Técnicas de reconocimiento
 - a) Ping Sweep
 - b) ARP Sweep
 - c) Syn Scan
 - d) Xmas Scan with Decoys
- 2) Ataques de red
 - a) ARP Poison
 - b) Syn Flooding
- 3) Malware
 - a) Nimda
 - b) Clientes infectados con un Bot
- 4) Explotación de vulnerabilidades
 - a) Ataque de fuerza bruta y de diccionario
 - b) SQL Injection y Path Traversal

Para ayudar a prevenir los pasos anteriores existen 2 métodos que son:

1. Sistemas de detección de intrusos (IDS)
2. Snort

A continuación se da una breve introducción de estos dos métodos ya que en el CAPÍTULO 5. *Defensa en redes*, Subtema 5.2 *Detección de intrusos*, se habla a detalle de ellos.

1. Sistemas de detección de intrusos (IDS)

Es una herramienta de seguridad que detecta o monitorea los eventos que van ocurriendo en un determinado sistema informático o red de computadoras en busca de patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa que intenten comprometer la seguridad del sistema.

Este método tiene una capacidad de prevención y de alerta anticipadamente a cualquier actividad sospechosa, aunque no está diseñado para detener un ataque pero sí puede generar ciertos tipos de respuesta ante éstos.

Un IDS puede aumentar la seguridad del sistema al vigilar el tráfico de la red e ir examinando los paquetes en busca de datos sospechosos y detectar las primeras fases de cualquier ataque como puede ser el análisis de la red, barrido de puertos, etcétera.

2. Snort

Es un IDS que se basa en la red (NIDS) al implementar un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como pueden ser los patrones que corresponden a ataques, barridos, intentos para aprovechar alguna vulnerabilidad, análisis de protocolos, etcétera. Todo esto lo hace en tiempo real.

2.2. VIII TRÁFICO DE RELLENO

Es un mecanismo de seguridad utilizado para brindar protección contra ataques de análisis de tráfico y consiste en enviar tráfico espurio (falso) junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

El tráfico de relleno pertenece a uno de los tipos de mecanismos de seguridad que existen, los cuales se pueden dividir en 2 grupos:

1. Específicos: Se pueden incorporar en alguna capa de red donde se use un protocolo; los servicios que más se incorporan son:
 - a) Cifrado.
 - b) Firma digital.
 - c) Control de acceso y autenticación.
 - d) Integridad de los datos.
 - e) Tráfico de relleno.
 - f) Control de enrutamiento.
 - g) Notarización.

2. Generales: Se relacionan con los niveles y manejo de seguridad requeridos. Se aplican a los sistemas para cumplir la política general de seguridad de la organización, los cuales pueden ser:
 - a) Funcionalidad fiable
 - b) Detección de acciones
 - c) Integridad de los datos
 - d) Informes para auditorías de seguridad
 - e) Recuperación de la seguridad

Funcionamiento

Produce una salida de texto cifrada de forma continua, incluso en ausencia de texto plano. Un flujo continuo de datos se genera al azar. Cuando el texto plano está disponible, éste es encriptado y transmitido. Cuando la entrada de texto plano no está presente, los datos aleatorios son encriptados y transmitidos. Esto hace que sea imposible que un atacante pueda distinguir entre el flujo de datos reales con el relleno y por lo tanto imposible deducir la cantidad de tráfico.

El tráfico de relleno es esencialmente una función de encriptación de enlace. Si solo se usa el cifrado de extremo a extremo, entonces las medidas de defensa son más limitadas. Si el cifrado se implementa en la capa de aplicación, un oponente puede determinar qué capa de transporte usa, las direcciones de la capa de red y los patrones de tráfico que siguen siendo accesibles.

Desventajas del tráfico de relleno

El uso de tráfico de relleno puede reducir el ancho de banda disponible de la red para atender el tráfico real. Al considerar el siguiente escenario en el que los paquetes pueden pasar a través de uno o más nodos intermedios. Por ejemplo, un enlace de una red superpuesta construido en la cima de las redes IP puede pasar a través de routers intermedios IP, mientras que un enlace de una red IP puede pasar a través de intermediarios switches Ethernet. En estos casos, el tráfico de relleno en el enlace aumentará la carga sobre los nodos intermedios y los enlaces adyacentes y por lo tanto, reduce su ancho de banda disponible para servir a otros de tráfico real. Teniendo en cuenta que el tráfico de relleno y el tráfico real se supone que son indistinguibles, y por lo tanto no sería apropiado asumir que los nodos intermedios pueden dar tratamientos normales de circulación preferencial sobre el tráfico de relleno.

El tráfico de relleno es un mecanismo de seguridad y depende de los recursos de la organización si decide usarlo porque afecta el rendimiento de la red durante un largo tiempo y si no se cuenta con una planeación correcta de la infraestructura puede llegarse a colapsar.

CAPÍTULO 3

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA



CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Se conoce como *IT (Information Technology, Tecnología de la Información)* a la utilización de tecnología (computadoras y dispositivos inteligentes) para el manejo y procesamiento de información (captura, almacenamiento, protección, recuperación de datos e información). Conforme el mundo y las sociedades utilicen cada vez más este valioso recurso y de igual forma dependan de él, más importante y crítica se volverá la seguridad de la información.

El conocimiento permite, en cierta forma, un determinado control o poder sobre alguna actividad o tarea; basado en esto, el contexto informático puede hablar de quien tiene el suficiente conocimiento para entender todo lo relativo a la computación, podrá entrar a un mundo diferente, donde se dará cuenta de quién tiene la información tiene el poder.

Por lo tanto, se debe poner mayor énfasis al valor de la información porque después de los recursos humanos, la información es el activo más valioso de cualquier organización o persona.

La seguridad de la información es un asunto que puede afectar la vida privada de las personas; por ello, resulta de interés proteger día a día la información de cualquier amenaza o ataque.

La forma principal para reducir la inseguridad de la información es crear conciencia de la importancia de proteger a la información al considerar: ¿qué se quiere proteger?, ¿de qué se quiere proteger? y ¿cómo se va a proteger la información?.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD **INFORMÁTICA**

3.1 FUNDAMENTOS TEÓRICOS

El concepto de *seguridad* se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar cualquier acción que comprometa la información.

La *información* es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Por lo tanto, la *seguridad de la información* son aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que éste último solo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

3.1.1 CONCEPTO DE SEGURIDAD INFORMÁTICA

Es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático al igual que a sus usuarios. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Técnicamente es imposible lograr un sistema informático seguro, pero teniendo buenas medidas de seguridad se evitan daños y problemas que pueden ocasionar los intrusos.

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

- a) Información contenida: Debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. Al no proteger la información

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

se corre el riesgo de que sea utilizada maliciosamente para obtener ventajas de ella o sea manipulada, ocasionando lecturas erradas o incompletas de la misma.

- b) Infraestructura computacional: Almacena y gestiona la información, la función principal de esta área es que los equipos funcionen adecuadamente y tenga elaborado un plan de fallas, robo de equipos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- c) Usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información, se deben establecer normas que minimicen los riesgos a la información o a la infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, crear perfiles de usuario, planes de emergencia y protocolos.

Evolución de la seguridad informática

En la siguiente tabla 3.1 se muestra la evolución que ha tenido la seguridad informática desde sus inicios.

Tabla 3.1 Historia de la seguridad informática

Principios (1940-1960)	<ul style="list-style-type: none">✓ Con la aparición de la informática, se generan los primeros intentos de acceder a la información confidencial.✓ Esto provoca que se comiencen a desarrollar estudios sobre la seguridad, por lo que aparecen el TEMPEST y los Tiger Teams.
Etapa de los modelos formales de Seguridad (1970-1980)	<ul style="list-style-type: none">✓ Esta etapa se centra en el control de acceso a los sistemas de información, comienzan a aparecer las contraseñas.✓ Aparecen los primeros modelos formales de seguridad, dentro de los que destacan: Bell, BIBA, Harrison-Russo-Ullman, Clark-Willson, Lattice, Chinese Wall, entre otros.✓ Se desarrollan los primeros sistemas operativos con mecanismos de seguridad (MULTICS).

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Etapa de los Estándares y Mejores Prácticas de Seguridad (1980-1990)	<ul style="list-style-type: none">✓ En 1983 el Orange Book (Libro naranja) establece criterios para medir el nivel de confianza de un sistema.✓ Se comienzan a desarrollar organismos de conocimiento de seguridad e informática como: ISACA, ITU, IEEE, NIST, BSI e ISO; que comienzan a desarrollar estándares de seguridad.
Etapa de la Seguridad Estratégica (1990-?)	<ul style="list-style-type: none">✓ En esta etapa la seguridad informática se sale de la esfera de influencia del área de tecnología y se vuelve estratégica para la organización.✓ Las organizaciones empiezan a buscar certificar sus operaciones de tecnología bajo estándares de seguridad reconocidos internacionalmente (BS7799-2, ISO 27001).✓ Aparece el IPSEC (protocolo para la transmisión segura de información) y AES (estándar para criptografía)

3.1.II VULNERABILIDAD

Es la capacidad, condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, son puntos débiles existentes en el activo o en el entorno que al ser explotados por una amenaza ocasionan un ataque.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Los primeros pasos para implementar la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información. Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Los puntos débiles dependen de la forma en que se organizó el ambiente en que se maneja la información y con la presencia de elementos que perjudican el uso adecuado de la información así como el medio en que la misma se está utilizando.

Con base en lo anterior, se observan seis tipos de vulnerabilidades.

a) Física

Son aquellas presentes en los ambientes donde la información se está manejando o almacenando físicamente, como ejemplos de este tipo de vulnerabilidad se distinguen:

1. Instalaciones inadecuadas del espacio de trabajo.
2. Ausencia de recursos para el combate a incendios.
3. Disposición desorganizada de cables de energía y de red.
4. Identificación de personal interno y externo.

b) Natural

Se relacionan con las condiciones de la naturaleza que puedan colocar en riesgo la información.

La probabilidad de estar expuestos a las amenazas naturales es determinante en la elección y construcción del inmueble. Se deberá tomar en cuenta lo siguiente:

1. Ambientes sin protección contra incendios.
2. Inmuebles próximos a ríos propensos a inundaciones.
3. Infraestructura incapaz de resistir las manifestaciones de la naturaleza como terremotos, maremotos, huracanes, etcétera.

c) Hardware

Los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos, se puede mencionar:

1. Al no instalar las actualizaciones que hace el fabricante donde se previenen los errores que se van encontrando en el software.
2. Conservación inadecuada de los equipos.
3. La falta de configuración de respaldos o equipos de contingencia.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Por ello, la seguridad de la información busca evaluar si el hardware utilizado está dimensionado correctamente para sus funciones. Si posee área de almacenamiento suficiente, procesamiento y velocidad adecuada.

d) Software

Son aplicaciones malintencionadas que permiten el acceso indebido al sistema informático incluso sin el conocimiento de un usuario o administrador de red, entre éstos se destacan:

La configuración e instalación indebida de programas en la computadora que podrán llevar al uso abusivo de los recursos por parte de usuarios malintencionados. A veces la libertad de uso implica el aumento del riesgo.

Las aplicaciones son los elementos que efectúan una lectura de información y que permiten el acceso de los usuarios a dichos datos por el medio electrónico y, por esta razón, se convierten en el objetivo predilecto de agentes causantes de amenazas.

1. Programas lectores de e-mail que permiten la ejecución de códigos maliciosos.
2. Editores de texto que permiten la ejecución de virus de macro.
3. Programas para la automatización de procesos.
4. Los sistemas operativos conectados a una red.

e) Red

Por donde sea que la información transite, ya sea vía cable, satélite, fibra óptica u ondas de radio debe existir seguridad. El éxito en la transmisión de los datos es un aspecto crucial en la implementación de la seguridad de la información.

Hay un gran intercambio de datos a través de medios de comunicación que rompen barreras físicas.

Siendo así, estos medios deberán cumplir con ciertas normas de seguridad adecuado con el propósito de evitar que: Cualquier falla en la comunicación haga que la información no esté disponible para los usuarios, o por el contrario, estar disponible para quien no posee derechos de acceso.

1. La ausencia de un método de encriptación en las comunicaciones pudiera permitir que personas ajenas a la organización obtengan información privilegiada.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

2. La mala elección de un sistema de comunicación para el envío de mensajes de alta prioridad de la empresa pudiera provocar que no alcanzara el destino esperado o bien se interceptara el mensaje en su tránsito.

f) Humana

Esta categoría está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta.

Los errores humanos pueden ser intencionales o no. Muchas veces estos errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los miembros internos de la empresa.

Se destacan los principales puntos débiles por su grado de frecuencia:

1. Falta de capacitación específica para la ejecución de las actividades inherentes a las funciones de cada uno.
2. Falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones.
3. Contraseñas débiles.
4. Falta de uso de criptografía en la comunicación.
5. Compartimiento de identificadores tales como nombre de usuario o credencial de acceso.

En lo que se refiere a las vulnerabilidades humanas de origen externo, se pueden considerar todas aquellas que puedan ser exploradas por amenazas como: vandalismo, estafas, invasiones, etcétera.

3.1.III AMENAZAS²

Se representa a través de una persona, circunstancia, evento, fenómeno o una idea maliciosa que puede provocar poco o mucho daño cuando existe una violación de la seguridad. Por lo tanto, es todo aquello que puede, intenta o pretende destruir a un

² Para mayor información véase el apéndice B

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

activo. Si no se ha efectuado ningún ataque se considera como un daño latente que no se ha concretado.

Los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales pueden ser: causas naturales o no naturales, causas internas o externas.

Las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia-tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil.

Las amenazas se clasifican dependiendo de las fuentes que las generan:

a) Factor humano

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos. Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados, por descuido, por inconformidad, etcétera.

b) Errores de hardware

Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

c) Errores de la red

Se presenta cuando la red de comunicación no está disponible para su uso, esto puede ser provocado por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema. Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red y la extracción lógica de información a través de ésta.

d) Software

Son fallas dentro del programa de un sistema operativo, mal desarrollado, diseñado o implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

e) Naturales

Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de inoperabilidad permanente. Este tipo de amenazas también incluye la falta de preparación.

Algunos tipos de desastres naturales que amenazan a un sistema de información son: inundaciones, terremotos, incendios, huracanes, tormentas eléctricas, etcétera.

Clasificación general de las amenazas o ataques inherentes a las redes

En el flujo normal de la información (figura 3.1) no debe existir ningún tipo de obstáculos para que la información llegue al destinatario.

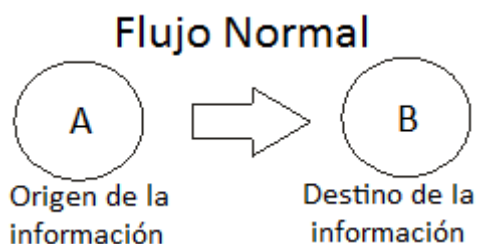


Figura 3.1 Flujo normal de la información

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- a) Interrupción: Un recurso del sistema es destruido o se vuelve no disponible (figura 3.2). Éste es un ataque contra la *disponibilidad*.

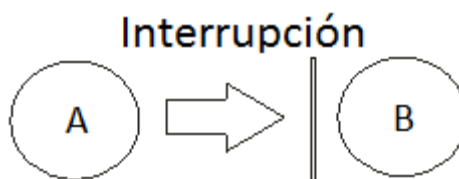


Figura 3.2 Flujo con interrupción

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- b) Intercepción: Una entidad no autorizada consigue acceso a un recurso (figura 3.3). Éste es un ataque contra la *confidencialidad*. La entidad no autorizada podría ser una persona o un programa.

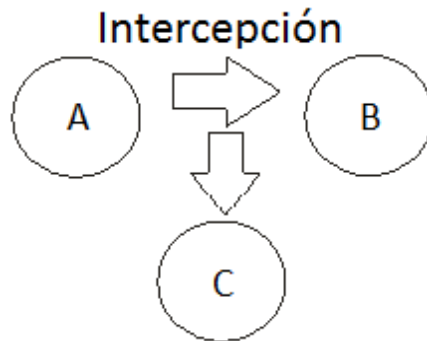


Figura 3.3 Flujo con intercepción

- c) Modificación: Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo (figura 3.4). Éste es un ataque contra la *integridad*.

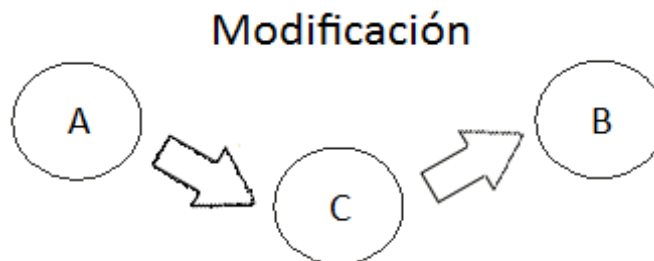


Figura 3.4 Flujo con modificación

- d) Suplantación o Falsificación: Una entidad no autorizada inserta objetos falsificados en el sistema (figura 3.5). Éste es un ataque contra la *autenticidad*.

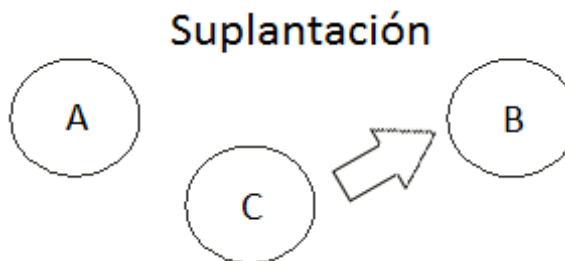


Figura 3.5 Flujo con suplantación

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

3.1.IV ATAQUES³

Un ataque es la realización o culminación de una amenaza. Representa pérdidas totales o parciales, incluso pueden no existir pérdidas. Se lleva a cabo por diferentes tipos de perpetradores y éstos se clasifican con base en su objetivo principal o tipo de ataque realizado. Puede dividirse en dos tipos con base en la acción que ejecuta en el sistema o la información.

1. **Pasivos**: No se modifica la información, el atacante se limita a escuchar, obtener y monitorear la información. Este tipo de ataque es difícil de detectar. Sus principales objetivos son:
 - a) Intercepción de datos.
 - b) Análisis de tráfico.

Además, con los ataques pasivos se obtiene información que puede consistir en:

- a) Obtención del origen y destinatario (cabeceras de los paquetes).
 - b) Control del volumen de tráfico (frecuencia y longitud de mensajes).
 - c) Control de las horas habituales (periodos de actividad).
2. **Activos**: Consiste en modificar y/o denegar el acceso a la información, es decir, un usuario no autorizado dentro de la red no solo accede a la información sino que también la modifica y/o impide el acceso a ésta.

Los ataques activos pueden clasificarse de la siguiente manera:

- a) Enmascaramiento o suplantación de identidad (el intruso se hace pasar por una entidad diferente).
 - b) Réplica o reactuación (retransmisión subsecuente de uno o varios mensajes legítimos).
 - c) Modificación de mensajes (una parte del mensaje real es alterada, retardada o reordenada).

³ Para mayor información véase el apéndice B

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Otra clasificación de los ataques:

a) Ataques de suplantación o contra la autenticación

Su objetivo es engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y contraseña.

b) Ataques de interceptación o contra la confidencialidad

Es el tener acceso a una línea para obtener datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos) o la lectura de las cabeceras de los paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

c) Ataques de interrupción o contra la disponibilidad

Es la destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

d) Ataques de modificación o contra la integridad

Es el cambio de valores en un archivo de datos, alterando un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Todos los ataques (pasivos y activos) se componen de 3 fases principales:

1. Planteamiento o planeación

- a) Objetivo: ¿Qué se quiere lograr?
- b) Observación y búsqueda en diversas fuentes: ¿Cómo se obtiene la información? y ¿qué se tiene que hacer para lograrlo?
- c) ¿A quién o a quiénes se quiere atacar?
- d) Metodología de ataque: ¿Cómo se llevará a cabo el ataque?

2. Activación (en qué tiempo y lugar se llevará a cabo el ataque)

- a) Hora
- b) Día (s)
- c) Acción realizada

Ejemplos: Bombas de tiempo y bombas lógicas (condición).

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

3. Ejecución (una vez que aconteció el ataque)

a) Atacante:

¿Se lograron los objetivos?

¿Qué beneficios se obtuvieron?

b) Atacado:

¿Qué daño se tuvo?

¿Cuáles son las pérdidas (totales o parciales)?

¿Cómo se le hace para que no vuelva a ocurrir de nuevo?

En base a lo anterior, se tiene que un ataque es realizado por un perpetrador o intruso. El perpetrador puede o no tener éxito y si lo tiene, éste puede causar gran o poco impacto. Además, se pueden clasificarse en:

a) Pasivos: Aquellos que solo analizan, observan la información o la escuchan. Lo mismo hacen con los bienes de la organización.

b) Activos: Aquellos que alteran, crean, borran cualquier tipo de activo, principalmente la información, actúan de tal manera que uno se da cuenta de ello.

Por tal razón, para poder entender cómo piensa el intruso se tiene lo siguiente:

Psicología del intruso

Ponerse en los zapatos del atacante para pensar y actuar como él lo haría. El objetivo es colocar las protecciones necesarias para evitar que el ataque ocurra alguna vez o se presente de nuevo.

3.2 SERVICIOS DE SEGURIDAD

Son aquellos que mejoran la seguridad de un sistema de información y el flujo de la información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio, éstos se clasifican de la siguiente manera:

1. Control de acceso

Limita y determina qué usuario o proceso está autorizado para acceder a un recurso o información, puede llevarse a cabo en el origen o en un punto intermedio.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Éstos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

Ejemplos de los privilegios o permisos de una entidad:

- a) Creación o destrucción
- b) Lectura o escritura
- c) Adición, supresión o modificación del contenido
- d) Exportación o importación
- e) Ejecución

Los privilegios o permisos pueden ser revocados y cambiados por el administrador autorizado de la red o del sistema en cuestión.

2. Confidencialidad

Asegura qué personas están autorizadas y tienen acceso a la información o recurso en cuestión. Se divide en:

- a) Confidencialidad de datos: Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación, se puede usar en segmentos seleccionados, porciones o en todos los datos usando un cifrado. Algunos tipos pueden ser:
 - I. Servicios de confidencialidad orientados a conexión. Proporcionan confidencialidad a los datos transmitidos durante su conexión.
 - II. Servicios de confidencialidad no orientados a conexión. Proporcionan confidencialidad de paquetes de datos.
 - III. Servicios de confidencialidad de campo selectivo. Proporcionan confidencialidad de campos específicos de los datos durante una conexión.

- b) Confidencialidad de flujo de tráfico: Proporciona protección a la información que de otra forma podría resultar comprometida u obtenida indirectamente mediante un análisis del tráfico ya que protege la identidad del origen y destino(s) del mensaje al enviar los datos confidenciales a muchos destinos además del verdadero, produce una cantidad de tráfico constante de forma que sea indistinguible para un intruso.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

La desventaja de este método es que incrementa drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

3. Integridad

Evita que los datos sean modificados por usuarios o procesos no autorizados para ello. Garantiza que los datos recibidos coinciden con los datos enviados usando un hash criptográfico con firma. La modificación incluye escritura, cambio, borrado, creación y reenvío de los mensajes transmitidos. Algunos servicios de integridad pueden ser:

- a) Orientados a conexión con recuperación de datos: Proporcionan integridad de los mismos durante una conexión. Si es posible, permiten la recuperación de fallos de integridad.
- b) Orientados a conexión sin recuperación de datos: Proporcionan integridad a los mismos durante una conexión. No se recuperan los fallos de integridad.
- c) Campo seleccionado orientado a conexión: Proporcionan integridad de campos específicos en los datos durante la conexión.
- d) No orientados a conexión: Proporcionan integridad a unidades de datos.
- e) Campo seleccionado no orientados a conexión: Proporcionan integridad de campos específicos dentro de las unidades de datos.

4. Autenticación

Verifica la identidad del usuario o proceso que desea acceder al recurso o a la información. Tiene una correcta identificación del origen del mensaje, asegurando que la entidad no es falsa. La autenticación es usada principalmente por:

- a) Entidad: Asegura la identidad de los participantes en la comunicación mediante biométrica (huellas dactilares, identificación de iris, etcétera.), tarjetas de banda magnética, contraseñas, o procedimientos similares.
- b) Origen de información: Asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

La autenticación es realizada principalmente a través de:

- a) Algo que se sabe: El sistema verifica la información contra la copia que tiene almacenada para determinar si la autenticación es exitosa o no, ejemplo: una contraseña o un número personal de identificación.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- b) Algo que se tiene: Es un elemento dado por el usuario para identificarlo, ejemplo: una tarjeta o un pasaporte.
- c) Algo que se es: Se usan elementos de la persona como la voz, retina, imagen del rostro o una huella digital para identificar de quién se trata y así realizar el proceso de autenticación.

5. No repudio

Es la protección que se ofrece para prevenir a los emisores o a los receptores de negar un mensaje transmitido, proporcionando una prueba ante una tercera parte que le informa a cada una de las entidades que han participado en una comunicación.

Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. Se puede dividir en:

- a) Servicio de no repudio con prueba de origen: Sirve para proporcionar al destinatario una prueba del origen de los datos.
- b) Servicio de no repudio con prueba de destino: Sirve para proporcionar al emisor una prueba de que los datos se han entregado al destinatario.
- c) Servicio de no repudio de presentación: Proveen pruebas de presentación de los datos, con ello protegen contra cualquier intento falso de negar que los datos fueron presentados para él envío.
- d) Servicio de no repudio de transporte: Proveen pruebas del transporte de los datos, con lo que protege contra cualquier intento de negar que los datos fueron transportados.
- e) Servicio de no repudio de recepción: Proveen pruebas de recepción de los datos, con esto se protege al emisor de que el receptor niegue haber recibido el mensaje.

Las *firmas digitales* constituyen el mecanismo más empleado para este fin porque éstas tienen la propiedad de que pueden ser creadas por los firmantes y ser verificadas por otros.

6. Disponibilidad

Posibilidad de acceder a los recursos o a la información requerida cuando sea oportuno o necesario hacerlo, garantizando que todos los recursos vitales son accesibles. Es importante aclarar que la disponibilidad se refiere únicamente al tiempo para obtener la información y no importa si es o no correcta. Al disponer de la información después del momento necesario equivale a la no disponibilidad.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Un caso grave es la *no disponibilidad absoluta* por haberse producido algún desastre y a medida que pasa el tiempo el impacto será mayor hasta convertirse en la *no continuidad de la entidad*.

3.3 POLÍTICAS DE SEGURIDAD

Surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia, sensibilidad de la información y servicios críticos. Éstos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos dentro de la misma, contemplando la seguridad informática.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

Los pasos para redactar una política de seguridad informática son:

- a) Debe ser explícita y comprensible porque es la base para tomar ciertas decisiones.
- b) Seleccionar una filosofía, la cual permite convertir las indicaciones precisas de qué es lo permitido y lo denegado en cierta parte de la operación de la organización:
 - I. Permisiva: Todo se permite excepto lo que esta explícitamente prohibido.
 - II. Prohibitiva: Todo se prohíbe excepto lo que esta explícitamente permitido.
- c) Redactar de manera positiva para evitar la susceptibilidad de las personas.
- d) Asignar responsabilidades, una política establece expectativas y responsabilidades entre el administrador de red, los usuarios y la gerencia; permite a todos saber qué esperar el uno del otro.
- e) Capacitación, ofrece la posibilidad de mejorar la eficiencia del trabajo de la empresa, permitiendo a su vez que la misma se adapte a las nuevas circunstancias que se presentan tanto dentro como fuera de la organización. Proporciona a los

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

empleados la oportunidad de adquirir mayores aptitudes, conocimientos y habilidades que aumentan sus competencias, para desempeñarse con éxito en su puesto.

- f) Evitar hostigamientos (considerar que las personas son humanas).

Al proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, constancia para renovar y actualizar dicha política en función del ambiente dinámico que rodea las organizaciones modernas.

El manual es elaborado tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación y comprometimiento.

Los pasos para realizar una política de seguridad son:

1. Detectar el problema.
2. Identificar qué se debe proteger.
3. Identificar de qué se debe proteger.
4. Identificar los diferentes tipos de usuarios.

Esta situación ha llevado a muchas empresas (con activos muy importantes) que estén expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen la información sensible y por ende su imagen corporativa.

Para solucionar esta situación los encargados de la seguridad deben considerar que las personas entiendan los asuntos importantes de la seguridad, conozcan sus alcances y estén de acuerdo con las decisiones tomadas en relación con esos asuntos.

Para que las políticas de seguridad sean aceptadas deben integrar una estrategia de negocio que incluya la misión y visión con el propósito de que se reconozca quién toma las decisiones, importancia, incidencias en las proyecciones y la utilidad en la empresa.

El contenido de las políticas de seguridad es:

- a) Ámbito de la aplicación.
- b) Análisis de riesgo.
- c) Enunciados de políticas.
- d) Sanciones.
- e) Sección del uso ético de los recursos.
- f) Sección de los procedimientos para el manejo de incidencias.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Más bien es una descripción de lo que se desea proteger y el porqué de ello.

Las principales personas que participan en la elaboración de las políticas de seguridad son:

- a) Administradores.
- b) Personas con autoridad.
- c) Representante jurídico.
- d) Editor/redactor.
- e) Usuario típico.

Se debe formar un equipo multidisciplinario que represente gran parte de los aspectos culturales y técnicos de la organización para establecer un comité que será formado por los responsables de cada área para elaborar las actividades referentes a la creación y aprobación de nuevas normas de seguridad en la organización.

Es responsabilidad del supervisor de seguridad informática, someter a revisión y divulgar en los medios de difusión (sitio web oficial, email, revista interna, etcétera.) los procedimientos de seguridad. El supervisor inmediato es responsable de capacitar a sus empleados en lo relacionado con los procedimientos de seguridad.

Las características principales de las políticas de seguridad son:

- a) Es un documento con vigencia permanente y actualizable periódicamente.
- b) Modelo de referencia para otros esquemas de seguridad.
- c) Enfocados a la problemática particular de cada institución.
- d) Tener una estructura bien definida.
- e) Aceptada como un documento oficial por las autoridades y la comunidad.
- f) Clara, exacta, precisa y concisa.
- g) Establece condiciones aceptables y no aceptables.
- h) Accesible a toda la comunidad.
- i) Aprobada por todas las personas que pueden ser afectadas.
- j) Establece obligaciones y derechos de los administradores y usuarios.

Es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la empresa, en ellas deben responder a intereses y necesidades empresariales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la empresa.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD **INFORMÁTICA**

3.4 MECANISMOS DE SEGURIDAD

Son técnicas que se utilizan para implementar un servicio están diseñados para detectar, prevenir o recobrase de un ataque de seguridad debido a que implementan varios servicios básicos de seguridad o combinaciones de estos.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar varios servicios de seguridad, los cuales poseen tres componentes diferentes:

- a) Información secreta: Claves y contraseñas, conocidas por las entidades autorizadas.
- b) Conjunto de algoritmos: Lleva a cabo el cifrado, descifrado y generación de números aleatorios.
- c) Conjunto de procedimientos: Definen como se usarán los algoritmos, quién envía qué, a quién y cuándo.

No existe un único mecanismo capaz de proveer todos los servicios, pero la mayoría de ellos hace uso de técnicas criptográficas basadas en el cifrado de la información. Los mecanismos pueden ser clasificados como preventivos, detectivos y recuperables.

Los mecanismos de seguridad pueden clasificarse en dos categorías:

1. Mecanismos de seguridad generalizados: Se relacionan con los niveles y manejo de seguridad requeridos. Se aplican a los sistemas para cumplir la política general de seguridad de la organización, a continuación se explica cada uno de ellos.
 - a) Funcionalidad de confianza: Se utiliza para extender los otros mecanismos de seguridad o para establecer su efectividad. Cualquier tipo de funcionalidad que proporcione directamente mecanismos de seguridad o el acceso a los mismos debe ser de confianza.
 - b) Etiquetas de seguridad: Están asociados a los recursos del sistema. A menudo es necesario que los datos de tránsito lleven una etiqueta de seguridad apropiada. Un nivel de seguridad puede implicar datos adicionales que se asocian a los datos transmitidos o puede ser implícito.
 - c) Detección de eventos: Detecta violaciones aparentes de la seguridad.
 - d) Seguimiento de auditorías de seguridad: Consiste en la revisión y examen independiente de los registros y las actividades del sistema para probar la operatividad de los controles, asegurar el cumplimiento de las políticas, procedimientos operacionales establecidos, recomendar los cambios adecuados en el control, políticas y procedimientos.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD

INFORMÁTICA

- e) Recuperación de seguridad: Trata con solicitudes de mecanismos como administradores de eventos y funciones de administración, realiza acciones de recuperación resultado de la aplicación de una serie de reglas.
2. Mecanismos de seguridad específicos: Definen la implementación de los servicios concretos, los cuales se enlistan a continuación.
- a) Cifrado: Se utiliza para proteger la confidencialidad de las unidades de los datos y la información del flujo de tráfico o para dar soporte y complementar otros mecanismos de seguridad.
- b) Firma digital: Hace referencia al cifrado, por medio de la clave secreta del emisor de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor para verificar su integridad. Juega un papel esencial en el servicio de no repudio.
- c) Control de acceso: Solo los usuarios autorizados pueden acceder a los recursos del sistema o a la red, por ejemplo las contraseñas de acceso.
- d) Integridad de datos: Asegura que los datos no sean alterados o destruidos. Este mecanismo trata con la integridad de una unidad o campo de datos simples y la integridad de una secuencia de unidades o campos de datos.
- e) Intercambio de autenticación: Verifica la supuesta identidad de los usuarios. En la ITU X.509 (ITU, 1987) se dice que un mecanismo de intercambio de autenticación es fuerte si se basa en el uso de técnicas criptográficas para proteger los mensajes que se van a intercambiar.
- f) Tráfico de relleno: Protege contra el ataque de análisis de tráfico. Mediante la generación de ejercicios de comunicación no autenticada, unidades de datos y datos ilegítimos. El objetivo no es revelar si los datos que se están transmitiendo representan y codifican realmente información. En consecuencia estos mecanismos únicamente serán efectivos si son protegidos por un servicio de confidencialidad de datos.
- g) Control de ruteo: Permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.
- h) Certificación: Se emplea para asegurarse que ciertas propiedades de los datos que se comunican entre dos o más entidades, como su integridad, origen, tiempo o destino. La certificación la realiza una tercera entidad de confianza, que es la que da testimonio de la autenticidad.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

3.5 SEGURIDAD FÍSICA⁴

Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Haciendo referencia a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Es uno de los aspectos que casi no se toman en cuenta a la hora de diseñar un sistema informático. Esto deriva que para un atacante es más fácil hacer una entrada ilegal de manera interna a la empresa haciendo una copia de la información que desee robar que intentar acceder de manera lógica a la misma.

Es muy importante concientizar que por más que la empresa sea la más segura desde el punto de vista de ataques externos. La seguridad de la misma será nula si no se ha previsto cómo combatir los principales desastres.

Principales Desastres

Cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como de la naturaleza en donde se encuentra ubicado el centro de cómputo.

En muchas de las ocasiones solo basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno, además de que estas soluciones son económicas y tienen la misma efectividad que si se invirtieran millones de pesos en la seguridad física del edificio.

Los principales factores a contemplar al momento de diseñar un centro de cómputo son:

- a) Evitar el uso de materiales combustibles o inflamables en todo el lugar, incluyendo muebles, piso, paredes y techo.
- b) Impermeabilizar el perímetro del lugar, incluyendo las puertas de acceso.
- c) Instalar mecanismos de ventilación con control de temperatura y humedad así como detectores de incendios y sistemas de extinción de los mismos.
- d) Establecer controles de acceso físico al sistema de detección de intrusos y alarmas.
- e) Implantar mecanismos de duplicación de la información y backups remotos.

⁴ Para mayor información véase el apéndice B

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Ventajas

Al evaluar y controlar permanentemente la seguridad física del edificio se comienza a integrar la seguridad como una función primordial dentro de cualquier organismo, así también se deberá contar con un plan de seguridad integral.

El tener controlado el ambiente y acceso físico permite:

- a) Disminuir siniestros.
- b) Trabajar mejor manteniendo la sensación de seguridad.
- c) Descartar falsas hipótesis si se produjeran incidentes.
- d) Tener los medios para luchar contra accidentes.
- e) Al tener una instalación adecuada, ésta considera los detectores de humo, extinguidores automáticos de incendios y sistemas de alarmas.
- f) Prevenir el acceso de personas no autorizadas.
- g) Al contar con un control del acceso a las computadoras, éstas estarán protegidas para que ninguna persona pueda robar, dañar los datos o el equipo.
- h) Se pueden minimizar y controlar los errores dentro de las compañías siempre y cuando tengan una buena estrategia de control de información, en la cual se evalúen los riesgos que los accidentes o errores pueden representar, así como contar con equipos de seguridad en sistemas y redes capaces de mantener la administración de identidades como parte de la estrategia.

Desventajas

- a) Los equipos informáticos son muy sensibles al calor, fuego y humo.
- b) El polvo es abrasivo y acorta la vida útil de los medios magnéticos y de las unidades ópticas y de cintas.
- c) Si se acumula mucho polvo en los sistemas de ventilación puede bloquear el flujo de aire impidiendo que éste les llegue a los equipos y puedan calentarse o sufrir fallas.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

3.6 SEGURIDAD LÓGICA

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos para salvaguardar la integridad de la información almacenada en una computadora y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta que *todo lo que no está permitido debe estar prohibido* y esto es lo que debe asegurar la seguridad lógica.

Involucra todas aquellas medidas establecidas por la administración (usuarios y administradores de recursos de tecnología de la información) para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

Los objetivos que se plantea son:

- a) Restringir el acceso a los programas y archivos.
- b) Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- c) Asegurar que se estén utilizando los datos, archivos y programas correctos en cada procedimiento.
- d) La información transmitida debe ser recibida solo por el destinatario al cual ha sido enviada y no a otro.
- e) La información recibida sea la misma que ha sido transmitida.
- f) Deben existir sistemas alternativos secundarios de transmisión entre diferentes puntos.

La falta de seguridad lógica o su violación puede traer las siguientes consecuencias a la organización:

- a) Cambio de los datos antes o cuando se le da entrada a la computadora.
- b) Copias de programas y /o información.
- c) Código oculto en un programa
- d) Entrada de virus

La seguridad lógica puede evitar una afectación de pérdida de registros y ayuda a conocer el momento en que se produce un cambio o fraude en los sistemas.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

El sistema integral de seguridad debe comprender:

- a) Elementos administrativos.
- b) Definición de una política de seguridad.
- c) Organización y división de responsabilidades.

Además, existen diferentes tipos de usuarios con ciertas responsabilidades, los cuales son:

- a) Propietario: Es el dueño responsable de la información, de la seguridad lógica, en cuanto a que puede realizar cualquier acción y autorizar a otros usuarios de acuerdo con el nivel que desee darles.
- b) Administrador: Solo puede actualizar o modificar el software con la debida autorización, pero no puede modificar la información. Es responsable de la seguridad lógica y de la integridad de los datos.
- c) Usuario principal: Está autorizado por el propietario para hacer modificaciones, cambios, lectura y utilización de los datos, pero no puede dar autorización para que otros usuarios entren.
- d) Usuario de explotación: Puede leer la información y utilizarla para explotarla haciendo reportes de diferente índole.
- e) Usuario de auditoría: Puede utilizar la información y rastrearla dentro del sistema con fines de auditoría.

Un método eficaz para proteger un sistema de computación es usar un software de control de acceso, este programa protege contra el acceso no autorizado, pues se pide al usuario una contraseña antes de permitirle el acceso a la información confidencial.

Al respecto, el NIST (National Institute for Standards and Technology, Instituto Nacional de Estándares y Tecnología) ha resumido los siguientes estándares de seguridad que se refiere a los requisitos mínimos de seguridad en cualquier sistema:

- a) *Identificación y autenticación.*

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina identificación al momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esta identificación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina single login o sincronización de contraseñas.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

b) *Roles.*

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

c) *Transacciones.*

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

d) *Limitaciones a los servicios.*

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para un cierto número de personas, en donde exista un control a nivel sistema que no permita la utilización del producto a otro usuario más que el permitido.

e) *Modalidad de acceso.*

Se refiere a los permisos concedidos al usuario sobre los recursos y a la información cuando accede a estos. Esta modalidad puede ser:

1. Lectura: Puede únicamente leer o visualizar la información pero no puede alterarla.
2. Escritura: Permite agregar, modificar o borrar información.
3. Ejecución: Otorga el privilegio de ejecutar programas.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

4. Borrado: Permite eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
5. Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

1. Creación: Permite crear nuevos archivos, registros o campos.
2. Búsqueda: Permite listar los archivos de un directorio determinado.

f) Ubicación y horario.

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso. Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

g) Control de acceso interno.

Determinan lo que un usuario (o grupo de usuarios) puede o no hacer con los recursos del sistema. Algunos métodos de control de acceso interno son:

1. Contraseñas (palabras claves): Generalmente se utilizan para realizar la autenticación del usuario, proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo.
2. ACL (Access Control List, Listas de Control de Acceso): Son condiciones que dan permisos o denegaciones que se aplican a direcciones IP o a los protocolos de la capa superior. Estas condiciones de la lista de acceso se utilizan para implementar las reglas de filtrado de paquetes.
3. Cifrado: La información encriptada solamente puede ser descifrada por quien posea la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado en el capítulo 4 *MÉTODO DE CIFRADO Y PROCESOS DE CONEXIÓN*.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

h) Control de acceso externo.

Es una protección contra la interacción del sistema propio con los servicios y gente externa a la organización. Los sistemas de control de acceso externo se dividen en 7 partes, donde cada una se encarga de una zona diferente, los cuales son:

1. Dispositivos de control de puertos: Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.
2. Firewalls o puertas de seguridad: Es un mecanismo de filtrado avanzado que protege la confidencialidad e integridad de la información al proteger una red de otra en la que no se tiene confianza.
3. Proxy: Es una aplicación o un dispositivo de hardware que está entre una red confiable y una no confiable, es el encargado de realizar la conexión.
4. Integridad del sistema: Es un mecanismo que almacena en una base de datos los hashes de archivos del sistema a monitorear con el fin de garantizar la integridad de los mismos.
5. VPN (Virtual Private Networks, Red Privada virtual): Es una tecnología que permite la conexión virtual segura entre puntos remotos cuya localización geográfica impide que la red local sea física.
6. DMZ (DeMilitarized Zone, Zona desmilitarizada): Es un área insegura entre áreas seguras. Hace referencia a una pequeña red que contiene servicios públicos conectados directamente a una protección ofrecida por un firewall o cualquier dispositivo de filtrado.
7. Herramientas de Seguridad: Son programas que permiten mantener a salvo la computadora de cualquier intruso.

i) Administración.

Una vez establecidos los controles de acceso sobre los sistemas de aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolla respecto a la seguridad lógica debe guiar las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de los perfiles de usuarios.

Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD

INFORMÁTICA

En este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

3.7 HERRAMIENTAS DE MONITOREO⁵

Al monitorear una red existen varios mecanismos preventivos y de control para detectar y solucionar diversos problemas como la disponibilidad a tiempo real de cualquier nodo. Esto permite agregar múltiples servidores o dispositivos para que sean monitoreados continuamente y así obtener el estatus a tiempo real de la disponibilidad de todos ellos; así, esto no solo se limita a monitorear los dispositivos de red sino también puede ser utilizado para monitorear cualquier servidor, sitio web o aplicación web.

Las herramientas que más se usan en el monitoreo de redes tienen distintos aspectos que dependen de los objetivos que se quieran obtener, una u otra herramienta podrá resultar más idónea en correspondencia a su funcionamiento y preferencias del administrador. Estas herramientas se dividen en dos:

- a) Control y seguimiento de acceso: Esta herramienta permite obtener información por medio de todos los intentos de conexión que se produzcan en el sistema o sobre otro que se indique, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP. Además, permite tener control sobre todos los paquetes que entran por la interfaz de red a la máquina por la conexión IP (TCP y UDP) e ICMP, analiza paquetes a nivel de aplicaciones (TELNET, FTP, SMTP), se puede utilizar junto con otras aplicaciones que permiten definir desde qué máquinas se hacen ciertas conexiones y de cuáles se prohíben. El programa se puede instalar en una computadora cuya interfaz de red funcione en modo promiscuo, así permitirá ir seleccionando las direcciones IP o la máquina a la que se le quiera hacer una auditoría. También ofrece protección ante posibles ataques aunque la computadora pueda ser utilizada para intentar comprometer el sistema, se puede dar seguimiento al ataque en la red cuando se sospeche que alguna de las máquinas ha sido comprometida.

- b) Integridad del sistema: Se ocupa de la seguridad del sistema al verificar que los archivos y programas ya instalados tengan el mismo tamaño en bytes, si no se

⁵ Para mayor información véase el apéndice C

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

mantienen se crea una alerta de modificación y se verifica que no se haya instalado un programa sospechoso que pueda estar ejecutándose en la máquina de forma oculta, al detectar la posible penetración al sistema se pueden determinar los alcances de los posibles daños.

Las características principales del monitoreo de red son:

- a) Monitorea la disponibilidad y el tiempo de respuesta de los servidores críticos.
- b) Envía emails para notificar anomalías.
- c) Soporta la configuración de email para diferentes severidades de las alertas.
- d) Mantiene el historial de alertas.

Se debe tomar en cuenta que al monitorear una red en tiempo real la herramienta provee el estatus actual de las aplicaciones, dispositivos y sitios web que pueden ir generando alertas cuando el tiempo de respuesta excede el límite del umbral definido o cuando el dispositivo no responde. El administrador define el límite del umbral para cada dispositivo a monitorear de manera individual o global así como el tipo de alerta. Para monitorear exitosamente la red se tiene que configurar el software de modo que supervise los signos vitales de la red que son:

- a) **Disponibilidad**: Comprueba si los servicios ofrecidos están en funcionamiento, si los usuarios internos como externos pueden acceder a ellos. Incluye el monitoreo de páginas web, servidores de correo electrónico y conexiones de Internet.
- b) **Velocidad**: Evita que las páginas web y los servicios de red tarden mucho tiempo en cargar debido a páginas, archivos o imágenes muy grandes.
- c) **Actividad**: Sirve para evaluar las cargas que los equipos de red tienen que sostener y para ver las tendencias de utilización.

Al instalar y configurar la herramienta de red se puede observar y obtener:

1. Control de desempeño

- a) Revisar los signos vitales de la red en tiempo real.
- b) Analizar y dar soporte a las demandas de nuevas aplicaciones (voz sobre IP (VoIP)).
- c) Determinar las tendencias de la red para cubrir las necesidades de incremento, la capacidad de los equipos de manera planeada y con herramientas de modelaje.
- d) Obtener mayor eficiencia de la red sin necesidad de aumentar el ancho de banda o de sus servidores.

CAPÍTULO 3 INTRODUCCIÓN A LA SEGURIDAD

INFORMÁTICA

2. Control de múltiples instalaciones

- a) Administra y controla redes remotas las 24 horas del día en los 7 días de la semana, usa hardware o software sin necesidad de realizar gastos ostentosos de viaje.
- b) Reporta simultáneamente a múltiples consolas el estado de la red.
- c) Integra la administración de redes con los estándares de monitoreo RMON (The Remote Network Monitoring, Monitoreo de red remoto) 1 y 2 y reporte HCRMON.
- d) Monitorea múltiples redes simultáneamente desde una consola.

3. Control de solución de problemas

- a) Aísla y responde a los asuntos que se presenten de manera rápida con un análisis unificado.
- b) Resuelve los problemas que se presenten tanto en las redes locales como en las remotas las 24 horas del día y los 7 días de la semana.
- c) Administra la configuración de dispositivos locales y remotos con toda la funcionalidad de SNMP.

4. Control de información

- a) Conserva y almacena datos de la red para manejar los reportes y tendencias.
- b) Observa y analiza la red así como el tráfico a través del tiempo.
- c) Monitorea el estado de la red en comparación a los reportes de análisis.
- d) Genera reportes sustentados para justificar las necesidades de actualización de la red.

Las herramientas de monitoreo de red contemplan todos los tipos de topologías de red y los medios de transmisión que pueden ser aéreos o terrestres. Un excelente programa para monitorear redes debe ser fácil de instalar y usar. Además que debe contar con las siguientes funcionalidades:

- a) Administración remota a través de navegador web, dispositivos móviles y aplicaciones.
- b) Notificaciones sobre fallos a través de correo electrónico, mensajería instantánea, SMS, etc.
- c) Amplia selección de sensores.
- d) Posibilidad de monitorear varios sitios con una sola instalación.
- e) Soporte de todos los métodos comunes de adquisición de datos de utilización (SNMP, sniffer de paquetes, NetFlow, sFlow, jFlow).

CAPÍTULO 4

MÉTODO DE CIFRADO



Un método de cifrado se entiende como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave.

Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los equipos. El uso del cifrado de datos puede iniciarse en el equipo o en el servidor al que se requiere conectar.

La criptografía hace varios años dejó de ser un arte y se convirtió en una técnica que trata de proteger la información. Las ciencias más usadas son: teoría de la información, matemáticas discretas, teoría de los grandes números y la complejidad algorítmica. Dichas ciencias se encargan de transformar un mensaje inteligible en otro que no lo es usando una clave que solo el emisor y el destinatario conocen, para que después puedan devolverlo a su forma original, sin que nadie vea el mensaje cifrado o sea capaz de entenderlo.

La importancia de la criptografía radica en que es el único método capaz de tener seguridad en la rama de la informática ya que mantiene la privacidad, integridad, autenticidad y el no repudio que se relaciona con el no poder negar la autoría y recepción de un mensaje enviado. Además, necesita también de la arquitectura cliente-servidor para poder establecer una conexión entre el emisor del mensaje encriptado y el destinatario a recibirlo.

4.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

Los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos informáticos y las calculadoras.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la web. Las transacciones que se realizan a través de la red pueden ser interceptadas porque actualmente resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse; por lo tanto, la criptografía tiene un papel muy importante.

4.1.1 CRIPTOLOGÍA

Del griego *kriptós* (ocultar) y *logos* (tratado) es la ciencia genérica encargada del ocultamiento de la información y que incorpora a la criptografía y al criptoanálisis.

La criptología tiene por objetivo esconder la información contenida en ciertos datos, así como transformarla por motivos de seguridad para que no se pueda identificar al propietario de los datos, al autor, el remitente de un mensaje, etcétera.

En ocasiones se emplean los verbos encriptar y cifrar como sinónimos, al igual que sus respectivas contrapartes, desencriptar y descifrar. No obstante, lo correcto es utilizar el término cifrar en lugar de encriptar, ya que se trata de un anglicismo sin reconocimiento académico, proveniente del término *encrypt*. Por otra parte, tampoco debe emplearse codificar en lugar de cifrar, puesto que el primero designa la emisión de un mensaje mediante algún código, mas no necesariamente tiene que ser oculto, secreto o indescifrable. Escribir en cualquier idioma implica el uso de un código, que será comprensible para los receptores que conozcan dicho código, pero no para otros individuos.

En tiempos recientes, el interés por la criptología se ha extendido a otras aplicaciones aparte de la comunicación segura de la información, actualmente uno de los usos de las técnicas y métodos estudiados por la criptología es la autenticación de información digital (también llamada firma digital).

Para cifrar los datos se utiliza un algoritmo, al cual se le puede considerar como una función matemática. Por lo tanto, un algoritmo de cifrado es una fórmula para desordenar la información de manera que ésta se transforme en dato incomprensible, usando un código o clave (en ocasiones, más de una).

Los mensajes que se tienen que proteger (texto en claro o texto plano), se transforman mediante esta función y a la salida del proceso de usar la clave se obtiene el texto cifrado o criptograma.

En muchos casos existe un algoritmo de descifrado encargado de reordenar la información y volverla inteligible, pero no siempre es así. Cuando existen ambas funciones, una para cifrar y otra para descifrar, se dice que el sistema criptográfico es de dos vías o reversible (a partir de un mensaje en claro se puede obtener uno cifrado y a partir de éste se puede obtener el mensaje original), si no existe una función para descifrar, se dice que el sistema es de una sola vía (a partir de un mensaje cifrado no es posible obtener el mensaje en claro que lo generó; una aplicación es el almacenamiento de contraseñas).

La transformación de datos provee una posible solución a dos de los problemas más importantes de la seguridad en el manejo de datos: el problema de la privacidad y el de la autenticación, evitando que personas no autorizadas puedan extraer información del canal de comunicación o modificar estos mensajes.

Desde el contexto histórico, los métodos de cifrado se han dividido en dos categorías:

1. Cifradores de sustitución

- a) Cada letra o grupo de letras se reemplaza por otra letra o grupo de letras para disfrazarlas.
- b) Preservan el orden de los símbolos del texto en claro pero los disfrazan.
- c) Se tiene de ejemplo el antiguo cifrador del César, atribuido a Julio César. En este método, A se representa con D, B con E, C con F y así cada letra se reemplaza por la que se encuentra tres lugares delante de ella, considerando que luego de la Z vuelve a comenzar por la A. Una variante de este método es permitir que el alfabeto cifrado se pueda desplazar k letras (no solo 3), convirtiéndose k en la clave.

2. Cifradores de transposición

- a) Reordenan las letras pero no las disfrazan.
- b) Consiste en una tabla con determinado número de columnas; este número de columnas estará dado por la cantidad de caracteres de la clave, que a su vez no tendrá ningún carácter repetido.
- c) La clave tiene el propósito de numerar las columnas, correspondiendo el número 1 a la primera letra en orden alfabético. El texto en claro se escribe en las filas de la tabla de arriba hacia abajo y el texto codificado será leído verticalmente comenzando por la columna 1, luego la 2, etcétera.

4.1.II **CRIPTOANÁLISIS**

Es la disciplina encargada del estudio de los métodos para romper los mecanismos de cifrado. Típicamente, esto se traduce en conseguir la clave secreta. También es la ciencia opuesta a la criptografía ya que si ésta trata principalmente de crear y analizar criptosistemas seguros, la primera intenta romper esos sistemas, demostrando su vulnerabilidad (tratar de descifrar los criptogramas).

Para establecer las posibles debilidades de un sistema de cifrado, se han de asumir las denominadas condiciones del peor caso: (1) el criptoanalista tiene acceso completo al algoritmo de encriptación, (2) el criptoanalista tiene una cantidad considerable de texto cifrado, y (3) el criptoanalista conoce el texto en claro de parte de ese texto cifrado. También se asume generalmente el Principio de Kerckhoffs, que establece que la seguridad del cifrado ha de residir exclusivamente en el secreto de la clave y no en el mecanismo de cifrado.

Aunque para validar la robustez de un criptosistema normalmente se suponen todas las condiciones del peor caso, existen ataques más específicos en los que no se cumplen todas estas condiciones. Cuando el método de ataque consiste simplemente en probar todas y cada una de las posibles claves del espacio de claves hasta encontrar la correcta, se encuentra ante un ataque de fuerza bruta o ataque exhaustivo. Si el atacante conoce el algoritmo de cifrado y solo tiene acceso al criptograma, se plantea un ataque solo al criptograma; un caso más favorable para el criptoanalista se produce cuando el ataque cumple todas las condiciones del peor caso; en este caso, el criptoanálisis se denomina de texto en claro conocido.

Si además el atacante puede cifrar una cantidad indeterminada de texto en claro, al ataque se le denomina de texto en claro escogido; éste es el caso habitual de los ataques contra el sistema de verificación de usuarios utilizado por Unix, donde un intruso consigue la tabla de contraseñas (generalmente /etc/passwd) y se limita a realizar cifrados de textos en claro de su elección y a comparar los resultados con las claves cifradas (a este ataque también se le llama de diccionario, debido a que el atacante suele utilizar un archivo *diccionario* con los textos en claro que va a utilizar).

El caso más favorable para un analista se produce cuando puede obtener el texto en claro correspondiente a criptogramas de su elección; en este caso el ataque se denomina de texto cifrado escogido.

Cualquier algoritmo de cifrado, para ser considerado seguro, ha de soportar cualquier ataque; sin embargo, en la criptografía, como en cualquier otro aspecto de la seguridad informática, no se debe olvidar un factor muy importante que son las personas. El sistema más robusto caerá fácilmente si se tortura al emisor o al receptor hasta que revelen el contenido del mensaje o si se le ofrece a uno de ellos una gran cantidad de dinero; este tipo de ataques (sobornos, amenazas, extorsión, tortura, etcétera.) se consideran siempre los más efectivos.

4.1.III CRIPTOGRAFÍA

Del griego kriptós (oculto) y graphé (escritura); ciencia encargada de encubrir y ocultar información. Trata del enmascaramiento de la comunicación de modo que solo resulte inteligible para la persona que posee la clave o método para averiguar el mensaje oculto.

Los sistemas capaces de transformar la información para ocultarla y salvaguardarla mediante el cifrado y descifrado de datos se denominan criptosistemas o sistemas criptográficos (véase la figura 4.1), sus elementos son:

- a) Texto plano o Mensaje en claro (Mcla): Información privada a resguardar.
- b) Clave o llave (k): Cadena o serie de signos que pueden ser de carácter alfanumérico conocidos solamente por el emisor y receptor para resguardar la información.
- c) Algoritmo de cifrado (C): Conjunto finito y ordenado de operaciones que combina la clave (k) con la información (Mcla) a fin de ocultarla y protegerla.

- d) Mensaje cifrado o criptograma (Crip): Es el resultado que se obtiene al procesar el texto plano con la clave mediante el algoritmo de cifrado.
- e) Algoritmo de descifrado (D): Conjunto finito y ordenado de operaciones que combina la clave (k) con el criptograma (Crip) a fin de recuperar de manera lícita la información resguardada.

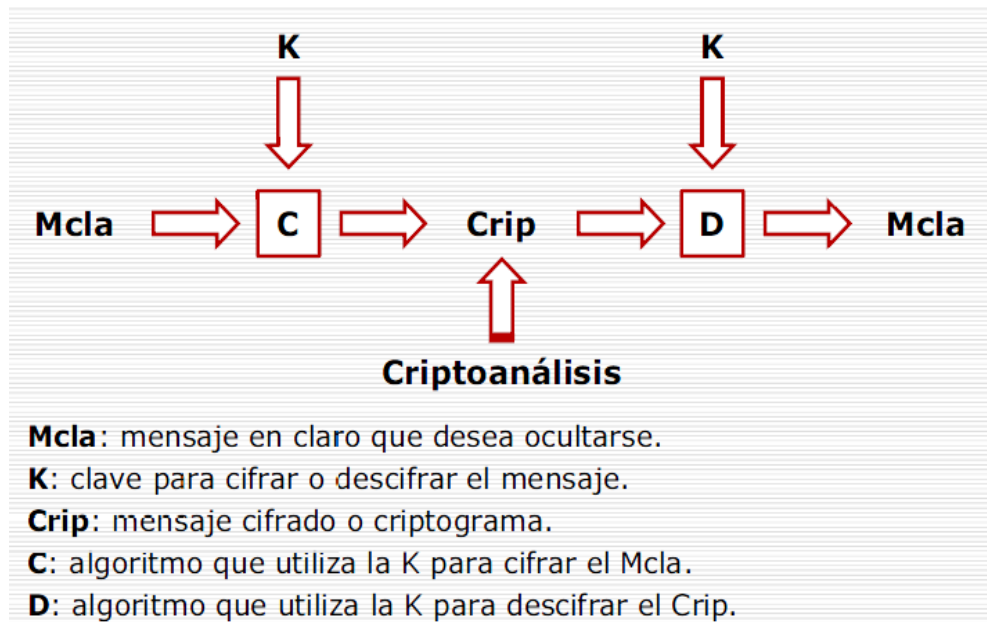


Figura 4.1 Sistema criptográfico o criptosistema

Principio de Kerckhoffs

Establece que la seguridad del cifrado ha de residir exclusivamente en el secreto de la clave y no en el mecanismo de cifrado.

Los seis principios de Kerckhoffs relativos a las propiedades deseables de un sistema criptográfico son:

1. No debe exigirse que sea secreto el diseño de un sistema criptográfico y no debe representar ningún problema el que éste sea conocido por el enemigo.
2. La clave debe ser fácilmente recordada, fácil de ser modificada, pero difícil de adivinar.
3. Debe ser aplicable en los sistemas de comunicación; así, el criptograma puede ser fácil de obtener, pero imposible de describir.

4. Los dispositivos y archivos criptográficos deben ser portables y operables por una sola persona.
5. Los criptogramas deberán dar resultados alfanuméricos y que el sistema sea fácil de usar.
6. El sistema debe ser fácil de utilizar.

Aplicaciones de la criptografía

La criptografía es una disciplina con multitud de aplicaciones, muchas de las cuales están en uso hoy en día. Entre las más importantes se destacan los siguientes:

- a) Seguridad de las comunicaciones: Permite establecer canales seguros sobre redes que no lo son. Con la potencia del cálculo actual y empleando algoritmos de cifrado simétrico (que se intercambian usando algoritmos de clave pública), se consigue la privacidad sin perder velocidad en la transferencia.
- b) Identificación y autenticación: Gracias al uso de la firma digital y otras técnicas criptográficas es posible identificar a un individuo o validar el acceso a un recurso en un entorno de red con más garantías que con los sistemas de usuario y clave tradicionales.
- c) Certificación: Es un esquema mediante el cual agentes fiables (como una entidad certificadora) validan la identidad de agentes desconocidos (como usuarios reales). El sistema de certificación es la extensión lógica del uso de la criptografía para identificar y autenticar cuando se usa a gran escala.
- d) Comercio electrónico: Gracias al uso de canales seguros y a los mecanismos de identificación se posibilita el comercio electrónico, ya que tanto las empresas como los usuarios tienen garantías de que las operaciones no pueden ser espiadas, reduciéndose el riesgo de fraudes, timos y robos además de diferentes tipos de estafas.

4.2 ALGORITMOS DE CRIPTOGRAFÍA

Actualmente la criptografía se puede entender como el conjunto de técnicas que resuelven los siguientes problemas de la seguridad informática: la autenticidad, integridad, confidencialidad y el no repudio. Desde este punto de vista, la criptografía se divide en dos grandes ramas: la criptografía simétrica y la asimétrica. Esencialmente, con la primera se resuelven los problemas de confidencialidad e integridad, mientras que con la segunda se resuelven los de autenticidad y no repudio.

Dependiendo del número de claves que se utilicen para llevar a cabo el proceso de cifrado así como las características de las claves que se empleen, se determinará el tipo de transformación que se llevará a cabo; así, una clasificación con base en las claves utilizadas es la que se presenta a continuación y que se divide en dos grandes grupos: los algoritmos simétricos (clave secreta) y los algoritmos asimétricos (clave pública).

4.2.1 SIMÉTRICOS

Los algoritmos simétricos se refieren al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que se llama clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía se conoce también como criptografía de clave privada o criptografía de llave privada (figura 4.2).

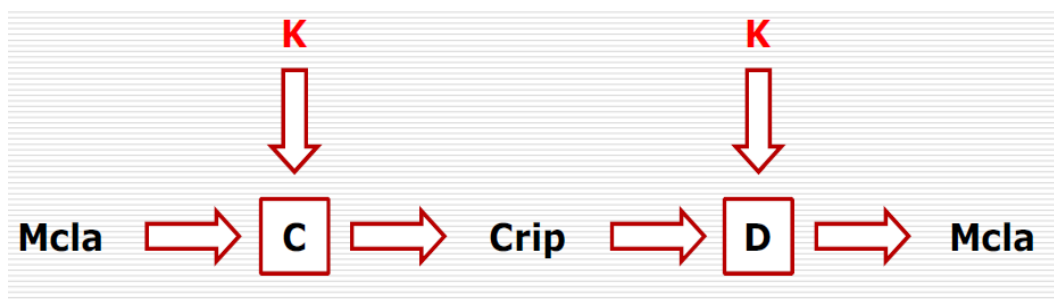


Figura 4.2 Algoritmo simétrico. Hacen uso de la misma clave, tanto para cifrar como para descifrar. La clave debe ser celosamente guardada por los participantes de la comunicación.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir con algunos requisitos básicos:

1. Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
2. Conocido el texto en claro y el texto cifrado debe resultar más caro en tiempo o en dinero descifrar la clave.

Existe una clasificación de este tipo de criptografía que se divide en tres familias: la criptografía simétrica de bloques o cifradores de bloques (block cipher), la criptografía simétrica de lluvia o cifradores de flujo (stream cipher) y la criptografía simétrica de resumen (hash functions, funciones hash). A continuación se describe cada uno:

1. Los cifradores de bloques: Se llaman así porque el mensaje es cifrado agrupando o formando bloques de datos del mensaje original, de manera que se van cifrando uno a uno los bloques de datos de tamaño constante, según lo estipulado por el algoritmo y utilizando para ello una clave del mismo tamaño del bloque. Un ejemplo es el DES (Data Encryption Standard, Estándar de cifrado de datos) que actualmente usa una versión más robusta denominada Triple-Des (consistente en aplicar tres veces DES).
2. Los cifradores de flujo: Se denominan así porque cifran bit por bit o byte por byte, la transformación se aplica sobre cada carácter del mensaje original, entre los más conocidos se encuentran el RC4 y el Seal.
3. Las funciones hash: Las más usadas son MD5, SHA-1 y RIPEMD-160.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, los principales algoritmos son: DES (Digital Encryption Standard), 3DES (Triple DES), IDEA (International Data Encryption Algorithm, algoritmo internacional de cifrado de datos) y el AES (Advanced Encryption Standard, Estándar de cifrado avanzado).

La gran ventaja de este tipo de algoritmos es que han sido implementados en diferentes dispositivos, manuales, mecánicos, eléctricos y hasta algoritmos actuales que son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar, de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Las principales desventajas de ellos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

Los principales algoritmos simétricos son:

1. DES (Data Encryption Standard, Estándar de cifrado de datos)

DES (Data Encryption Standard) es un esquema de cifrado simétrico desarrollado en 1977 por IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de datos. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de Estados Unidos.

DES se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), posteriormente será sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para el cifrado, mientras que los 8 restantes son de paridad y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, es posible tener un total de $2^{56} = 72,057,594,037,927,936$ claves posibles, es decir, unos 72,000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

Un aspecto fundamental que eleva considerablemente su robustez es que en cada vuelta los parámetros de la función de cifrado dependen tanto de los bloques de datos como de las claves, actuales y previos.

Las partes principales del algoritmo son las siguientes:

- a) Fraccionamiento del texto en bloques de 64 bits (8 bytes)
- b) Permutación inicial de los bloques
- c) Partición de los bloques en dos partes: izquierda y derecha, denominadas I y D respectivamente
- d) Fases de permutación y de sustitución repetidas 16 veces (denominadas rondas)
- e) Reconexión de las partes izquierda y derecha, seguida de la permutación inicial inversa

El proceso inicia con una permutación que es fija, enseguida agrupa los datos en dos bloques (izquierdo y derecho) y realiza un proceso de cifrado que consiste en una operación modular con una transformación (solamente con el bloque izquierdo) que se repite 16 veces y en cada vuelta al concluir la operación se intercambian izquierdo y derecho de manera que se procesan alternadamente (figura 4.3). Finalmente, en la vuelta 16 no se realiza el intercambio de bloques y se concluye con una permutación final (la inversa de la inicial).

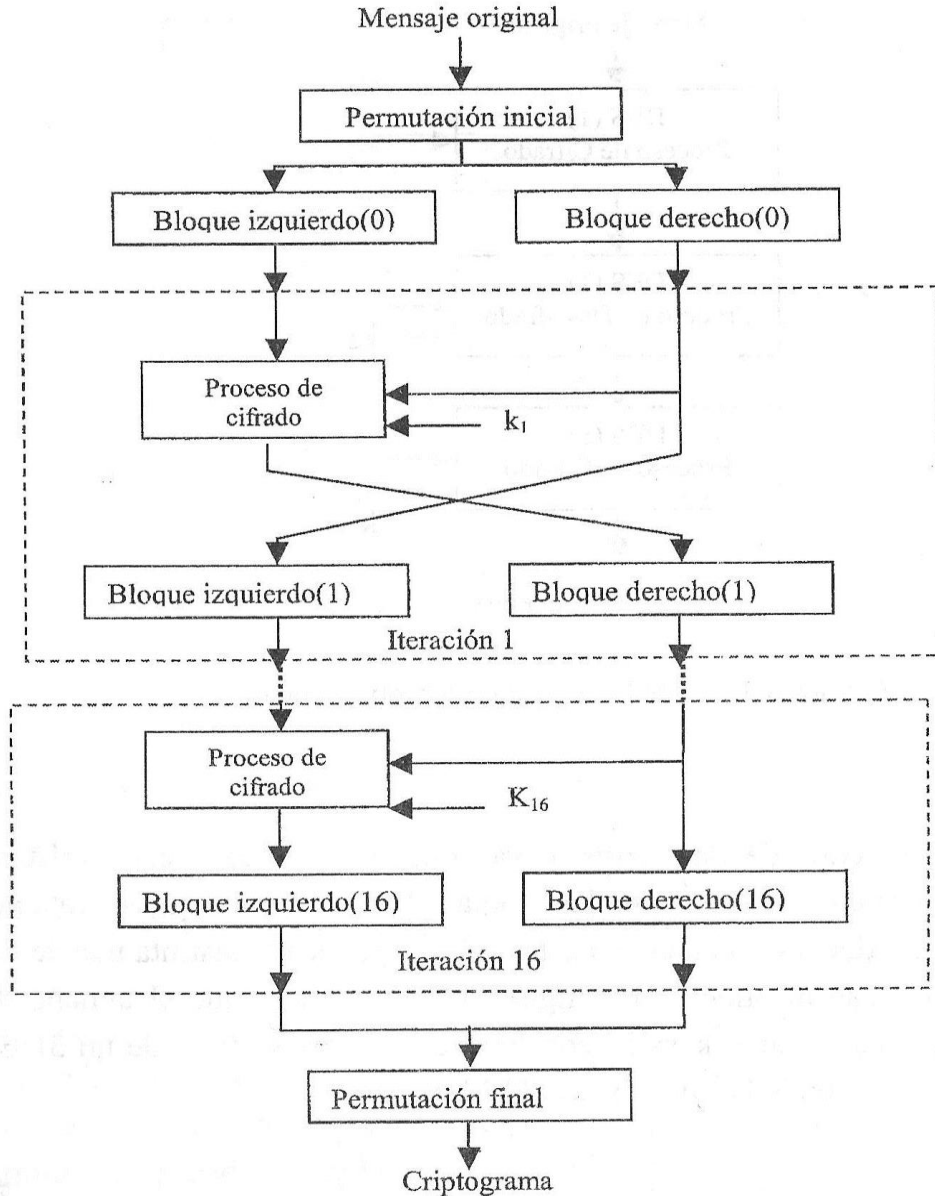


Figura 4.3 Algoritmo DES

2. Triple DES

También es conocido como TDES o 3DES, fue desarrollado por IBM en 1998. Actualmente se utiliza con una clave de 128 bits que es compatible con el DES visto anteriormente. Utiliza dos o tres claves diferentes para la generación de las subclaves que se emplean en las iteraciones correspondientes para el cifrado de los datos. Este nuevo algoritmo toma una clave de 128 bits y la divide en dos de 64 bits cada una de la siguiente forma:

- a) Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
- b) Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
- c) Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

No llega a ser un cifrado múltiple, porque no son independientes todas las subclases. Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con dos claves diferentes se aumenta el tamaño efectivo de la clave.

La variante más simple del Triple DES funciona de la siguiente manera (figura 4.4):

$$C = E_{DES}^{k_3} \left(D_{DES}^{k_2} \left(E_{DES}^{k_1} (M) \right) \right)$$

Donde M es el mensaje a cifrar y k1, k2 y k3 las respectivas claves DES. En la variante 3TDES las tres claves son diferentes; en la variante 2TDES, la primera y tercera clave son iguales.

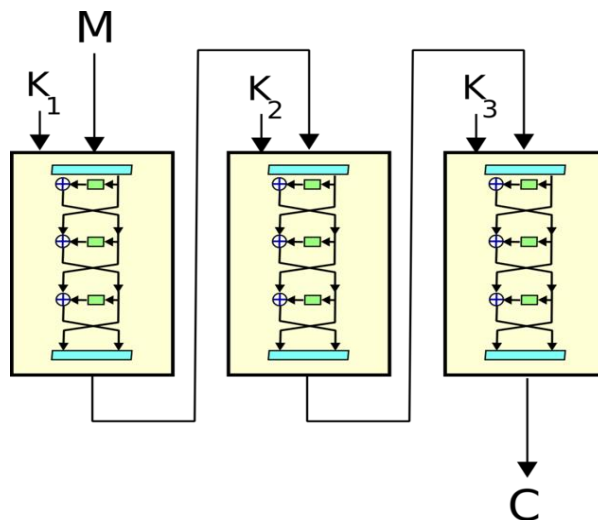


Figura 4.4 Proceso del algoritmo TDES

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, TDES fue elegido como forma de agrandar el largo de la clave sin necesidad de cambiar de algoritmo de cifrado. Este método de cifrado es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave (112 bits), pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES. Por tanto, la longitud de la clave usada será de 192 bits, aunque como se ha dicho, su eficacia solo sea de 112 bits.

El Triple DES está desapareciendo lentamente, siendo reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo Triple DES (anteriormente usaban el DES). Por su diseño, el DES y el TDES son algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad.

3. IDEA (International Data Encryption Algorithm, Algoritmo Internacional de Cifrado de Datos)

Es un cifrador por bloques diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zurich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del DES. IDEA fue una revisión menor de PES (Proposed Encryption Standard, Estándar de Cifrado Propuesto), un algoritmo de cifrado anterior. Originalmente IDEA había sido llamado IPES (Improved PES, PES Mejorado).

El nombre IDEA es una marca registrada licenciada mundialmente por MediaCrypt aunque sus patentes acaban de caducar en el periodo 2011-2012. Además, fue utilizado como el cifrador simétrico en las primeras versiones de PGP (PGP v2.0) y se incorporó luego de que el cifrador original usado en la v1.0 (*Bass-O-Matic*) se demostró inseguro. Es un algoritmo opcional en OpenPGP.

También opera con bloques de texto de 64 bits usando una clave de 128 bits, consiste de ocho transformaciones idénticas (cada una llamada ronda) y una transformación de salida (llamada media ronda). Realiza operaciones como XOR bit a bit, adición y multiplicación modular. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos que son algebraicamente *incompatibles* en cierta forma.

El algoritmo de descifrado es muy parecido al de cifrado, por lo que resulta muy fácil y rápido de programar, hasta ahora no ha sido roto nunca, aportando una longitud de clave segura y fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

En primer lugar, el ataque por fuerza bruta resulta impracticable, ya que sería necesario probar 1038 claves, cantidad imposible de manejar con los medios informáticos actuales. Los diseñadores analizaron IDEA para medir su fortaleza frente al criptoanálisis diferencial y concluyeron que es inmune bajo ciertos supuestos. No se han informado de debilidades frente al criptoanálisis lineal o algebraico. Se han encontrado algunas claves débiles, las cuales en la práctica son poco usadas siendo necesario evitarlas explícitamente. Es considerado por muchos como uno de los cifrados en bloque más seguros que existen.

4. AES (Advanced Data Encryption Standard, Estándar avanzado de cifrado de datos)

Es uno de los algoritmo más reciente publicado por el NIST (Instituto Nacional de Estándares y Tecnología) en 2001, el cual presenta diferencias notables con respecto al resto de los cifradores simétricos, entre ellas destacan: el tamaño de los bloques de 128 bits, manejo de claves de longitudes diferentes y uso de matemáticas polinomiales en estructuras de campos finitos.

El procesar los datos en bloques de tamaño fijo con claves de diferentes longitudes impacta en el número de iteraciones que se realizan durante el cifrado y descifrado, de manera que la cantidad de vueltas va de 10 a 14; sin embargo, esto no altera la longitud del criptograma ya que éste siempre genera 128 bits.

AES es una red de sustitución-permutación, no una red de Feistel (como DES). También es mucho más rápido que DES, tanto en hardware como en software y además, requiere poca memoria.

La descripción de AES es simple si se cuentan con todos los elementos. Ésta consiste en dos partes, la primera se da en el proceso de cifrado y la segunda en el proceso de generación de subclaves, la cual se muestra en la figura 4.5.

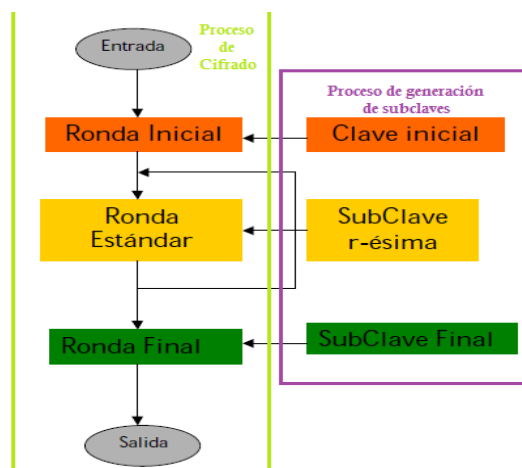


Figura 4.5 Estructura básica de AES (Advanced Encryption Standard)

En la actualidad, se han intentado varios ataques contra el AES siendo exitosos sobre versiones reducidas a 7 rondas para claves de 128 bits, de 8 rondas para las claves de 192 bits, y de 9 rondas, para las claves de 256 bits. Sin embargo, es cierto que en estos ataques se evidencia una escasa diferencia entre las rondas reales pero con una mejora en los ataques, cabría la posibilidad de romper un cifrado que use todas las rondas.

El método más común de ataque hacia un cifrador por bloques consiste en intentar varios ataques sobre versiones del cifrador con un número menor de rondas. El AES tiene 10 rondas para llaves de 128 bits, 12 rondas para llaves de 192 bits, y 14 rondas para llaves de 256 bits. En el año 2005, los mejores ataques conocidos son sobre versiones reducidas a 7 rondas para llaves de 128 bits, 8 rondas para llaves de 192 bits y 9 rondas para llaves de 256 bits (Ferguson et al, 2000).

Algunos criptógrafos muestran preocupación sobre la seguridad del AES. Ellos sienten que el margen entre el número de rondas especificado en el cifrador y los mejores ataques conocidos es muy pequeño. El riesgo es que se puede encontrar alguna manera de mejorar los ataques y de ser así, el cifrado podría ser roto. En el contexto criptográfico se considera *roto* un algoritmo si existe algún ataque más rápido que una búsqueda exhaustiva (ataque por fuerza bruta). De modo que un ataque contra el AES de llave de 128 bits que requiera solo 2120 operaciones sería considerado como un ataque que rompe el AES aun tomando en cuenta que por ahora sería un ataque irrealizable. Hasta el momento, tales preocupaciones pueden ser ignoradas.

Otra preocupación es la estructura matemática de AES. A diferencia de la mayoría de los cifradores de bloques, AES tiene una descripción matemática muy ordenada. Esto no ha llevado todavía a ningún ataque, pero algunos investigadores están preocupados que futuros ataques quizá encuentren una manera de explotar esta estructura.

4.2.II ASIMÉTRICOS

Se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede descifrar lo que la otra ha cifrado.

Una de las claves de la pareja, llamada clave privada, es usada por el propietario para cifrar los mensajes, mientras que la otra, llamada clave pública, es usada para descifrar el mensaje (figura 4.6).

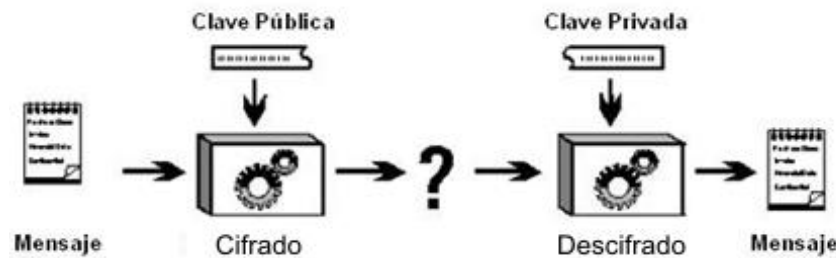


Figura 4.6 Algoritmo asimétrico. Hacen uso de una clave para cifrar, y otra diferente para descifrar. La clave para cifrar es pública; la clave para descifrar es privada.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre por parejas, estando cada una de ellas ligada intrínsecamente a la otra.

Mientras que la clave privada se debe mantener en secreto por su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir con los siguientes puntos:

- Conociendo el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
- Conociendo el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto cifrado con la clave privada.
- Dado un texto cifrado con una clave privada solo existe una pública capaz de descifrarlo y viceversa.

El primer sistema de clave pública que apareció fue el de Diffie-Hellman en 1976, fue la base para el desarrollo de los algoritmos que después aparecieron, entre los que destacan está el RSA (Rivest, Shamir y Adelman), los más utilizados en la actualidad son el DSA, Gamal y la criptografía de curva elíptica.

Los principales algoritmos asimétricos son:

1. Diffie-Hellman

Este algoritmo de cifrado de Whitfield Diffie y Martin Hellman fue el punto de partida para los sistemas asimétricos, basados en clave pública y privada a partir de 1976. Se le conoce como el algoritmo de Intercambio Exponencial, el cual basa su seguridad en la dificultad de calcular logaritmos discretos en un campo finito y se emplea para la distribución de claves, pero no para cifrar y descifrar.

Permite que dos entidades se pongan de acuerdo en un número a través de un canal público con la ventaja de que dicho número no pueda ser conocido por cualquier atacante que esté monitorizando la comunicación, lo cual es de suma importancia ya que dicho número es el que representa la clave simétrica a compartir por ambas entidades en el intercambio de información de manera confidencial.

Proceso

A los interlocutores de esta supuesta conversación *se les llama Ana y Rogelio*, siguiendo una convención usada en criptografía. Por la misma razón, al tercer elemento que observa la conversación en la sombra que intenta conocer el secreto se le llama *Vanesa*.

- a) Ana selecciona dos números, llamados q y x_a .
- b) Rogelio selecciona otros dos, llamados n y x_b . Mediante su canal de comunicaciones no cifrado (que puede ser correo electrónico, faxes o simplemente diciéndolo en la plática), ambos hacen saber q y n a las partes respectivas.
- c) Ana entonces calcula el nuevo número y_a , mediante la fórmula: $y_a = (n^{x_a}) \bmod q$.
- d) De igual forma, Rogelio calcula su nuevo número y_b : $y_b = (n^{x_b}) \bmod q$.
- e) Y de nuevo a voz en grito, Ana y Rogelio hacen públicos y_a , y_b .
- f) Ahora Ana calcula un último valor, k_a , mediante $k_a = (y_b^{x_a}) \bmod q$ y Rogelio su correspondiente k_b con $k_b = (y_a^{x_b}) \bmod q$.
- g) Los números k_a y k_b son el mismo; los interlocutores tienen ya un secreto compartido, que Vanesa no sabe, pese a haber tenido acceso a todo el intercambio de información.
- h) Ana y Rogelio pueden ahora usar sus claves para cifrar un mensaje.
- i) Para dificultar que Vanesa pueda conseguir algo por el método de la fuerza bruta, los números elegidos tienen que ser primos y grandes.

Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número; si bien, el cálculo de potencias discretas es fácil, la obtención de su función inversa, el logaritmo discreto, no tiene una solución analítica para números grandes.

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos, ya que en la práctica solo es válido para el intercambio de claves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer, Capa de conexión segura) y VPN (Virtual Private Network, Red privada virtual).

2. RSA (Rivest, Shamir, Adlman)

Fue creado en 1978 por Rivest, Shamir y Adlman, es el sistema criptográfico asimétrico más conocido y usado. Este método está basado en el artículo de Diffie-Hellman sobre sistemas de llave pública.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya se tendría un divisor del número.

Ahora bien, si el número considerado es un número primo (el que solo es divisible por 1 y por él mismo), para factorizarlo habrá que empezar por 1, 2, 3,... hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves y se buscan dos números primos lo suficientemente grandes p y q (de entre 100 y 300 dígitos) de la siguiente forma:

- a) Se obtienen los números $N = p * q$ y $\phi = (p-1) * (q-1)$.
- b) Se busca un número e tal que no tenga múltiplos comunes con ϕ .
- c) Se calcula $d = e-1 \text{ mod } \phi$, con mod = resto de la división de números enteros.
- d) Y ya con estos números obtenidos se obtiene la clave pública $K_{pb} = (N, e)$ y la clave privada $K_{pv} = (N, d)$. Los números p , q y ϕ se destruyen. También se hace pública la clave $K_{pb} = (N, e)$, necesario para alimentar el algoritmo.

El cálculo de estas claves se realiza en secreto en el nodo en el que se va a guardar la clave privada, y una vez generada ésta, conviene protegerla mediante un algoritmo criptográfico simétrico.

Para cifrar un mensaje M_{cla} utilizando $K_{pb} = (N, e)$, se procede a realizar la potenciación

$$Crip = M_{cla}^e \text{ mod } N$$

Para el proceso de descifrado, debe utilizarse $K_{pv} = (N, d)$, nuevamente, con una potenciación:

$$M_{cla} = Crip^d \text{ mod } N$$

En cuanto a las longitudes de las claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 procesadores trabajando en paralelo para hacerlo).

Además, basa su seguridad en ser una función computacionalmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo \emptyset no es factible a menos que se conozca la factorización de e , clave privada del sistema.

RSA es el más conocido y usado de los sistemas de clave pública y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos por ser más rápidos. Se suele usar también en los sistemas mixtos para cifrar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

3. DSA (Digital Signature Algorithm, Algoritmo de firma digital)

Tiene como finalidad firmar documentos electrónicos pero de ninguna manera cifra información. Fue desarrollado por el NIST (Instituto Nacional de Estándares y Tecnología) en 1994. La firma digital se apoya en el uso de un bloque de datos de resumen (de longitud fija), que es generado mediante alguna función Hash, la cual debe ser verificada por el receptor del documento firmado para garantizar su autenticidad.

Se basa en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible (logaritmo discreto). Al contrario que RSA, este algoritmo no proporciona la capacidad para proporcionar el servicio de confidencialidad.

El algoritmo es más rápido para generar la firma que para validarla, al revés de lo que sucede con el RSA. Emplea claves de 1024 bits (originalmente eran 512 bits, pero se aumentó por falta de seguridad). No se conocen ataques eficientes contra este algoritmo, solo existen problemas con un conjunto de números primos, pero son fácilmente evitables si se siguen los sistemas adecuados de generación de claves.

La elección de este algoritmo como estándar de firmado generó multitud de críticas: se pierde flexibilidad respecto al RSA (que es un estándar), la verificación de firmas es lenta, el proceso de elección fue poco claro y la versión original empleaba claves que lo hacían poco seguro.

Su funcionamiento básico se describe a continuación:

Generación de llaves

- Elige un número primo p de L bits, donde $512 \leq L \leq 1024$ y L es divisible por 64.
- Elige un número primo q de 160 bits, tal que $p-1 = qz$, donde z es algún número natural.
- Elige h , donde $1 < h < p - 1$ tal que $g = hz(\text{mod } p) > 1$.
- Elige x de forma aleatoria, donde $0 < x < q$.
- Calcular $y = g^x(\text{mod } p)$.

Los datos públicos son p, q, g e y .
 x es la llave privada.

Firma

- Elige un número aleatorio s , donde $1 < s < q$.
- Calcular $s1 = (g^s \text{ mod } p) \text{ mod } q$.
- Calcular $s2 = (H(m) + s1 * x) \text{ mod } q$, donde $H(m)$ es la función hash SHA-1 aplicada al mensaje m .
- La firma es el par $(s1, s2)$. Si $s1$ o $s2$ es cero, se vuelve a repetir el procedimiento.

Verificación

- Calcular $w = (s2)^{-1}(\text{mod } q)$.
- Calcular $u1 = H(m) * w(\text{mod } q)$.
- Calcular $u2 = s1 * w(\text{mod } q)$.
- Calcular $v = [g^{u1} * y^{u2} \text{ mod } p] \text{ mod } q$.
- La firma es válida si $v = s1$.

Las funciones hash tienen una importancia en la criptografía porque se enfocan a solventar los problemas de la integridad de los mensajes, así como la autenticidad tanto del mensajes como de su origen.

Son funciones matemáticas que realizan el resumen de un documento a firmar, de manera que para ello comprimen el documento en un único bloque de longitud fija, bloque cuyo contenido resulta ilegible y no tiene ningún sentido real.

El valor hash de un mensaje es un valor único generado a partir de él. Esto se realiza pasando el mensaje a través de una función criptográfica con las siguientes propiedades:

- a) Su algoritmo es conocido públicamente.
- b) Es de un solo sentido ya que a partir del valor hash no se pueden obtener los datos originales.
- c) Es muy poco probable obtener el mismo valor hash a partir de otros datos.

4. El Gamal

Es un algoritmo basado en Diffie-Hellman (en el problema de logaritmo discreto) y que fue descrito por Taher ElGamal en 1984. Este algoritmo se utiliza en GNU Privacy Guard, PGP, y otros sistemas criptográficos como la generación de firmas digitales.

Este algoritmo no está bajo ninguna patente lo que lo hace de uso libre. La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido y la dificultad de calcular un logaritmo discreto.

El algoritmo es bastante similar a Diffie-Hellman, constando de tres partes importantes: el generador de claves, el cifrado y descifrado.

Generación de claves (pasos)

1. Los usuarios A y B seleccionan sus parámetros n , α y Z_n^* y los hacen públicos.
2. Tanto A como B eligen un número aleatorio primo que sea de gran tamaño para a y b dentro de los límites de n (sus respectivas claves privadas).
3. Cada usuario debe calcular $\alpha^a \bmod n$ y $\alpha^b \bmod n$ respectivamente, de manera que los valores obtenidos representan las respectivas claves públicas.

Cifrado - A cifra un mensaje M y lo envía a B (pasos)

1. A genera un número aleatorio v que representa un número de sesión y utilizando los parámetros que han hecho públicos B calcula $\alpha^v \bmod n$.
2. Con la clave pública de B, $K_{pBB} = [\alpha^b \bmod n]$ A calcula $(\alpha^b)^v \bmod n$ y $(M * \alpha^{bv}) \bmod n$. El criptograma que se enviará será $Crip = [\alpha^v \bmod n, (M \alpha^{bv}) \bmod n]$.

Descifrado - B descifra el criptograma Crip que le envió A (pasos)

1. B recibe $Crip = [\alpha^v \bmod n, (M \alpha^{bv}) \bmod n]$.
2. Se toma el primer dato, es decir, $\alpha^v \bmod n$, para calcular $(\alpha^v)^b \bmod n$.
3. Ahora B realiza la operación $[(M \alpha^{bv}) \bmod n] * [(\alpha^v)^b \bmod n]^{-1}$. El resultado de esta operación es el $Mcl = M$.

NOTA: El inverso multiplicativo modular es un número z tal que:

$$(z * z^{-1}) \equiv 1 \bmod n$$

5. Curvas elípticas

Son entidades algebraicas y geométricas que han sido aplicadas a la criptografía por parte de Neal Koblitz y Victor Miller en 1985.

Los sistemas de cifrado en este caso, utilizan los grupos de curvas elípticas, donde un grupo es un conjunto de elementos con operaciones aritméticas definidas en estos elementos, para los grupos de curvas elípticas, estas operaciones específicas están definidas geoméricamente.

El criptosistema de curvas elípticas (ECC) es un sistema de llave pública basado en la dificultad para calcular logaritmos discretos sobre una curva elíptica y tienen las siguientes características:

- a) Dada la curva elíptica E definida sobre el campo finito K , P y Q que son puntos de $E(K)$ tal que: $Q = dP$
- b) El problema de determinar d dados los puntos P y Q es considerado altamente difícil ya que:
 - i. La multiplicación escalar es la operación dominante en ECC.
 - ii. En general, d es usada como la llave secreta y Q como la llave pública.

Ventajas

- a) Es más atractivo que RSA porque requiere llaves significativamente más cortas para brindar el mismo nivel de seguridad (tabla 4.1).

Tabla 4.1 Comparación del tamaño de la llave (bits) entre ECC y el RSA

	Tamaño de llave (bits)				
ECC	160	224	256	384	512
RSA	1024	2048	3072	8192	15360

- b) Más rápida ejecución y menores requerimientos de memoria
- c) Ahorro en transferencias de los datos
- d) Ideal para dispositivos portátiles como PDAs, smartcards, celulares, etcétera.

Algunos ejemplos de protocolos usando ECC:

- a) ECDSA (EC Digital Signature Algorithm, Algoritmo de firma digital de curvas elípticas)
- b) ECDH (EC Diffie-Hellman key agreement, Intercambio de llaves de curvas elípticas Diffie-Hellman)

CAPÍTULO 5

INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR



CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Una arquitectura cliente/servidor es el procesamiento cooperativo de la información por medio de un conjunto de procesadores, en el cual múltiples clientes, distribuidos geográficamente, solicitan requerimientos a uno o más servidores centrales. Siendo ésta una arquitectura distribuida, permite a los usuarios finales obtener acceso a la información de forma transparente aun en entornos multiplataforma.

Es un modelo desarrollado para los sistemas de información, en el que las transacciones se dividen en procesos independientes que cooperan entre sí para intercambiar información, servicios o recursos. Se denomina cliente al proceso que inicia el diálogo o solicita los recursos y servidor al proceso que responde a las solicitudes. Es el modelo de interacción más común entre aplicaciones en una red

La mayoría de los servicios de Internet son de tipo cliente-servidor. La acción de visitar un sitio web requiere una arquitectura cliente-servidor, ya que el servidor web despliega las páginas web al navegador (al cliente).

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

5.1 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Una arquitectura es un conjunto de reglas, definiciones, términos y modelos que se emplean para producir un producto.

La arquitectura cliente/servidor agrupa conjuntos de elementos que efectúan procesos distribuidos y cómputo cooperativo.

En la familia de protocolos TCP/IP, las comunicaciones entre computadoras se rigen básicamente por el modelo cliente/servidor, siendo un modelo que intenta proveer usabilidad, flexibilidad, interoperabilidad y escalabilidad en las comunicaciones.

El término cliente/servidor fue usado por primera vez en 1980 para referirse a las computadoras que están en red. Este modelo empezó a ser aceptado a finales de 1980. Su funcionamiento es sencillo al usar una máquina cliente que requiere un servicio de una máquina servidor y éste a su vez realiza la función para la que está programado (figura 5.1).

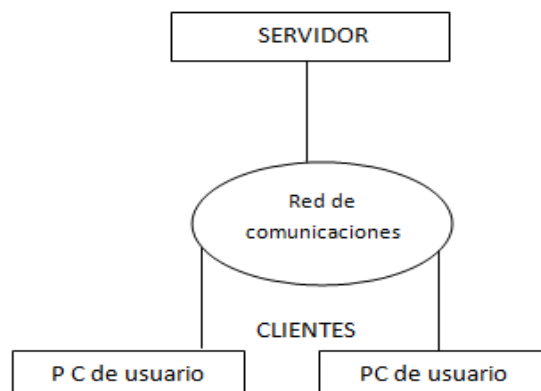


Figura 5.1 Modelo Cliente/Servidor

Los principales beneficios son:

- a) Mejor aprovechamiento de la potencia de cómputo (reparte el trabajo).
- b) Reduce el tráfico en la red.
- c) Opera bajo sistemas abiertos.
- d) Permite el uso de interfaces gráficas variadas y versátiles.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Esta arquitectura se divide en dos partes, la primera es el servidor y la segunda es un conjunto de clientes.

- 1) Servidor: es una máquina potente que actúa y funciona como un sistema de base de datos.
- 2) Clientes: suelen ser estaciones de trabajo que solicitan varios servicios al servidor.

Ambas partes deben estar conectadas entre sí mediante una red. Además, necesita de tres tipos de software para su correcto funcionamiento:

- a) Software de gestión de datos: Se encarga de la manipulación y gestión de los datos almacenados y requeridos por las diferentes aplicaciones. Normalmente, se aloja en el servidor.
- b) Software de desarrollo: Se aloja en los clientes y solo en aquellos que se dediquen al desarrollo de aplicaciones.
- c) Software de interacción con los usuarios: Reside en los clientes y es la aplicación gráfica de usuario para la manipulación de datos, siempre a nivel usuario (consultas principalmente).

Aparte del software anterior existen más aplicaciones para el correcto funcionamiento de la arquitectura cliente/servidor pero están condicionados por el tipo de sistema operativo instalado y el tipo de red en la que se encuentra (figura 5.2).

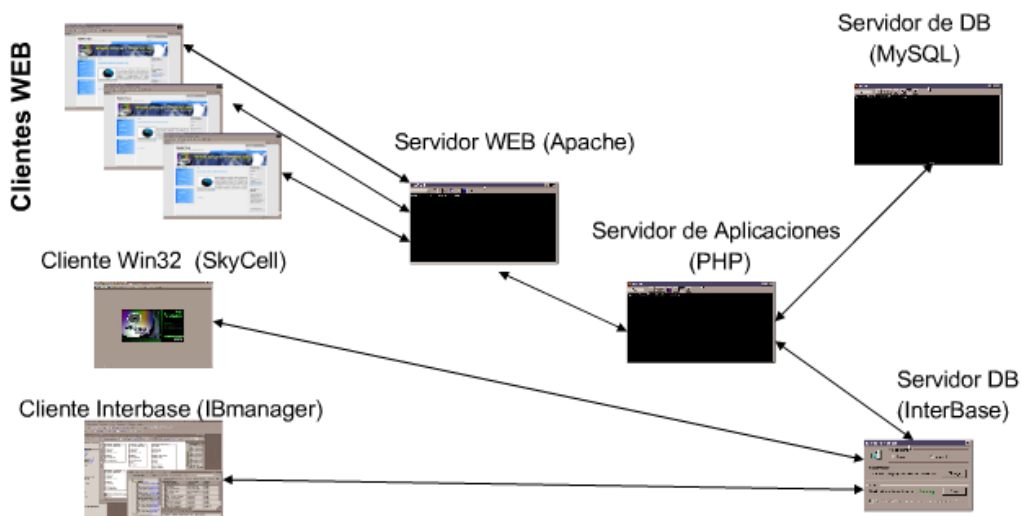


Figura 5.2 Interacción de clientes y servidores

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

A continuación se mencionan las características, ventajas, desventajas, los diferentes modelos que existen y los modelos de dos, tres y N capas de la arquitectura cliente/servidor.

Características

- a) Combinación de un cliente que interactúa con el usuario y un servidor que interactúa con los recursos compartidos. El proceso del cliente proporciona la interfaz entre el usuario y el resto del sistema. El proceso del servidor actúa como un motor de software que maneja recursos compartidos tales como bases de datos, impresoras, módems, etcétera.
- b) Las tareas del cliente y del servidor tienen diferentes requerimientos en cuanto a recursos de cómputo como velocidad del procesador, memoria, capacidad del disco duro, salidas y entradas de dispositivos (input-output devices).
- c) Se establece una relación entre distintos procesos, los cuales pueden ser ejecutados en la misma máquina o en máquinas diferentes distribuidas a lo largo de la red.
- d) Existe una clara distinción de funciones basada en el concepto de servicio que se establece entre clientes y servidores.
- e) La relación establecida puede ser de muchos a uno, en la que un servidor puede dar servicio a muchos clientes, regulando su acceso a recursos compartidos.
- f) Los clientes corresponden a procesos activos en cuanto éstos hacen peticiones de servicios a los servidores. Éstos últimos tienen un carácter pasivo ya que esperan las peticiones de los clientes.
- g) No existe otra relación entre clientes y servidores que no sea la que se establece a través del intercambio de mensajes entre ambos. El mensaje es el mecanismo para la petición y entrega de solicitudes de servicio.
- h) El ambiente es heterogéneo. La plataforma de hardware y el sistema operativo del cliente y del servidor no son siempre la misma. Precisamente una de las principales ventajas de esta arquitectura es la posibilidad de conectar clientes y servidores independientemente de sus plataformas.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

- i) El concepto de escalabilidad tanto horizontal como vertical es aplicable a cualquier sistema cliente/servidor. La escalabilidad horizontal permite agregar más estaciones de trabajo activas sin afectar significativamente el rendimiento. La escalabilidad vertical permite mejorar las características del servidor o agregar múltiples servidores.

Ventajas

- a) La posibilidad de utilizar máquinas considerablemente más económicas que las requeridas por una solución centralizada que se basa en sistemas grandes al utilizar componentes de hardware como de software y de varios fabricantes lo cual contribuye considerablemente a la reducción de costos y favorece la flexibilidad en la implantación y actualización de soluciones.
- b) El esquema cliente/servidor facilita la integración entre diferentes sistemas y comparte información permitiendo que las máquinas ya existentes puedan ser utilizadas pero utilizando interfaces más amigables al usuario así se pueden integrar computadoras con sistemas medianos y grandes, sin necesidad de que todos tengan que utilizar el mismo sistema operacional.
- c) El uso de interfaces gráficas interactivas en los sistemas construidos bajo este esquema tienen mayor interacción y más intuitivo con el usuario. En esta arquitectura presenta la ventaja, con respecto a uno centralizado, de que no siempre es necesario transmitir información gráfica por la red ya que lo puede residir el cliente, con lo cual permite aprovechar mejor el ancho de banda de la red.
- d) Es más rápido el mantenimiento y el desarrollo de aplicaciones porque se pueden emplear herramientas ya existentes.
- e) La estructura inherentemente modular integra nuevas tecnologías y el crecimiento de la infraestructura computacional al favorecer la escalabilidad de las soluciones.
- f) Esta arquitectura contribuye a proporcionar a los diferentes departamentos de una organización soluciones locales que permiten la integración de la información relevante a nivel global.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Desventajas

- a) El mantenimiento de los sistemas es más difícil pues implica la interacción de diferentes partes de hardware y de software distribuidas por distintos proveedores lo cual dificulta el diagnóstico de fallas.
- b) Se cuenta con pocas herramientas para la administración y ajuste del desempeño de los sistemas.
- c) Es importante que los clientes y los servidores utilicen el mismo mecanismo con lo cual implica que se deben tener mecanismos generales que existan en diferentes plataformas.
- d) Hay que tener estrategias para el manejo de errores y para mantener la consistencia de los datos.
- e) Si tiene un bajo desempeño, la red puede provocar problemas por congestión, dificultad de tráfico de datos, que se pierda la conexión, etcétera.

I. Modelo cliente/servidor de dos capas (Two-Tier Model)

En una arquitectura cliente/servidor clásica se tienen dos capas:

- 1) Una donde está el cliente que implementa la interface.
- 2) Otra donde se encuentra el gestor de bases de datos que trata las peticiones recibidas desde el cliente.

La lógica de la aplicación se encuentra repartida entre el cliente y servidor (figura 5.3).

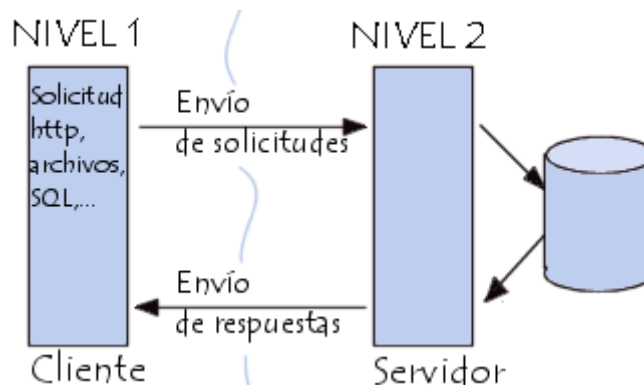


Figura 5.3 Arquitectura cliente/servidor de dos capas (Two-tier)

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Las principales ventajas son:

- a) Se mantiene una conexión persistente con la base de datos.
- b) Se minimizan las peticiones en el servidor trasladándose la mayor parte del trabajo al cliente.
- c) Se gana en rendimiento gracias a la conexión directa y permanente con la base de datos. A través de una única conexión se realiza el envío y recepción de varios datos.

Las principales desventajas son:

- a) Es muy dependiente del tipo controlador JDBC (Java Data Base Connectivity, Conectividad a la Base de Datos de Java) que se utilice para acceder a la base de datos. El acceso se realiza desde el cliente y esto significa que es el que tiene que tener instalado en su sistema los controladores necesarios para que se produzca la comunicación con la base de datos.
- b) Debe tomar en cuenta el modelo de seguridad de Java, el cual impide que desde un applet sin validar, como lo son la mayoría de los que se ejecutan en un navegador, se puedan realizar las siguientes operaciones:
 - i. Tener acceso general mediante JDBC a la bases de datos situada en diferentes direcciones URL a las que procede el mismo applet.
 - ii. Poder configurar los recursos locales como de información de la fuente de datos ODBC (Open Data Base Connectivity, Abrir una Conexión a la Base de Datos) para usar el puente JDBC-ODBC.
 - iii. Descargar clases nativas cuyo nombre empieza por *Java*. Esta restricción afecta directamente a los navegadores que utilizan JDK 1.0.2 o anterior, pues JDBC es posterior a esta versión, de forma que las clases apropiadas no estarán instaladas localmente ni podrán ser descargadas de Internet por el applet.
- c) Es conocido que los programas de Java pueden ser descompilados muy fácilmente para tener el acceso a las bases de datos mediante un applet de Java que conlleva un riesgo considerable en cuanto a la seguridad.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

II. Modelo cliente servidor de tres capas (Three-Tier Model)

Con esta arquitectura se añade una nueva capa entre el cliente y el servidor donde se implementa la lógica de la aplicación. De esta forma el cliente es básicamente una interface que no tiene por qué cambiar si cambian las especificaciones de la base de datos o de la aplicación, quedando así aislado completamente del acceso a los datos (figura 5.4).

Así un applet de Java se carga en el navegador del cliente y se comunica con un servlet que corre en la máquina servidor o accede a la base de datos a través de un formulario HTML. El servlet establece una conexión a la base de datos mediante JDBC.

En este caso se tiene total libertad para escoger dónde se coloca la lógica de la aplicación: en el cliente, servidor de base de datos o en otro servidor aunque también se tiene total libertad para la elección del lenguaje a utilizar.

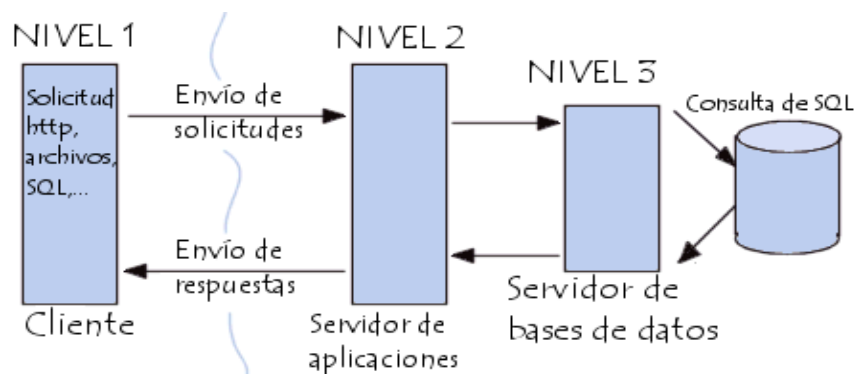


Figura 5.4 Arquitectura cliente/servidor de tres capas (Three-tier)

No existe compromiso alguno con el uso de lenguajes propietarios, por tal motivo las aplicaciones serán totalmente portables sin cambio alguno.

Puede determinarse en qué servidor se quieren hacer funcionar estos procedimientos. En aplicaciones críticas se pueden agregar tantos servidores de aplicación como sean necesarios sin comprometer en absoluto la integridad de la base de datos, obteniendo una escalabilidad muy grande sin necesidad de tocar el servidor de dicha base de datos.

Las principales ventajas de este modelo son:

- a) No existe ningún problema con respecto al tipo de controlador JDBC utilizado para acceder a la base de datos. Todos los recursos necesarios para establecer la conexión con la base de datos se encuentran en el servidor y por tanto el cliente no necesita instalar nada adicional en su máquina para poder acceder a la base de datos.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

- b) Proporciona considerables mejoras desde el punto de vista de la portabilidad de la aplicación, escalabilidad, robustez y reutilización del código. Asimismo facilita las tareas de migración o cambios en el sistema gestor de la base de datos.
- c) Desaparecen las restricciones debidas a las limitaciones de los applets impuestas por el modelo de seguridad de Java.

La principal desventaja de este modelo es:

- a) Esta solución es menos eficiente que la del modelo de dos capas ya que añade una capa intermedia más de software.

III. Modelo cliente servidor de N capas (N-Tier Model)

En la arquitectura en 3 niveles cada servidor (nivel 2 y 3, ver figura 5.5) realiza una tarea especializada (un servicio). Por lo tanto el servidor puede utilizar los servicios de otros servidores para proporcionar su propio servicio. Por lo tanto, la arquitectura en 3 niveles es potencialmente una arquitectura en N-niveles.

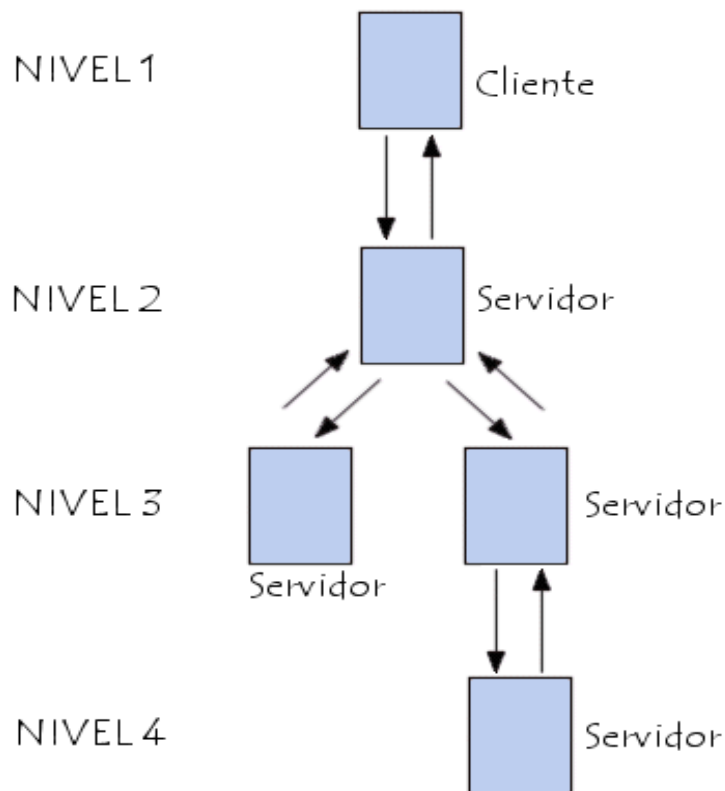


Figura 5.5 Arquitectura cliente/servidor de N capas (N-tier)

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

A continuación se dará una introducción a los principales temas de la arquitectura Cliente/Servidor.

I. Puertos

Un puerto es una forma genérica de denominar a una interfaz por la cual diferentes tipos de datos pueden ser enviados y recibidos. Dicha interfaz puede ser física o puede ser a nivel software.

La asignación de puertos permite que una máquina pueda establecer simultáneamente diversas conexiones TCP/IP con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección IP, pero van dirigidos a puertos diferentes.

También una máquina puede establecer simultáneamente diversas comunicaciones TCP/IP con otra utilizando puertos distintos para cada conexión.

Como se ha indicado, los números de puerto se indican mediante una palabra de 2 bytes (16 bits), por lo que el rango de valores es de 2^{16} (0 a 65,535) y en principio una aplicación puede utilizar cualquier número dentro del rango.

Sin embargo, con el fin de unificar criterios en cuanto a los puertos que utilizarían las aplicaciones de Internet, la IANA (Assigned Numbers Authority, Agencia de Asignación de Números) realizó una asignación de los números disponibles en tres categorías:

- a) *Puertos bien conocidos (Well known ports)*: Comprendidos entre 0 y 1023. Estos 1024 (2^{10}) puertos pueden ser representados con 10 bits y son reservados para servicios conocidos.
- b) *Puertos registrados (Registered ports)*: 48,127 puertos comprendidos entre 1024 y 49,151. Son normalmente empleados por las aplicaciones de usuario de forma temporal cuando se conectan con los servidores aunque también pueden representar servicios que hayan sido registrados por un tercero.
- c) *Puertos dinámicos y privados*: Los comprendidos entre los números 49,152 y 65,535. Son usados por las aplicaciones de usuario aunque son menos frecuentes. Además, no tienen significado fuera de la conexión TCP en la que fueron usados.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

ii. Socket

Es un mecanismo de comunicación entre dos o más procesos por el cual es posible enviar o recibir información.

El conjunto de servicios que tiene un socket es para facilitar una conexión entre procesos ya sea que se ejecuten en una sola máquina o si lo hacen en red. Estos procesos intercambian información transmitiendo datos a través de mensajes que circulan entre un socket en un proceso y otro socket en otro proceso, para así tener una comunicación entre máquinas que suelen utilizar los protocolos TCP/IP, logrando así la independencia del hardware y de la arquitectura de red mediante la cual se establece el enlace; siendo esto posible por la estructura en capas que posee una red de ordenadores.

Los sockets son conexiones que pertenecen a la capa de transporte del modelo OSI. Una aplicación con sockets debe especificar los puertos del protocolo local y remoto, la dirección IP remota, el protocolo (TCP o UDP) y debe especificar si iniciará la transferencia o esperará por una conexión (si funcionará como servidor o cliente).

El mecanismo de un socket está diseñado de forma genérica ya que por sí mismo no contiene información suficiente para realizar una comunicación entre procesos.

Un socket opera dentro de un dominio de comunicación de tal forma que determina el formato de direcciones a utilizar y el protocolo de comunicación, así como el dominio que define si los dos procesos se comunican en el mismo sistema o en sistemas diferentes y cómo pueden ser direccionados.

Un socket puede clasificarse según su dominio y el tipo de conexión que realice.

- a) Sockets stream: Es un servicio orientado a conexión donde los datos se transfieren sin encuadrarlos en registros o bloques. Para establecer una comunicación utilizando el protocolo TCP.
- b) Sockets datagrama: Es un servicio de transporte sin conexión que utiliza el protocolo de transporte UDP. Cada vez que se envían datagramas es necesario enviar el descriptor del socket local y la dirección del socket que deberá recibir el datagrama. Hay que enviar datos adicionales cada vez que se realice una comunicación. Los datos se envían y reciben en paquetes cuya entrega no está garantizada.
- c) Sockets raw: Da acceso a la capa de software y de red subyacente o a protocolos de más bajo nivel. Se utilizan sobre todo para la depuración del código de los

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

protocolos. Los sockets raw proporcionan acceso al ICMP que se utiliza para comunicarse entre varias entidades IP.

- d) Socket de flujo: Da un flujo de datos de dos vías que es confiable y no tiene duplicados ni tampoco límites de grabación. El flujo opera en forma parecida a una conversación telefónica, utiliza un socket stream.
- e) Socket de paquete secuencial: Da una conexión de dos vías, secuencial y confiable para datagramas de una longitud fija máxima.
- f) Socket orientado a conexión: Establece un camino virtual entre el servidor y el cliente de tal manera que la conexión sea fiable, sin pérdidas de información ni duplicados. La información llega en el mismo orden que se envía. El cliente es el que abre una sesión en el servidor y éste guarda el estado del cliente.
- g) Socket no orientado a conexión: Envía datagramas de tamaño fijo, tiene el inconveniente de que no es fiable, puede haber pérdidas de información y duplicados. La información puede llegar en distinto orden del que se envía. No se guarda ningún estado del cliente en el servidor por lo tanto es más tolerante a fallos en el sistema.

iii. Procesos del cliente

Un cliente es un conjunto de software y hardware que invoca los servicios de uno o varios servidores que inicia un requerimiento. Este requerimiento puede convertirse en múltiples requerimientos de trabajo a través de redes LAN o WAN. La ubicación de los datos o de las aplicaciones es totalmente transparente para el cliente.

El cliente normalmente maneja todas las funciones relacionadas con la manipulación y despliegue de datos, por lo que están desarrollados sobre plataformas que permiten construir interfaces gráficas de usuario además de acceder a los servicios distribuidos en cualquier parte de una red.

Los pasos principales para que un cliente se conecte a un servidor son:

1. Abre el canal de comunicaciones para conectarse a la dirección de red atendida por el servidor.
2. Enviar al servidor un mensaje de petición de servicio y esperar hasta recibir respuesta.
3. Cerrar el canal de comunicación y terminar la ejecución del proceso.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Características principales del cliente:

- a) El cliente oculta el servidor y la red.
- b) Detecta e intercepta peticiones de otras aplicaciones y puede redirigirlas.
- c) Dedicado a la sesión del usuario (inicia, mantiene y termina).
- d) El método más común por el que se solicitan los servicios es a través de RPC (Remote Procedure Calls, Llamada de Procedimiento Remoto).

Las funciones principales que lleva a cabo el proceso del cliente:

- a) Administrar la interfaz de usuario.
- b) Interactuar con el usuario.
- c) Procesar la lógica de la aplicación y hacer validaciones locales.
- d) Recibir resultados del servidor.
- e) Formatear resultados.
- f) Mantener y procesar todo el diálogo con el usuario.
- g) Menús e interpretación de comandos.
- h) Entrada de datos y validación.
- i) Procesamiento de ayudas.
- j) Recuperación de errores.
- k) Generación de consultas e informes sobre las bases de datos.

La funcionalidad del proceso cliente marca la operatividad de las aplicaciones. De este modo el cliente se puede clasificar en:

- a) Cliente basado en aplicación de usuario: Los datos son de baja interacción y están fuertemente relacionados con la actividad de los usuarios de esos clientes.
- b) Cliente basado en lógica de negocio: Toma datos suministrados por el usuario y la base de datos y efectúa los cálculos necesarios según los requerimientos del usuario.

iv. Procesos del servidor

Es un conjunto de hardware y software dedicado a responder y atender los múltiples requerimientos de los clientes que hacen peticiones de algún recurso administrado por él. Los servidores pueden estar conectados a los clientes a través de redes LAN o WAN para proveer múltiples servicios y devuelvan los resultados a los clientes y éstos tengan acceso a bases de datos, fax, impresoras, procesamiento de imágenes, etcétera.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

El servidor normalmente maneja todas las funciones relacionadas con la mayoría de las reglas del negocio y los recursos de datos. En algunos casos existen procesos auxiliares que se encargan de recibir las solicitudes del cliente, verificar la protección, activar un proceso servidor para satisfacer el pedido, recibir su respuesta y enviarla al cliente. Manejan interbloqueos, recuperación ante fallas, manejar servicios de administración de la red, mensajes, control y administración de entrada al sistema (login), auditoría, recuperación y contabilidad.

Los pasos principales de un servidor mientras espera a que se conecte un cliente son:

1. Abre el canal de comunicación e informa a la red de la dirección a la que responderá y de la disposición para aceptar peticiones de servicio.
2. Espera a que el cliente realice una petición de servicio en la dirección que él tiene declarada.
3. Cuando recibe una petición de servicio, atiende al cliente.
4. La conexión es cerrada.

Tipos principales de servidores:

- a) Servidor de archivos.
- b) Servidor de bases de datos (SQL, CBASE, ORACLE, INFORMIX).
- c) Servidor de comunicaciones
- d) Servidor de impresión.
- e) Servidor de aplicaciones.

Las funciones principales que lleva a cabo el proceso del servidor:

- a) Acceso, almacenamiento y organización de datos.
- b) Actualización de datos almacenados y administración de recursos compartidos.
- c) Ejecución de toda la lógica para procesar una transacción.
- d) Procesamiento común de elementos del servidor (datos, capacidad de CPU, almacenamiento en disco, capacidad de impresión, manejo de memoria y comunicación).
- e) Aceptar los requerimientos de bases de datos que hacen los clientes.
- f) Procesar requerimientos de bases de datos.
- g) Formatear datos para transmitirlos a los clientes.
- h) Procesar la lógica de la aplicación y realizar validaciones a nivel de bases de datos.
- i) Gestión de periféricos compartidos.
- j) Control de accesos concurrentes a bases de datos compartidas.
- k) Enlaces de comunicaciones con otras redes de área local o extensa

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

Puede darse el caso que un servidor actúe a su vez como cliente de otro servidor. Existen numerosos tipos de servidores, cada uno de los cuales da lugar a un tipo de arquitectura cliente/servidor diferente.

v. Tipos de servidores para la arquitectura cliente/servidor

Los servidores pueden clasificarse de dos maneras:

a) Servidores iterativos

Este servidor recibe y atiende un requerimiento a la vez. Poseen un solo hilo de control que realiza tres pasos para establecer una conexión:

- I. Acepta una conexión.
- II. Lee la petición.
- III. Lee desde el archivo y escribe en el socket hasta encontrar el fin de archivo.

Las principales desventajas de este servidor son:

- El problema es que todo cliente debe esperar su turno para ser atendido.
- Si uno de ellos pide un archivo muy grande los demás tienen que esperar.
- La mayor parte de espera es debido a las operaciones de entrada y salida, hay capacidad de CPU desperdiciada.

b) Servidores concurrentes

Este servidor atiende múltiples clientes al mismo tiempo y en forma segura. Mientras está atendiendo sigue escuchando. Crear un nuevo proceso o línea de ejecución cada vez que un cliente llega a solicitar un servicio.

Las principales ventajas de este servidor son:

- 1) Poseen un hilo que espera por conexiones y crea un hilo ante la llegada de un nuevo cliente.
- 2) Este hilo se hace cargo de los requerimientos del cliente y luego termina (exit) cuando el cliente se va.
- 3) Requiere una capacidad de ejecución de tareas concurrentes.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

vi. Demonios (Daemon)

Es un tipo especial de proceso que se ejecuta de forma:

- a) Continúa (infinitamente) y transparente para el usuario.
- b) Simultánea con otros procesos por tal motivo se puede encontrar en sistemas multitarea.
- c) No dispone de una interfaz directa con un humano ya sea gráfica o textual.
- d) No hace uso de las entradas y salidas estándar para comunicar errores o registrar su funcionamiento.
- e) Por el contrario usan archivos del sistema en zonas especiales (/var/log/) o utiliza otros demonios especializados en dicho registro como el syslogd.

Los usos más importantes de este proceso son:

- a) Los demonios cronológicos realizan mantenimiento del sistema en segundo plano.
- b) El proceso de un sistema de protección en tiempo real de un antivirus.
- c) El proceso de protección de un firewall de capa de red/aplicación.

vii. Hilos (Threads)

Es un flujo secuencial de control dentro de un programa con una secuencia de instrucciones en ejecución.

El concepto de hilo puede ser muy similar al de un proceso, con la excepción de que múltiples hilos pueden ejecutarse dentro del mismo proceso compartiendo los datos y el código de programa.

La mayoría de los programas tienen un único hilo, por lo cual solo existe un único camino de ejecución en el programa, tiene un inicio que realiza una serie de cálculos y se finaliza.

Las principales ventajas de los hilos son:

- a) Un hilo es un proceso ligero (muy rápido y económico).
- b) Generalmente un proceso (padre) genera diversos hilos (procesos hijos), formando así un árbol de procesos.
- c) Los programas multihilo pueden tener varios flujos de control en diferentes partes del código ejecutándose simultáneamente.

CAPÍTULO 5 INTRODUCCIÓN A LA ARQUITECTURA CLIENTE/SERVIDOR

- d) Un hilo demonio es un hilo de baja prioridad que consta de un bucle infinito y se suele utilizar para prestar servicios cuando se necesite (refresco de memoria, mostrar imágenes, etcétera).

viii. Procesos

Es cualquier secuencia de operaciones que se está ejecutándose en memoria activa, realizando una o varias instrucciones sobre ciertos datos. Los procesos pueden ser concurrentes o paralelos

a) Procesos concurrentes

Cada proceso representa un programa secuencial que ejecuta una serie de instrucciones. Al ejecutarse un programa secuencial, éste sigue un solo hilo de control que inicia con una operación indivisible del proceso y se mueve a través del proceso conforme las operaciones se van ejecutando.

La ejecución de un programa concurrente resulta del seguimiento de múltiples hilos de control que se comunican entre sí. Los procesos cooperan entre sí utilizando una forma de comunicación que se puede lograr mediante el uso de memoria compartida o paso de mensajes. Los procesos se pueden dividir en:

- I. *Procesos disjuntos*: Se ejecutan en diferentes bloques del programa sin posibilidad de accederse entre sí. Ambos inician su ejecución simultáneamente y proceden concurrentemente hasta que terminan.
- II. *Procesos cooperativos*: Pueden comunicarse entre sí en la realización de una tarea, compartiendo recursos en común por lo que requieren una sincronización.

b) Procesos paralelo

Es paralelo o distribuido aquel que se forma por varios procesos secuenciales que se ejecutan en varios procesadores conectados entre sí. Si la red se forma por conexiones dentro de una sola computadora se considera un esquema de programación paralela pero si la red se forma por conexiones entre diferentes computadoras se considera un esquema de programación distribuida.

CAPÍTULO 6

DEFENSA EN REDES



Con el paso del tiempo, la tecnología informática ha ido evolucionando al desarrollar servicios que se utilizan a través de Internet conocida como la computación en la nube, este tipo de interconexión se hace a nivel mundial; por lo tanto, los datos más sensibles pasan por la red y cualquier persona puede capturarlos con el fin de obtener información valiosa de la empresa u organización; por lo que, da una oportunidad a delincuentes informáticos de explotar estas vulnerabilidades.

El gobierno de cada país y las empresas más importantes a nivel mundial comparten sus datos en las redes informáticas y de comunicaciones. Las empresas que tienen más de 500 empleados son los más propensos a tener una violación de seguridad informática que les costaría reparar entre 4 a 5 millones de dólares, por lo tanto es necesario asegurar todos los datos e implementar barreras en la red informática para garantizar una seguridad dinámica y proteger a los activos vitales.

En los últimos años, la cantidad de ataques informáticos ha aumentado considerablemente y causado serios daños, todos los países y las empresas que administran datos sensibles en red han desarrollado diferentes mecanismos para defender las redes informáticas que se basan en tecnologías y procesos como:

- ✓ Seguridad en redes inalámbricas
- ✓ Detección de intrusos
- ✓ Auditoría de red
- ✓ Análisis forense
- ✓ Impacto social y económico de la seguridad informática
- ✓ Nuevas tendencias y tecnologías

6.1 SEGURIDAD EN REDES INALÁMBRICAS

Una red inalámbrica permite a los usuarios conectarse a una red local o a Internet sin estar conectado por medio de cables ya que los datos (paquetes de información) se transmiten por el aire mediante ondas de radio, tienen la facilidad o desventaja de que cualquier persona con una computadora portátil o un smartphone (teléfono inteligente) puede encontrarla fácilmente y en ocasiones lograr acceder a ella.

Si una red inalámbrica está bien configurada se puede tener confianza al enviar información confidencial. Los principales puntos a tomar en cuenta al momento de configurarla son:

- a) Cambiar las claves por defecto cuando se instala el software del punto de acceso.
- b) Control de acceso seguro con autenticación bidireccional.
- c) Control y filtrado de direcciones MAC e identificadores de red para restringir a los adaptadores y puntos de acceso que se puedan conectar.
- d) Configuración del método de cifrado de paquetes, esta codificación puede depender del tamaño de la clave y su nivel de seguridad. Es recomendable que el cifrado sea mayor a 128 bits.
- e) Utilizar equipos que solo sean compatibles con los miembros que usan la red por si un intruso intenta entrar y tenga que trabajar con un modelo compatible al usado.
- f) Usar un radio de transmisión o extensión de cobertura para que se pueda controlar la transmisión de red y así conseguir un nivel de seguridad alto.

Las inseguridades de las redes inalámbricas radican en:

- a) La configuración del servidor.
- b) Usar la encriptación WEP.

Los datos son transmitidos de la misma manera con la que se reciben las ondas de televisión o radio, si alguien tiene un receptor puede ver los datos o si quiere puede alterar los sistemas de transmisión (figura 6.1).

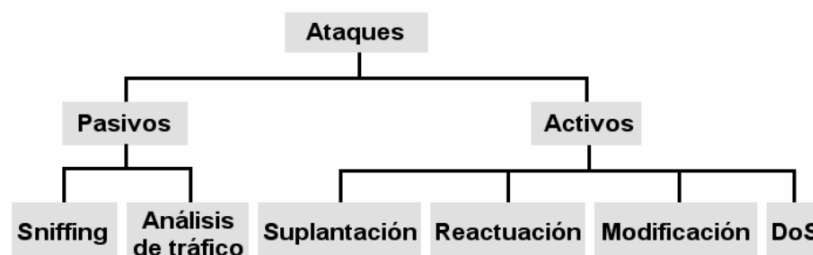


Figura 6.1 Principales ataques a una red inalámbrica

Las ventajas de las redes inalámbricas son:

- a) Se instala fácilmente ya que no usa nodos, lo que conlleva cables, canaletas, perforaciones ductos, etcétera.
- b) Suelen ser más baratas.
- c) Permite gran movilidad dentro del alcance de la red ya que tienen hasta 100 metros desde la base transmisora.

Las desventajas de las redes inalámbricas son:

- a) El ancho de banda se divide entre todos los usuarios que se encuentren dentro de la red, lo que afecta el rendimiento.
- b) Es más susceptible a ataques por la red.
- c) Es más fácil obtener la contraseña de acceso a Internet o información confidencial.
- d) Personas ajenas a la red podrían recibir la señal y robarla.

6.1.1 ACCESS POINT (PUNTO DE ACCESO)⁶

Es un dispositivo utilizado en redes inalámbricas de área local para interconectar computadoras relativamente cercanas sin la necesidad de cables, estas redes funcionan a base de ondas de radio. El access point es un transmisor y receptor central que hace la función de puerta de entrada a la red inalámbrica en un lugar específico y tiene una cobertura de radio determinada para cualquier dispositivo que solicite acceder siempre y cuando esté configurado y tenga los permisos necesarios.

Una red inalámbrica puede tener doble función, la cual es de interconectar computadoras y dispositivos cercanos entre sí y la segunda es la de proveer el servicio de Internet a todos los dispositivos.

El servidor tiene su propio sistema operativo al igual que los usuarios que van a acceder a la red local, estos sistemas operativos siempre son incompatibles entre sí, por lo que el access point tiene una función llamada bridge o puente en la que evita que se interrumpa la comunicación al permitir que los dispositivos trabajen aunque tengan diferentes plataformas, siendo cada una la encargada de interpretar los datos recibidos. Permite evaluar y filtrar la información así como descongestionar las redes al dividir las en subredes y enviando la información de manera paralela y más veloz.

⁶ Para mayor información véase el apéndice C

6.1. II SSID (SERVICE SET IDENTIFIER, IDENTIFICADOR DE CONJUNTO DE SERVICIOS)

Es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para que se puedan identificar como parte de esta red. Este código tiene un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID; cuando hay diferentes SSID en un mismo espacio físico esto permite que existan diferentes WLAN en el mismo lugar compartiendo diferentes servicios, por lo general el SSID se le conoce como el nombre que tiene la red (figura 6.2).

El SSID debe ser idéntico en el punto de acceso inalámbrico y en el adaptador de red a fin de permitir el acceso a la misma. Una red que utiliza el modelo ad-hoc (cada nodo reenvía datos a los demás) consiste en usar una máquina que va a ser el cliente sin que tenga un punto de acceso ya que usa el BSSID (Basic Service Set Identifier, Identificador básico de conjunto de servicios) para hacer la conexión. En las redes con infraestructura que tienen un punto de acceso se usa el ESSID (Extended Service Set Identifier, Identificador de conjunto de servicios extendido).

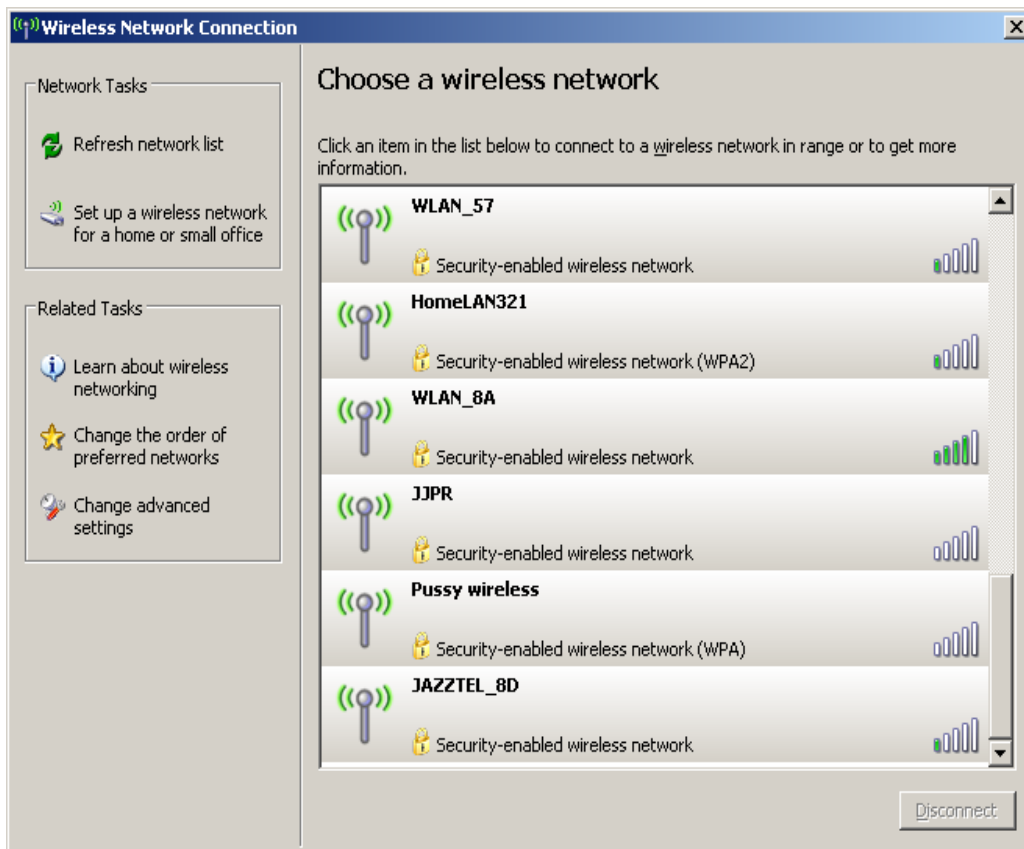


Figura 6.2 Nombres que puede tener un SSID

6.1. III WEP (WIRED EQUIVALENT PRIVACY, PRIVACIDAD EQUIVALENTE AL CABLE)⁷

Es un algoritmo de seguridad que brinda protección a las redes inalámbricas, se incluyó en la primera versión del estándar IEEE 802.11 y no ha tenido cambios en las nuevas versiones (802.11a y 802.11b) con el fin de garantizar la compatibilidad entre los distintos fabricantes. WEP es un sistema de cifrado estándar implementado en la MAC, se utiliza como una solución rápida en las redes inalámbricas aunque no es compatible con el protocolo IPSec.

El estándar 802.11 en redes WLAN usa un mecanismo de seguridad por medio de autenticación y cifrado llamado WEP que intenta conseguir un nivel de seguridad similar al de las redes cableadas empleando el algoritmo RC4 para cifrar las transmisiones que se realizan a través del aire con el propósito de evitar que usuarios no autorizados puedan acceder a la red. WEP utiliza una clave secreta que es compartida entre el dispositivo inalámbrico y el punto de acceso, así todos los datos que son enviados y recibidos entre el dispositivo y el punto de acceso pueden ser cifrados utilizando esta clave compartida.

Existen 2 maneras de autenticación:

- a) Sistema abierto: Todos los usuarios tienen permiso para acceder a la WLAN.
- b) Clave compartida: Controla el acceso a la WLAN y evita que los usuarios no autorizados accedan a la red.

Al elegir la autenticación por clave compartida se evita que un intruso se conecte al sistema y que envíe, reciba, altere o falsifique los mensajes dentro de la red.

Las principales ventajas de la WEP:

- a) Proporciona confidencialidad, autenticación y control de acceso en redes WLAN.
- b) Tiene la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits), al usar la clave de 128 bits se le conoce como WEP2.
- c) Se puede usar en modo dinámico para incorporar los mecanismos de distribución automática de claves y de autenticación de usuarios mediante 802.1x/EAP/RADIUS.

⁷ Para mayor información véase el apéndice C

Las principales desventajas de la WEP:

- a) Utiliza la misma clave simétrica y estática en las estaciones y del punto de acceso.
- b) Se tiene que escribir manualmente la clave en cada uno de los elementos de red.
- c) Al usar WEP2 no se resuelven los problemas de WEP porque se basa en el algoritmo RC4 que aún mantiene las mismas vulnerabilidades.
- d) El cifrado WEP llega a reducir el ancho de banda utilizable.
- e) Existen diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP.

El protocolo WEP no debe ser la única herramienta o política para asegurar la confidencialidad e integridad de los datos, se deben emplear más alternativas complementarias, como el uso de VPNs (Redes Privadas Virtuales), WPA y WPA2 (IEEE 802.11i) que son los sucesores de WEP o cualquier otro método de cifrado que se adapte al tipo de seguridad que se requiera dar.

6.1.IV RADIUS AUTHENTICATION (REMOTE AUTHENTICATION DIAL IN USER SERVICE, AUTENTICACIÓN REMOTA TELEFÓNICA DE SERVICIO DE USUARIO)

Es un protocolo de autenticación utilizado por el estándar de seguridad 802.11X, inicialmente no fue creado para ser un método de seguridad en redes inalámbricas, pero este protocolo mejora el estándar de cifrado WEP junto con los métodos de seguridad como EAP (Extensible Authentication Protocol, Protocolo de autenticación extensible) o PEAP (Protected Extensible Authentication Protocol, Protocolo de autenticación extensible protegido).

Además, es conocido como AAA (Autenticación, Autorización y Administración) para aplicaciones que requieren de acceso a redes o movilidad IP que deseen tener una excelente seguridad. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Para que el acceso a la red sea permitido, los datos son enviados primero al dispositivo NAS (Network Access Server, Servidor de Acceso de Red) usando el protocolo PPP (Point-to-point Protocol, Protocolo punto a punto), quien redirige la petición por medio del protocolo RADIUS a un servidor radius. El servidor radius verifica que la información sea correcta usando alguno de los protocolos del esquema de autenticación como puede ser PAP (Password Authentication Protocol, Protocolo de autenticación), CHAP (Challenge Handshake Authentication Protocol, Protocolo de autenticación por desafío mutuo) o EAP (Extensible Authentication Protocol, Protocolo de autenticación extensible). Si es

aceptada, el servidor autorizará el acceso al sistema del ISP y le asignará una dirección IP y todos los recursos de red que necesite.

Una característica importante del protocolo RADIUS es la capacidad de manejar sesiones, notificar cuando comienza y termina una conexión, ver el total de paquetes transferidos, determinar el tiempo que el usuario usó el servicio y facturarle este consumo, los datos que guarda se pueden utilizar con propósitos estadísticos.

En la actualidad existen muchos servidores radius que son de código abierto o usan el hecho por el fabricante. La gestión de los usuarios se puede hacer en archivos de texto, es muy común que se utilice SNMP para monitorear remotamente el servicio. Los servidores proxy radius se usan para la administración centralizada ya que pueden reescribir paquetes en el momento.

6.1.V 802.11(X)⁸

Debido a las carencias del estándar 802.11 ha sido necesario establecer una nueva normatividad que permita la autenticación y el intercambio dinámico de contraseñas de forma fácil y segura.

La seguridad es una parte fundamental de este estándar, con la familia 802.11i, c, f y j son servicios y extensiones que tienen un uso específico. Para la seguridad informática los protocolos 802.11a, b, g, i e n son los más usados para transferir archivos en las redes locales, el control de acceso en estos estándares está compuesto por:

- a) Solicitante: Cliente WiFi.
- b) Autenticador: Generalmente el AP.
- c) Servidor de autenticación: Puede ser cualquier servidor, pero en este caso será RADIUS.

Los principales métodos de cifrado son:

- a) WEP: Fue diseñado con el fin de proteger los datos que se transmiten en una conexión inalámbrica, opera en la capa 2 del modelo OSI.
- b) WPA: Es un estándar que resuelve los problemas de WEP al mejorar el cifrado de los datos usando el protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de Clave Temporal) y ofrece un mecanismo de autenticación que cambia la clave

⁸ Para mayor información véase el apéndice C

compartida entre el punto de acceso y el cliente cada cierto tiempo para evitar ataques que puedan revelar la clave.

- c) WLAN VPN: Emplea tecnología de cifrado para crear un canal virtual privado sobre una red de uso público. Una VPN puede proteger una red inalámbrica debido a que funciona sobre cualquier tipo de hardware inalámbrico y supera las limitaciones de WEP.

La autenticación de este estándar está dada por:

- a) Sistema Abierto (Open System Authentication): Permite que cualquier cliente entre en la red al asociarse con cualquier punto de acceso que esté en la zona de cobertura.
- b) Autenticación por MAC: Consta de 2 partes, el que requiere autenticar y el verificador que comparten la clave de la función MAC y la mantienen en secreto, así cuando el verificador recibe el valor MAC puede revisar si este valor corresponde con el que se tiene.
- c) Autenticación por EAP: Mecanismo de autenticación arbitrario que valida las conexiones de acceso remoto.
- d) Autenticación por EAP-MD5: Mecanismo de autenticación por desafío mutuo de síntesis de mensaje basado en PPP, con la diferencia de que los desafíos y las respuestas se envían como mensajes EAP.

6.1.VI NUEVAS TECNOLOGÍAS DE SEGURIDAD⁹

Las nuevas tecnologías de seguridad de red protegen los activos contra el robo y el uso incorrecto de la información confidencial, ofreciendo una protección contra ataques maliciosos, virus y gusanos que circulan por Internet.

La seguridad en una red no se basa en un método concreto sino que utiliza un conjunto de barreras que defienden a la empresa de diferentes formas, si una solución llega a fallar habrá otra que protegerá a la empresa y a los datos. Las principales tecnologías de seguridad que se emplean son:

1. Ipv6

Es la versión 6 del protocolo de Internet IP que se encarga de dirigir y encaminar los paquetes en las redes; es conocido como el IP de siguiente generación o IPng. Esta nueva

⁹ Para mayor información véase el apéndice C

versión sustituye a IPv4 ya que éste tiene un límite de direcciones de red con lo cual impide el crecimiento de las redes. Las principales mejoras de IPv6 son: mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad.

Para que un dispositivo se conecte a la red se necesita de una dirección IP. Con IPv4 solo se dispone de 2^{32} posibles direcciones con una longitud de 32 bits y con IPv6 se dispone de 2^{128} posibles direcciones con una longitud de 128 bits.

Las principales características son:

- a) Infraestructura de direcciones, enrutamiento eficaz y jerárquica.
- b) Mejora de compatibilidad para calidad de servicio (QoS) y clase de servicio (CoS).
- c) Multicast en el envío de un mismo paquete a un grupo de receptores.
- d) Anycast en el envío de un paquete a un receptor dentro de un grupo.
- e) Mayor movilidad, posibilidad de conexión y desconexión de las computadoras en redes IPv6.
- f) Seguridad integrada con IPsec que permite una autenticación y cifrado del propio protocolo base.
- g) Capacidad de ampliación, calidad del servicio y velocidad.

2. Internet2

Internet2 o UCAID (University Corporation for Advanced Internet Development, Corporación Universitaria para el Desarrollo de Internet Avanzado) es un consorcio sin ánimo de lucro que desarrolla y utiliza avanzadas aplicaciones de red con tecnologías para propósitos educativos así como la transferencia de datos a alta velocidad. Su objetivo es facilitar y coordinar el desarrollo, despliegue, funcionamiento y transferencia tecnológica de servicios y aplicaciones de red avanzados con el fin de ampliar el liderazgo de los Estados Unidos de América en el campo de la investigación y de la educación superior, y acelerar la disponibilidad de nuevos servicios y aplicaciones en internet.

Además, dispone de un gran ancho de banda en las instituciones académicas que normalmente están interconectadas a 2 Mbps y que pasarán a 34 Mbps, conforme se vaya saturando este ancho de banda irá creciendo hasta llegar a los gigabytes por segundo.

La calidad en el servicio (QoS) va a estar proporcionada conforme lo requiere cada aplicación, mejora la calidad en la red, será más fiable, garantiza la transmisión de cierta cantidad de datos en un tiempo dado. Las características generales son:

- a) Ancho de banda dedicado.
- b) Mejora las características de pérdida.
- c) Administra la congestión de la red.

- d) Moldea el tráfico de la red.
- e) Fija prioridades de tráfico.

Las principales ventajas del Internet2 son:

- a) Posibilita el desarrollo de aplicaciones mucho más rápidas.
- b) Potencializa la utilización de bibliotecas digitales multimedia.
- c) Permite escanear, procesar y compartir imágenes con rapidez.
- d) Ofrece calidad y nitidez para la utilización de videoconferencias como medio de comunicación en tiempo real.
- e) Almacena y posibilita compartir gigantescas bases de datos de forma remota.

Las desventajas que tiene Internet2 son:

- a) No todos tienen acceso a esta red.
- b) Requiere equipos sofisticados y de redes avanzadas para funcionar.
- c) Las aplicaciones creadas para Internet2 no pueden funcionar en las computadoras de usuarios finales como cualquier otra aplicación.
- d) Existen muchas limitaciones de infraestructura que dificultan la estandarización y mayor difusión de Internet2 en instituciones educativas y organizaciones de investigación.

3. 802.16

Es un estándar inalámbrico metropolitano que permite la recepción de datos mediante microondas y la retransmisión mediante ondas de radio para facilitar el acceso en zonas pobladas o aisladas. Se conoce como IEEE-802.16.

Está regulado por WiMAX (Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas) que se encarga del desarrollo y control de la compatibilidad e interoperabilidad de los diferentes elementos que intervienen en una red (antena, router, switch, receptor, etcétera.).

Con WiMAX se pueden unir varias redes WiFi permitiendo crear redes de malla en las que se conectan dos puntos de acceso mediante el estándar 802.16, por medio de estos puntos de acceso se puede dar soporte a una red WiFi con el protocolo 802.11.

Las principales características de WiMAX son:

- a) Capa MAC con soporte de múltiples especificaciones físicas (PHY).
- b) Distancias de hasta 50 kilómetros (teórica).
- c) Velocidades de hasta 70 Mbps.

- d) Facilidades para añadir más canales.
- e) Anchos de banda configurables y no cerrados.
- f) Soporte nativo para calidad de servicio (QoS).

4. VoIP (Voice over Internet Protocol, Voz sobre el Protocolo de Internet o Telefonía IP)

VoIP usa el protocolo RTP (Real-Time Protocolo, Transporte en Tiempo Real) que define cómo las aplicaciones envían el audio de la comunicación en tiempo real.

Es una tecnología que permite transmitir voz a través de redes IP en forma de paquetes de datos, caracterizándose principalmente para poder hacer llamadas telefónicas a través del servicio que ya tiene contratado Internet. Las principales características son:

- a) Ahorra costos: Combina el tráfico de voz y datos dentro de la red.
- b) Estándares abiertos e Interoperabilidad: Las empresas y proveedores de servicios pueden comprar los equipos de diferentes fabricantes y eliminar la dependencia en las soluciones propietarias.
- c) Redes que integran voz y datos: Al concebir que la voz sea una aplicación IP el tráfico que se envía de voz y datos lo hace sobre la misma red existente.

Las ventajas que tiene VoIP son:

- a) Se puede tener más de una comunicación por la misma línea telefónica.
- b) Las llamadas entrantes se pueden canalizar a un teléfono especial de VoIP, sin importar en qué punto de la red está conectado.
- c) Los teléfonos VoIP se pueden integrar con los servicios ya existentes como video, mensajería, intercambio de datos, etcétera., en forma simultánea y con los usuarios que estén en línea.
- d) Se tiene comunicación desde cualquier lugar del mundo.

Las principales desventajas de la VoIP son:

- a) Al momento de transmitir puede tener retrasos, cortes y a veces pérdidas de información si los paquetes se llegan a ir por diferentes rutas o puede que no lleguen a su destino.
- b) Sin el protocolo RTP no se garantiza la correcta transmisión de los datos.

6.2 DETECCIÓN DE INTRUSOS

Mediante Internet la información viaja de manera fluida de un punto a otro transportando cualquier tipo de dato, en ocasiones llegan a ser datos personales o hasta financieros. Los perpetradores buscan objetivos vulnerables como los sistemas que no están actualizados, sistemas infectados con troyanos y redes ejecutando servicios inseguros. Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de seguridad que ha ocurrido una entrada ilegal para que puedan responder en tiempo real a la amenaza. Por este motivo se han diseñado los sistemas de detección de intrusos para que notifiquen al administrador de la red cualquier cambio.

6.2.1 SISTEMAS DETECTORES DE INTRUSOS (IDS)¹⁰

Es un proceso o dispositivo activo que analiza la actividad del sistema y de la red de entradas no autorizadas o actividades maliciosas. Además, detecta todas las anomalías en el sistema, pero éstas pueden llegar a variar ampliamente por eso se debe configurar dependiendo de lo que se quiera cuidar ya que el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a los recursos. También audita las configuraciones de la red, analiza el sistema para encontrar vulnerabilidades y revisa la integridad de los datos.

Existen muchos beneficios directos e incidentales al usar cualquier IDS, pero al entender cómo funcionan se dará la clave para determinar cuál será el tipo apropiado para incluirlo en una política de seguridad. Los IDS se pueden dividir en:

- a) *Basado en conocimiento*: Alerta a los administradores de seguridad antes de que ocurra una intrusión usando una base de datos de ataques comunes.
- b) *Comportamiento*: Hace un seguimiento de todos los recursos usados buscando cualquier anomalía, lo que es usualmente una señal positiva de actividad maliciosa.

Un IDS brinda diferentes servicios de manera independiente y escucha pasivamente la actividad registrando cualquier paquete externo como sospechoso, combina las herramientas del sistema estándar, revisa que la configuración no esté modificada al igual que ve el registro de manera detallada, al combinar estas herramientas con la intuición y la experiencia del administrador se puede crear un kit poderoso de detección de intrusos.

¹⁰ Para mayor información véase el apéndice C

Las principales desventajas de las IDS son:

- a) La implementación requiere de un conocimiento profundo del comportamiento de la red o sistema.
- b) Puede detectar falsos positivos que son tolerables.
- c) Puede detectar falsos negativos que son imperdonables.
- d) Es un mecanismo de seguridad complementario a los ya existentes (no puede reemplazar un firewall, router, etcétera.).
- e) Es un mecanismo de detección y no de prevención. Sin embargo, es importante para hacer una investigación de análisis forense (post mortem).

6.2.II FALSOS POSITIVOS

Es cuando el sistema de seguridad interpreta que algo (un programa, un código, una dirección web, etcétera.) es malicioso cuando no lo es. Este error es más frecuente en el software de antivirus ya que reportan que un archivo o área del sistema está infectada, cuando en realidad el objeto está limpio de virus.

Los falsos positivos pueden ser causados por dos cuestiones:

- a) Humanas: Cuando un miembro del laboratorio de la aplicación de seguridad clasifica algo en forma errónea.
- b) Automáticas: Cuando las reglas en las que se basa el sistema de seguridad no están desarrolladas correctamente y detectan más de lo que debería ser algo dañino.

Algunos ejemplos de falso positivo son:

- a) Compresor de ejecutables: Son usados para disminuir el tamaño de los archivos o hacerlos más difíciles de crackear, lamentablemente los creadores de virus también necesitan esas funciones, por lo que algunas compañías detectan por defecto a cualquier archivo empaquetado por esa aplicación.
- b) Heurística: Es la más usada en los antivirus para brindar a los usuarios una reacción inmediata ante las nuevas amenazas informáticas sin que éstas se encuentren en su base de datos. Lamentablemente la heurística no es perfecta y puede encontrar secciones de código malicioso en programas que no son maliciosos, esto puede causar un falso positivo.
- c) Cracks y keygens: Unos pueden contener malware real, pero otros no. La mayoría de los antivirus detectan a todo este tipo de software como una amenaza.

6.2. III FALSOS NEGATIVOS

Es un error de software que falla al momento de detectar un archivo o área del sistema que está realmente infectada. Esta falla se puede producir porque el antivirus empleado no contiene los microcódigos exactos del virus ya que en ocasiones no se encuentran en una misma y única cadena o se trata de una nueva variante de la especie. Hay veces en donde los métodos heurísticos no tienen una buena técnica de programación o al ser compilados no se haya probado lo suficiente, esta falla puede llegar a reportar falsos negativos.

También pueden ser interpretados como ataques reales considerados como actividades legítimas o irregularidades detectadas como actividad normal, etcétera. Por ejemplo, se tiene a las múltiples conexiones de una misma IP hacia un servidor web.

6.2.IV MÉTODOS DE DETECCIÓN DE INTRUSOS

Un administrador se encarga de la seguridad de un sistema informático al configurar correctamente un servidor e ir revisando las fallas o bugs que van surgiendo. Al realizar estas tareas existe la probabilidad del 85% de evitar que un hacker o intruso entre en el sistema y obtenga algún acceso no autorizado, en ocasiones el principal riesgo viene de los propios usuarios internos a la red ya que poseen el acceso al sistema y solo es cuestión de tiempo u ociosidad para ir buscando los errores y tener acceso a la información. Por este motivo, los métodos de detección de intrusos indican el orden en que deben imponerse los diferentes procesos que son necesarios para lograr un fin dado u obtener varios resultados, estos métodos se dividen en:

- a) Análisis de tráfico: Permite conocer cuánto ancho de banda consumen los enlaces LAN o de WAN/ADSL; previene y elimina los ataques; detecta, analiza y correlaciona el tráfico al identificar las amenazas de red. Cualquier analizador de tráfico de red puede capturar datos de cualquier adaptador Ethernet, establecer filtros, hacer búsquedas, ver el contenido de cada paquete y de qué protocolo se trata así como identificar el proceso que genera el tráfico cuando este proviene del equipo local.
- b) HIDS (HostIDS): Depende del éxito del intruso al momento de entrar a la red ya que generalmente dejará rastros de sus actividades en el equipo atacado o al instante de intentar adueñarse del mismo, con el propósito de llevar a cabo otras actividades. El HIDS intenta detectar estas modificaciones en el equipo afectado y hacer un reporte de las actividades.

- c) NIDS (NetworkIDS): Detecta, recoge y analiza todos los paquetes que pasan por el segmento de red en busca de posibles ataques. Su interfaz debe funcionar en modo promiscuo para ir capturando todo el tráfico, esta captura de paquetes se puede realizar desde cualquier medio y con cualquier protocolo, por lo general se usa TCP/IP. La captura se realiza antes de llegar a las computadoras por lo que este método suele ser un primer perímetro de defensa en la protección de una red.
- d) Nuevos métodos de detección: Se divide en dos partes, los cuales se enuncian a continuación.
 - 1. *Detección de anomalías*: Constantemente se monitorea el sistema para detectar cualquier cambio en los patrones de utilización o el comportamiento del mismo.
 - 2. *Detección de mal uso*: Consta en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico.

Los métodos más usados para la detección son los sistemas que tengan una alerta temprana como son Decoy, Honey, Tarpit, etcétera.

6.2.V IDENTIFICACIÓN DE ATAQUES

Un ataque informático consiste en aprovechar y descubrir las vulnerabilidades o debilidades en el software, hardware y en las personas que tienen acceso a la red con el fin de poder acceder a la misma y modificar o eliminar los archivos. Las principales maneras de tener acceso es realizando un ataque de tipo:

- a) Físico: Se puede realizar en la infraestructura de red, enfocándose en el hardware.
- b) Lógico: Consiste en descubrir las vulnerabilidades del software.
- c) WIFI: Se basa en poder engañar y suplantar las identidades y/o dispositivos que pertenecen a la red inalámbrica que se está atacando.
- d) Sniffer: Es un programa que captura las tramas de red, generalmente se usa para gestionar una red aunque también puede ser utilizado con fines maliciosos.

Para que un perpetrador pueda realizar cualquiera de los ataques anteriores, primero debe pasar por cinco etapas en las cuales irá recabando información antes de ejecutar el ataque:

- 1. Reconocimiento: Involucra el obtener información de una víctima potencial que puede ser una persona u organización, en esta fase se usan diferentes recursos de Internet como buscadores para recolectar datos del objetivo.

2. Exploración: La información obtenida en el paso anterior se usa para sondear el blanco y tratar de obtener información sobre el sistema de la víctima así como las posibles direcciones IP, nombres de hosts, datos de autenticación, etcétera.
3. Obtener acceso: En esta parte se comienza a materializar el ataque a través de la explotación de las vulnerabilidades y defectos del sistema que fueron descubiertos durante las fases de reconocimiento y exploración.
4. Mantener el acceso: Cuando el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.
5. Borrar huellas: Cuando el atacante logró obtener y mantener el acceso al sistema, éste intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado, así mismo buscará eliminar los archivos de registro (log) o alarmas del sistema de detección de intrusos (IDS).

Para evitar la identificación de ataques es necesario conocer las vulnerabilidades del sistema que se va a proteger para establecer el nivel de riesgo aceptable, se puede emplear un IDS como elemento de identificación de ataque al configurar las reglas apropiadas de detección acorde con el nivel de riesgo que se puede aceptar.

6.2.VI ANÁLISIS DEL TIEMPO DE RESPUESTA DE LOS IDS

Las unidades de respuesta de un sistema de detección se encargarán de iniciar acciones al momento en que se detecte un ataque o intrusión. Estas acciones de respuesta se pueden dividir en:

- a) Automáticas (respuesta activa): Tiene como objetivo actuar en contra de un ataque al intentar neutralizarlo en el momento en que es detectado o mientras la intrusión todavía está en curso. Este tipo de respuesta puede cancelar la conexión de red que originó un ataque o llevar un seguimiento que permitiría más adelante el análisis correspondiente. El principal problema de respuesta es que puede acabar en una denegación de servicio contra usuarios o en sistemas legítimos.
- b) Requiere interacción humana (respuesta pasiva): Se limita a lanzar una alarma para informar y describir el ataque detectado por el administrador del sistema. La mayoría de estos componentes de respuesta pasiva ofrecen distintas formas de hacer llegar la información al administrador, las más comunes son mediante: correo electrónico o utilizar mensajes SMS.

Con base en lo anterior, la mayoría de las empresas contratan especialistas que personalmente analicen los informes generados por el sistema de detección para determinar si es necesaria una respuesta ante algún aviso. Los sensores y las unidades de

respuesta se pueden clasificar en distintas categorías dependiendo de la manera en que actúan. Las dos principales categorías son:

- a) Unidades de respuesta basadas en equipo: Se encargan de actuar a nivel del sistema operativo (bloqueo de usuarios, finalización de procesos, etcétera).
- b) Unidades de respuesta basadas en red: Actúan a nivel de red cortando los intentos de conexión, filtrando direcciones sospechosas, etcétera.

6.3 AUDITORÍA DE RED

Se toman en cuenta diversos elementos internos como externos, analiza los distintos factores como son: puntos débiles y críticos, vulnerabilidades, realiza un análisis del espacio de IPS (Sistema de Prevención de Intrusos) de la empresa, verifica los servicios brindados y las posibles intrusiones, además de los ataques de denegación de servicio.

Es importante mantener las premisas fundamentales de la seguridad informática (integridad, confidencialidad y disponibilidad) ya que éstas deben estar garantizadas en todo momento para brindar un correcto funcionamiento de la red y de sus servicios hacia el usuario final.

Cuando se rompe una de las tres premisas y la seguridad en la información ha sido comprometida; debe dar paso a la ejecución del DRP (Disaster Recovery Plan, Plan de recuperación de desastres) o en menor medida hacer un análisis de la intrusión y restablecer los servicios.

Además de un análisis exhaustivo, se extraen conclusiones y recomendaciones de la información que se ha recabado, el cual es uno de los puntos más importantes a la hora de brindar un informe detallado al cliente donde se le indican las mejoras o hardening de la empresa.

6.3.1 CONCEPTO

La auditoría en red procura asegurar la administración de la misma a través de procedimientos y controles que permitan detectar el grado de confianza, satisfacción y desempeño que brinda a la organización. Para lo anterior se requieren de parámetros de

medición del desempeño de la red (gráficas, estadísticas, etcétera.), evaluación de controles y otros.

Entre las principales actividades que se realizan para auditar esta área se encuentran:

- a) Comparación de proyectos con la planeación de la auditoría.
- b) Concertar citas con el personal que debe ser entrevistado.
- c) Revisión del formulario correspondiente, así como su actualización de acuerdo con las necesidades de la organización.
- d) Elaboración de un borrador.
- e) Clasificación y almacenado de la información de soporte en dispositivos de almacenamiento seguro.
- f) Elaboración formal de conclusiones y recomendaciones finales.

La auditoría en red se está convirtiendo en una herramienta indispensable para el mantenimiento de la misma ya que revela información vital de la empresa, por ejemplo:

- a) Confirma la topología existente y la configuración de los dispositivos.
- b) Revela cualquier vulnerabilidad encontrada.

Al confirmar la topología y la configuración ésta proporciona a los administradores de TI la seguridad de que:

- a) La red está configurada para maximizar la eficacia y la seguridad.
- b) Todos los dispositivos conectados a la red están configurados apropiadamente para el mismo propósito.

Una auditoría integral de red revelará cualquier vulnerabilidad que impacte negativamente en el rendimiento o que entorpezca las operaciones. El software de auditoría de red identifica dispositivos, componentes que necesitan ser reemplazados y de cualquier actualización de software que falte.

El diagrama de red representa todos los componentes encontrados, mostrando todas las rutas de acceso disponibles en esa o cualquier otra red. La precisión del diagrama es crítica porque los cambios realizados deben ser reflejados en el diagrama general. Un buen software de auditoría de red asegurará que todas las rutas son escaneadas y explicadas sin importar el tamaño de la red o la localización de los dispositivos.

Una auditoría fomentará el conocimiento de la red recuperando información del hardware como memoria, procesadores, adaptadores gráficos, dispositivos de almacenamiento, detalles de placas base, impresoras y puertos en uso. También proporciona información sobre qué personas han accedido y las acciones que han realizado.

6.3.II HERRAMIENTAS DE AUDITORÍA

El trabajo de campo del auditor consiste en obtener toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para llevar a cabo lo anterior se debe comenzar solicitando el cumplimiento de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Sobre esta base, se estudia y analiza la documentación recibida, de tal modo que un análisis determine la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Algunos métodos, técnicas o herramientas de auditoría son:

- a) Entrevistas: El auditor comienza a relacionarse con el auditado y puede hacerlo de tres formas:
 1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
 2. Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
 3. Por medio de entrevistas en las que el auditor sigue un método preestablecido y busca finalidades concretas.
- b) Tunning: Es el conjunto de técnicas de observación y medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en general. Estas acciones deben ser diferentes a los controles habituales que realiza el personal técnico en sistemas. Este método posee una naturaleza más revisora, estableciendo previamente planes y programas de actuación según los síntomas observados.
- c) Optimización de los sistemas y subsistemas: Técnica que realiza acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la operatividad de los sistemas ni el plan crítico de producción diaria de explotación.
- d) Optimización: Cuando se instala una aplicación, normalmente está vacía al inicio y a medida que se va llenando, ésta se hace cada vez más lenta; porque todas las referencias a tablas es cada vez mayor junto a la información que se está moviendo. Entonces, se tiene que hacer un análisis de performance para optimizarla y así mejorar el rendimiento de dicha aplicación.

- e) *Checklist*: El auditor profesional es aquél que reelabora sus cuestionarios en función de los escenarios auditados. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior. El auditor conversará y hará preguntas normales, que en realidad servirán para el cumplimiento sistemático de sus cuestionarios (Checklists).

6.3.III MAPEO DE LA RED

Es una representación gráfica de todas las computadoras y dispositivos en una red que muestra cómo están conectados entre sí en una LAN. La utilidad que tiene es evitar que haya intrusión por parte de personas ajenas a la red. Al tener mapeada la red se sabe qué equipos se tienen y así se detecta fácilmente a los intrusos que se hayan agregado a sí mismos. También puede servir para acceder rápidamente a cualquier elemento de la red de forma rápida.

Muchas organizaciones crean mapas de red de su propio sistema. Estos mapas se pueden hacer manualmente con herramientas simples o mediante el uso de métodos que integran la detección automática de la red con el mapeo.

Además, existen servicios de mapeo destacados que permiten personalizar los mapas e incluir sus propias etiquetas y agregar elementos que no hayan sido descubiertos. El mapeo sofisticado se utiliza para ayudar a visualizar la red y comprender las relaciones entre los dispositivos finales y las capas de transporte que prestan servicio. Los elementos tales como cuellos de botella y root cause analysis (Administrador de análisis de causa) pueden ser más fáciles de detectar usando estas herramientas.

Existen tres técnicas principales utilizadas para el mapeo de la red:

- a) *Enfoques basados en SNMP*: Recupera los datos del MIB router y del switch con el fin de construir el mapa de la red.
- b) *Activos de sondeo*: Se basa en una serie de paquetes de sondeo como traceroute (trazo de ruta) con el fin de construir el mapa de la red.
- c) *Análisis de rutas*: Se basa en la información de los protocolos de enrutamiento para construir el mapa de la red.

6.3.IV MONITORES DE RED

Es una herramienta de diagnóstico que supervisa las redes de área local y proporciona una representación gráfica de las estadísticas. También ofrece información acerca del tráfico de la red que fluye hacia y desde el equipo donde está instalado. Al capturar la información y analizarla puede diagnosticar y solucionar diversos tipos de problemas relativos a la red. Además, recopila información que ayudará a mantener la red en pleno rendimiento, gracias a funciones que permite identificar patrones y solucionar problemas.

Los administradores de red pueden utilizar estas estadísticas para realizar tareas rutinarias de solución de problemas, como encontrar un servidor que no funciona o recibir un número desproporcionado de solicitudes de trabajo.

Otros ejemplos de uso de monitores de red son:

- a) Puede configurar desencadenadores para que el monitor de red inicie o detenga la captura de información cuando se cumpla una condición o un conjunto de condiciones.
- b) Se pueden especificar filtros para controlar la información que el monitor de red captura o muestra.

6.3.V AUDITORÍA A FIREWALLS

Antes de profundizar en el tema, se debe conocer en qué consiste un firewall (puerta de seguridad). El firewall permite que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización, adicionalmente a estos beneficios los firewalls reducen la carga del sistema en procesos de seguridad y facilitan la centralización de servicios (figura 6.3).

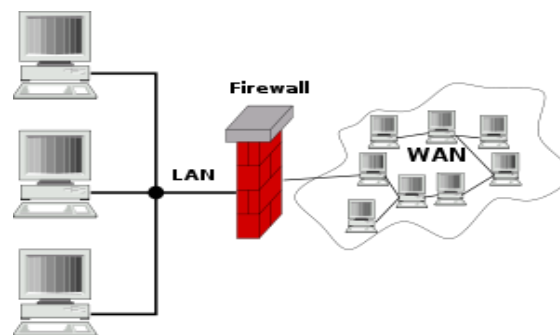


Figura 6.3 Esquema de una red de computadoras que utiliza un cortafuegos

Funcionalmente el firewall es un dispositivo lógico que tiene funciones de separación, limitación y análisis del flujo de la información que circula entre sus dos puertas, ejerce un control de acceso centralizado y su efectividad exige que lo atraviese todo usuario interno/externo/remoto para acceder desde/a las redes internas protegidas.

Los firewalls presentan las siguientes limitaciones:

- a) No protegen frente a desastres
- b) No protegen frente a virus
- c) No autentican el origen de los datos
- d) No garantizan la confidencialidad de los datos

La auditoría a este dispositivo analiza la configuración de firewall por las normas de seguridad de mapeo a las zonas en las que controlan el acceso y los servicios que lo permitan. Este análisis se lleva a cabo fuera de línea con la entrada que se proporcione:

- a) Configuración de firewall.
- b) Definición de las zonas: Proporciona un mecanismo simple para la definición de zonas en la red como la dirección MAC, DMZ y las redes inalámbricas.
- c) Lista de servicios que se deben permitir: Son aquellos que están dentro y fuera de la zona de red, DMZ y zonas inalámbricas.

Además, realizará procedimientos que determinan su arquitectura y combine medidas de control tanto a nivel de aplicación como a nivel de red.

Cuando se audita el firewall desde dentro y fuera de la red se obtiene una clara visión de cuál es la superficie de ataque. La entrega de los resultados puede ser de la siguiente manera:

- a) Informe sobre vulnerabilidades existentes.
- b) Referencia técnica sobre soluciones.
- c) Evaluación de las políticas de seguridad.
- d) Recomendaciones de mantenimiento de seguridad.

Una auditoría de logs de firewall recopila, analiza, informa y archiva los logs soportados por el firewall que pueden ser de utilidad durante las auditorías de red para cumplir con las normas regulatorias. Con estos registros almacenados y utilizando los logs archivados, se puede realizar un análisis histórico de tendencias durante las auditorías y se podrá configurar el período de tiempo durante el cual se necesita almacenar o archivar los archivos logs.

6.3.VI PRUEBAS DE PENETRACIÓN SOBRE REDES

También llamado hackeo ético es una evaluación activa de las medidas de seguridad de la información. En los entornos de red complejos la exposición potencial al riesgo es cada vez mayor y proteger los sistemas se convierte en un auténtico reto. Además, está dirigido a la búsqueda de agujeros de seguridad en uno o varios recursos críticos, como puede ser el firewall o el servidor web.

A través de la prueba de penetración es posible detectar el nivel de seguridad interno y externo de los sistemas de información de la organización, determinando el grado de acceso que tendría un atacante con intenciones maliciosas. Además, el servicio revisa las vulnerabilidades que pueden ser vistas y explotadas por individuos no autorizados, agentes de información, ladrones, antiguos empleados, competidores, etcétera.

Otra cuestión, es que deben incluir pruebas de la capa de aplicación y de red, además de los controles, los procesos de las redes y las aplicaciones; en la cual, deben realizarse tanto del exterior de la red (pruebas externas) como desde el interior de la red (pruebas internas).

Los servicios de pruebas de penetración permiten:

- a) Evaluar vulnerabilidades por medio de la identificación de debilidades de configuración que puedan ser explotadas.
- b) Analizar y categorizar las debilidades explotables basadas en el impacto potencial y posibilidad de ocurrencia.
- c) Proveer recomendaciones mediante prioridad para mitigar y eliminar las debilidades.

Los tipos de pruebas de penetración que se efectúan son:

- a) Ataques del entorno: El software no se ejecuta aislado. Depende de cualquier número de archivos binarios y módulos de código equivalente, como scripts y complementos. Puede usar también información de configuración del registro o del sistema de archivos, así como de bases de datos y de servicios que podrían residir en cualquier parte.
- b) Ataques de entrada: Procede de fuentes que no son de confianza. Éstas incluyen rutas de comunicación como, por ejemplo, protocolos de red y sockets, funcionalidades remotas expuestas como DCOM, llamadas a procedimiento remoto (RPC, Remote Procedure Calls) y servicios web, archivos de datos (binarios o de texto), archivos temporales creados durante la ejecución y archivos de control como scripts y archivos XML los cuales están sujetos a manipulaciones.

- c) *Ataques de datos y de lógica*: Son errores que se encuentran incrustados en los mecanismos internos de almacenamiento de datos de la aplicación y en la lógica de algoritmos.

6.3.VII ANÁLISIS DE LA INFORMACIÓN Y RESULTADOS

Es un estudio general donde se indica qué computadoras estuvieron comprometidas en un ataque así como sus características; éstas usualmente vienen en la introducción del informe. Para elaborar el informe es necesario hacer un análisis descriptivo donde se plantean y responden ciertas preguntas como son dónde, cómo, y quién recolectó la información, esto implica que se tiene que revisar la información, identificar vínculos, patrones y temas comunes, ordenar los hechos y presentarlos como fueron sucediendo sin agregar ningún comentario. Se presenta en un informe que lleva el mismo nombre y puede ordenarse de manera cronológica (según la secuencia de los hechos) o jerárquica (según la importancia de los temas).

Las etapas principales en el análisis e interpretación de la información son:

- a) *Análisis descriptivo*: Incluye suficientes detalles que permitan al lector saber qué pasos siguieron en la investigación, cómo llegó a tomar esa decisión metodológica o cómo cambió la dirección y por qué. Los hechos se tienen que presentar de manera clara, coherente y completa antes de ser interpretados.
- b) *Interpretación*: Consiste en determinar el significado de los resultados y cuán significativos son respecto a su contexto específico, esta interpretación debe reflejar los comentarios, sugerencias, métodos, herramientas analíticas y de investigación.
- c) *Juicio*: Las dos etapas anteriores permiten evaluar los resultados como positivo o negativo, es importante lograr tener un equilibrio justo entre ambos aspectos para que los resultados positivos se recalquen sin dejar de lado los negativos y de la misma manera los resultados negativos se deben poder discutir de modo que se exploren todas las posibles soluciones prácticas o remedios factibles.
- d) *Recomendaciones*: En esta parte se generan varias acciones para las etapas anteriores, entre más personas participen en esta etapa más fácil será hacer una lista de posibles sugerencias o acciones para llevar a cabo en un determinado caso.

Cuando se hayan concluido las etapas anteriores, se tendrá suficiente información almacenada en bitácora, archivos e índices organizada cronológicamente para tomar la mejor decisión posible ante un determinado suceso.

6.3. VIII DOCUMENTACIÓN REFERIDA DEL CASO

Es un registro donde se detallan todos los problemas que sucedieron con el servidor o la computadora afectada; además, se usa en las auditorías de red ya que todos los problemas están contenidos en el reporte del auditor. Esta documentación facilita la planeación, diseño, supervisión y revisión de la calidad del trabajo que provee la persona que auditó a la empresa. El informe que es entregado a la empresa puede ser revisado por el administrador de la red para que examine la documentación escrita de las evidencias de la auditoría (incluye los registros de la planeación, el desempeño del trabajo, los procedimientos ejecutados, evidencia obtenida y las conclusiones a las cuales llegó el auditor).

A la documentación de auditoría también se le puede llamar papeles de trabajo o documentos de trabajo y es revisada por el personal encargado de la organización con la finalidad de que se familiaricen con los siguientes puntos:

- a) Los auditores nuevos primero revisan la documentación del año anterior para entender el trabajo que se realizó y cómo ayuda a planear y ejecutar el compromiso actual.
- b) El personal de supervisión revisa la documentación preparada por los asistentes.
- c) Los supervisores y revisores leen la documentación para entender cómo el equipo alcanzó las metas y planteó las conclusiones importantes basándose en las evidencias que se tienen.
- d) El auditor sucesor revisa la documentación de la auditoría que realizó el auditor predecesor.
- e) Equipo de inspección, internos y externos, revisan la documentación para valorar la calidad de la auditoría y el cumplimiento con los estándares de la práctica profesional de la auditoría y relacionados; las leyes, reglas y regulaciones aplicables; y las políticas de control de calidad del auditor.

6.3.IX LOG DE SEGURIDAD

Es un registro oficial de eventos durante un rango de tiempo en particular, los encargados en seguridad informática usan estos registros de datos para saber quién, qué, cuándo, dónde y por qué ocurrió un evento en un dispositivo en particular o aplicación; la palabra log es equivalente a bitácora en español.

Los logs son almacenados o desplegados en un formato estándar, el cual tiene un conjunto de caracteres para dispositivos comunes y aplicaciones, así cada log que fue generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.

Un log es una evidencia digital construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales, si se revisan las salidas de estos archivos se pueden determinar los eventos que han sucedido para tomar la acción necesaria y poder corregir el problema o iniciar una investigación en caso de un incidente de seguridad.

La mejor manera de almacenar un log es guardarlo en dispositivos de almacenamiento para que los datos permanezcan incorruptibles (CD-R y DVD-R) a lo largo del tiempo. Deben guardarse en modo de solo lectura para no sufrir modificación y posea una protección adecuada. Se puede usar también el cifrado de datos cuando el log de seguridad tiene datos que son muy sensibles o valiosos para la empresa.

El administrador puede encargarse de los logs usando la herramienta Syslog, la cual captura y administra los logs generados por el sistema sin ir preguntando o dando algún aviso y utiliza un demonio para llevarlo a cabo.

6.4 ANÁLISIS FORENSE

Aunque existen barreras de protección establecidas para salvaguardar los activos de información, los incidentes de seguridad se seguirán produciendo; es fundamental reaccionar ante un ataque, por ello una de las fases más importantes es la respuesta a incidentes que consiste en la investigación del mismo para saber por qué se produjo la intrusión, quién la perpetró y qué sistemas afectó. Esta investigación se conoce como análisis forense.

Así, esta disciplina no solo hace uso de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia informática o en sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El poder mantener su integridad se basa en que la evidencia digital o electrónica es sumamente frágil.

6.4.1 INTRODUCCIÓN

El análisis forense o también llamado cómputo forense permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales y autenticarlos, explicar las características técnicas del uso aplicado a los datos y bienes informáticos. Sus objetivos son los siguientes:

- a) Recrear qué ha ocurrido en un dispositivo digital.
- b) Analizar y esquematizar las incidencias de forma que se impida la repetición de la misma en el futuro.
- c) Disposición y procesamiento judicial en pruebas incriminatorias.

Además, comprende dos fases: la primera, la captura de las evidencias y su protección; la segunda, el análisis de las mismas. Sin embargo, los crímenes digitales resultan difíciles porque no pueden ofrecer respuestas a las interrogantes, especialmente quién realizó el ataque; la investigación forense se centra en averiguar qué fue dañado, cómo fue dañado y cómo arreglarlo.

Durante la fase de recolección de evidencias se captura todo aquello que resulte susceptible a un posible análisis posterior y pueda arrojar evidencias de los detalles que incriminan a un delito.

El análisis de evidencia es la fase más extensa y delicada, ya que requiere poseer conocimientos avanzados para interpretar las pruebas incautadas, cuyo volumen puede llegar a ser inmenso. Dependiendo de la calidad de los datos de registro de actividad se podrá realizar de forma sencilla el análisis de la evidencia. Igualmente, dependiendo de la información existente se procederá a obtener resultados. Así, los principales principios del análisis forense son:

- a) Evitar la contaminación.
- b) Actuar metódicamente.
- c) Controlar la cadena de evidencias.

Los principales pasos para realizar un análisis forense son:

- a) Estudio preliminar.
- b) Adquisición de datos.
- c) Recuperación en caso de avería o sabotaje y de datos ocultos o borrados.
- d) Análisis de evidencias.
- e) Generación de informes.
- f) Presentación de las pruebas.

El proceso de análisis forense a una computadora se describe de la siguiente manera:

1. Identificación

Se deben conocer los antecedentes, situación actual y el proceso que se quiere seguir para tomar la mejor decisión con respecto a las búsquedas y estrategias de investigación. Incluye la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

2. Preservación

Incluye la revisión y generación de las imágenes forenses de la evidencia para realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para mantener la integridad de la evidencia y la cadena de custodia que se requiere. Realizar una imagen forense se refiere al proceso que se requiere para generar una copia *bit-a-bit* de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro.

3. Análisis

Aplica técnicas científicas y analíticas a los datos duplicados por medio del proceso forense para encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca y modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etcétera.

4. Presentación

Recopila toda la información obtenida a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

Algunos conceptos fundamentales que deben tratarse en el análisis forense son:

- a) Cadena de custodia: Es la identidad de las personas que manejan la evidencia en el tiempo del suceso y de la última revisión del caso (fechas de entrega y recepción). Es responsabilidad de la persona asegurar que los artículos son registrados y contabilizados durante el tiempo en el cual están en su poder y que son protegidos.

- b) *Imagen forense*: Llamada también espejo. Es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos, áreas borradas incluyendo particiones escondidas.
- c) *Análisis de archivo*: Examina cada archivo digital descubierto y crea una base de datos de información relacionada al archivo (metadatos), consiste en la firma del archivo o hash (indica la integridad del archivo), autor, tamaño, nombre y ruta, así como su creación, último acceso y fecha de modificación.

Las dificultades que presenta el investigador forense son las siguientes:

- a) Conflicto por conseguir las herramientas necesarias para obtener la evidencia.
- b) Existencia de averías y sabotajes en los soportes de almacenamiento.
- c) Técnicas anti forense, ocultación de datos, claves y encriptación.
- d) Apoyo de externos para evitar una auditoría.
- e) Tener problemas al realizar un informe ágil.
- f) Bajo rendimiento al presentar y explicar los informes ante el órgano competente.

La desventaja que presenta el análisis forense es que no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello se encarga la seguridad informática. Es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

6.4.II OBTENCIÓN Y PROTECCIÓN DE LA EVIDENCIA

En esta fase, se procede a ejecutar los tres pasos mostrados en la figura 6.4 para adquirir la evidencia sin alterarla o dañarla. Se autentica que la información de la evidencia sea igual a la original.

Se deben definir los equipos y herramientas para llevar a cabo la investigación así como lograr un entorno de trabajo adecuado para su análisis. Además, se inicia una bitácora que permita documentar (de manera precisa), identificar y autenticar los datos que se recogen siendo del tipo:

- a) ¿Quién realiza la acción y por qué lo hicieron?
- b) ¿Qué estaban tratando de lograr?
- c) ¿Cómo se realiza la acción, incluidas las herramientas que utilizaban y los procedimientos que siguieron?
- d) Cuándo se realizó la acción (fecha y hora) y los resultados.

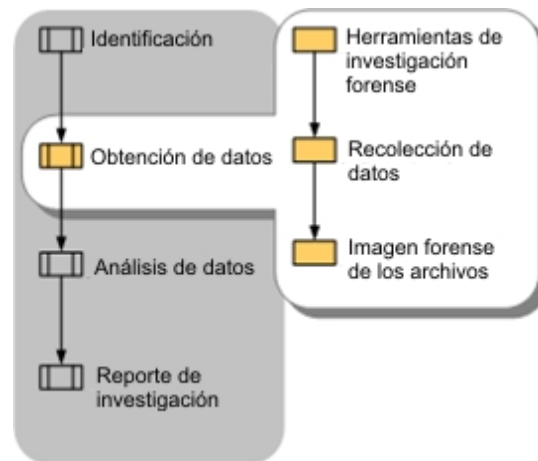


Figura 6.4 Fase de obtención y protección de datos

De igual forma, se toman en cuenta otras fuentes de información de los sistemas vivos como lo son los datos volátiles:

- a) Caché del sistema y archivos temporales.
- b) Registros de sucesos, internos y externos de los dispositivos de red, tales como firewalls, routers, servidores proxy, etcétera.
- c) Logs del sistema y aplicaciones.
- d) Tablas de enrutamiento (ARP, caché de Netbios, lista de procesos, información de la memoria y el kernel).
- e) Registros remotos e información de monitoreo relevante.

Además, se debe realizar una copia de la imagen de los dispositivos (bit a bit), con una herramienta apropiada y firmar su contenido con un hash de MD5 o SHA1, generando así el segundo original, a partir de éste se generarán las copias para el análisis de datos. Cada copia debe ser comprobada con firmas digitales nuevamente con MD5 o SHA1.

A continuación se documenta la evidencia con el registro de embalaje para garantizar que se incluye la información acerca de sus configuraciones (fabricante, modelo, interfaz, condición de la unidad y el tamaño del dispositivo). Para conservar la información y evidencia, se tienen los siguientes puntos:

- a) Tener un lugar para almacenar los datos, evitando así su manipulación. No se olvide de documentarlo.
- b) Proteger los equipos de almacenamiento de los campos magnéticos (estática).
- c) Realizar como mínimo una imagen del dispositivo original, de éste realizar otra copia para el análisis y posteriormente almacenarlo en un sitio seguro.
- d) Asegurar que la evidencia está protegida digitalmente y físicamente.
- e) Nuevamente, actualizar el documento de cadena de custodia.

6.4.III ANÁLISIS SOBRE EL SISTEMA

Este apartado se enfoca en tres pasos (figura 6.5) para llevar a cabo el análisis sobre el sistema.

1. Análisis de datos de la red: Se centra en identificar los dispositivos de comunicación y defensa perimetral (servidores web, firewall, IDS's, IPS's, proxys, filtros de contenido, analizadores de red, servidores de logs, etcétera.) que están en la red con la finalidad de recuperar los logs.
2. Análisis de los datos del host: Se logra con la información obtenida de los sistemas vivos, de la lectura de las aplicaciones y los sistemas operativos. Además, se limita a tratar de recuperar los archivos de la evidencia en procesos de recuperación de datos y definir criterios adecuados de búsqueda.
3. Análisis de los medios de almacenamiento: Se definen los criterios de búsqueda con objetivos claros, debido a la gran cantidad de información disponible, ya que puede desviar la atención o sencillamente complicar el proceso de análisis de la información. Se tienen en cuenta las siguientes buenas prácticas:
 - a) Utilizar la copia del segundo original, ésta a su vez hay que seguirla manteniendo en buen estado y continuar con la cadena de custodia.
 - b) Determinar si los archivos no tienen algún tipo de cifrado.
 - c) Verificar si el archivo comprimido está completo.
 - d) Crear una estructura de directorios e identificar y recuperar los archivos objetivo (aquellos que han sido afectados por el incidente).
 - e) Analizar archivos de inicio, registro del sistema, software instalado, actualizaciones y parches.
 - f) Llevar un registro de login (entrada) y logout (salida) del sistema, nombres de usuario e información del AD (Directorio Activo).
 - g) Estudia los metadatos (Identifica las marcas de tiempo, creación, actualización, acceso, modificación, etcétera.).

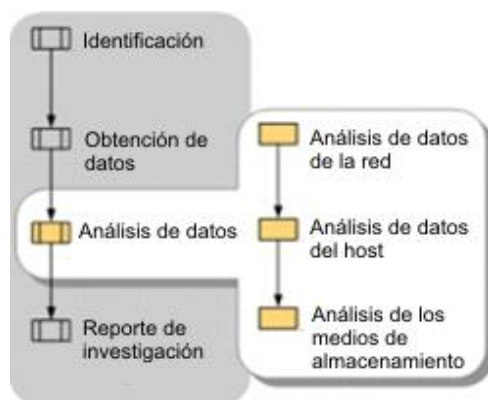


Figura 6.5 Fase de análisis de datos

6.4.IV HERRAMIENTAS PARA OBTENER INFORMACIÓN DE LA RED

En este punto se le dará un enfoque en seguridad informática donde se mencionan algunas herramientas forenses para el análisis en red, las cuales pueden ser:

- a) NetworkMiner: Su propósito es recolectar información (como evidencia forense) sobre los hosts en vez de recoger información concerniente al tráfico de la red. Es usado también como sniffer pasivo o herramienta de captura de paquetes con el objetivo de detectar detalles específicos del host (sistema operativo, nombre del host, sesiones, etcétera.) sin generar ningún tráfico en la red.
- b) Xplico: Mediante el archivo de tráfico de red obtenido, éste será capaz de extraer y clasificar por categorías la totalidad de datos de las aplicaciones intervinientes en la generación de la misma. Además, extrae datos en formato SQLite/MySQL, funciona en tiempo real, soporte IPv6 y modularidad (cada componente es en sí un módulo).
- c) NetIntercept: Captura paquetes enteros y reensambla casi todas las conexiones TCP directamente, reconstruyendo los archivos que circularon por la red y creando una base de datos sobre sus descubrimientos. Reconoce varios protocolos de red y tipos de archivos.
- d) TrueWitness: Vigila y monitorea la red desde un puesto externo. Sus características son: Identifica amenazas internas y externas en la red, captura paquetes en tiempo real, reconstruye sesiones de red convirtiendo los paquetes capturados en streams completos de datos, mantiene detalles para cada conexión TCP/IP y no produce impacto en la velocidad de la red.
- e) Tcpflow: Captura los datos transmitidos como parte de una conexión TCP y los almacena de forma conveniente para su depuración y análisis. Además, reconstruye los streams de datos actuales y almacena cada flujo en un archivo separado.
- f) Tcpextract: Extrae archivos de tráfico de red basándose en su estructura interna. Además, intercepta archivos transmitidos a través de la red. Sus características son: Tiene algoritmos de búsqueda eficiente y escalable, ya que buscan a través de los límites de los paquetes para una total cobertura y calidad forense.

6.4.V ANÁLISIS DE LA INFORMACIÓN Y RESULTADOS

Es la fase más delicada e importante (figura 6.6), la cual será el documento que sustentará una prueba en un proceso legal. Básicamente, debe tomar en cuenta dos pasos importantes:

1. Organización de la información

- a) Retoma toda la documentación generada en las fases de metodología; además, de cualquier información anexa (notas, antecedentes o informe de auditoría).
- b) En la investigación se identifica lo más importante y pertinente.
- c) Realiza conclusiones (teniendo en cuenta los hechos) y crea una lista de las pruebas para presentar en el informe.

2. Escribir el informe final

- a) Debe ser claro, conciso y escrito en un lenguaje no técnico (personas comunes).
- b) Contiene como mínimo:
 - i. Propósito del Informe: Explica el objetivo y el por qué se preparó el informe.
 - ii. Autor del informe: Todos los autores y co-autores, incluyendo sus posiciones, las responsabilidades durante la investigación y sus datos de contacto.
 - iii. Resumen de incidentes: Introduce el incidente y explica el impacto.
 - iv. Pruebas: Describe la evidencia en la forma en que fueron adquiriéndose durante la investigación.
 - v. Detalles: Describe la evidencia examinada, los métodos de análisis que se utilizaron, así como sus resultados y pruebas. Justifica cada conclusión generada y proporciona información sobre aquellos individuos que realizaron o participaron en la investigación.
 - vi. Conclusión: Resume los resultados de la investigación de forma clara y sin ambigüedades. Además, incluye una justificación junto con las pruebas y la documentación.
 - vii. Documentos justificativos: Incluye cualquier información referente al informe, tales como diagramas de red, documentos que describen los procedimientos de investigación, da un panorama general y crea un glosario de términos utilizados en el informe.

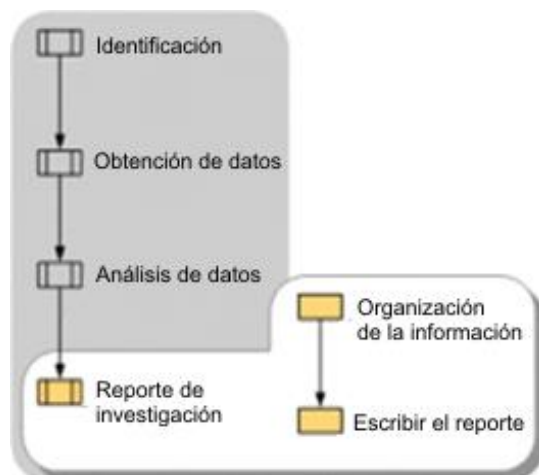


Figura 6.6. Reporte de la investigación forense

6.5 ENTORNO SOCIAL E IMPACTO ECONÓMICO DE LA SEGURIDAD INFORMÁTICA¹¹

El entorno social define a un individuo con determinadas condiciones de vida (trabajo, nivel educativo e ingresos) relacionado a los grupos a los que pertenece. El impacto social se refiere al cambio efectuado en la sociedad debido al producto de las investigaciones. Además, es la medida o grado en que la seguridad informática se ha involucrado en la sociedad, sus actividades, el nivel de acceso a la ciencia y tecnología por parte de los habitantes, los conocimientos que posee en cuanto a los equipos de cómputo y tecnologías.

Con respecto al impacto económico, se refiere a la inversión privada y gubernamental al proteger la información de las organizaciones así como el apoyo a las instituciones para llevar a cabo proyectos de adquisición tecnológica, la situación del empleo y sus remuneraciones.

Impacto social

La proliferación de los delitos informáticos ha hecho que la sociedad sea más escéptica de utilizar tecnologías de la información, las cuales pueden ser de gran beneficio para la sociedad en general. El grado de especialización técnica que adquieren los delincuentes para cometer este tipo de delitos depende de personas con conductas maliciosas donde

¹¹ Para mayor información véase el apéndice C

idean planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a global. Además, las empresas son más celosas y exigentes en la contratación del personal porque poseen importantes activos informáticos y puede afectar en forma positiva o negativa a la sociedad laboral.

Las personas que poseen conocimientos en informática no son vulnerables a ser víctimas de un delito como aquellos que no conocen nada del tema. La falta de cultura informática puede impedir a la sociedad luchar contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

Impacto económico

La tecnología informática es tan importante que se ha generalizado de manera espectacular generando ingresos altos a la economía mundial. Hoy en día, la informática está presente por medio de dispositivos inteligentes en cualquier oficina, negocio, bancos o prácticamente cualquier lugar en el que se maneje información.

Para conocer cuál es el impacto económico en la tecnología informática, se tiene que decir que la economía mundial ya no se concibe sin la informática. Todas las facetas de la economía de cualquier país están gestionadas por la seguridad informática.

En la economía actual, el desarrollo tecnológico es el que provoca el cambio y la reducción de costos. Dentro de la tecnología informática el campo que más ha impulsado a la economía mundial ha sido el de las redes de comunicación y de sus usos comerciales. Con la aparición de World Wide Web se desarrolló rápidamente Internet y mediante el desarrollo de las redes informáticas se empezó a preveer que el impacto económico será mayor en los próximos años. La utilización masiva de la informática traerá las siguientes consecuencias:

- a) Aumento de la productividad, inversión, salarios y tiempo libre.
- b) Incremento de puestos de trabajo en ciertas empresas.
- c) Indirectamente también se podrá tener una mejor gestión de las empresas como resultado de una mayor calidad de la información que manejan sus directivos al contar con sistemas eficientes.

En los últimos años la inseguridad en la red informática ha provocado serios problemas en la actual sociedad, como son: uso no autorizado de información u otro recurso, pérdidas monetarias, etcétera. Todos esos ataques son por motivos de dinero, de conflictos personales entre otras cosas. Existen diferentes métodos de ataques, como son: las actividades de copia, distribución o uso de programas informáticos realizadas infringiendo las normas legales que protegen los derechos de propiedad intelectual de sus autores, etcétera.

El crimen informático es un problema en expansión en el mundo actual. Entre las causas de estos problemas se encuentran:

- a) Carencia de educación en los internautas.
- b) Características del diseño de la red.
- c) Sistemas propietarios.

6.6 NUEVAS TENDENCIAS Y TECNOLOGÍAS

En la mayoría de los estudios se ha encontrado que el escaso conocimiento de los usuarios es la principal causa individual de las brechas de seguridad en los sistemas de información (redes). La problemática es más compleja por la falta de seguridad de la información ya que no plantean un programa de seguridad integral que proteja los recursos informáticos de las amenazas actuales. La tecnología no es el único aspecto clave en la seguridad y control de los sistemas de información pero ante la falta de políticas de administración, la mejor tecnología, incluso puede ser anulada.

La investigación así como la configuración de reglas permite fortalecer la seguridad de la información. Año con año surgen nuevos estándares, se actualizan los existentes, se fabrican más y de mejor tecnología encaminada a la protección de datos y a la reflexión de los rangos de disponibilidad de los servicios. La seguridad de la información, lejos de perder importancia, se vuelve cada vez más un aspecto fundamental en todos los ámbitos: en el intercambio de ideas y en los conocimientos en las relaciones de negocios.

La mayoría de las organizaciones están implementando y renovando sus procesos, la infraestructura de sus redes incorporan procedimientos de acceso en manejo de información cada vez más rigurosos.

6.6.1 CULTURA DE LA SEGURIDAD INFORMÁTICA

Es un elemento indispensable para el desarrollo de los países con menor desarrollo. Desde que los dispositivos inteligentes interactúan entre sí y acceden a Internet, los datos pueden ser vulnerables. Al disponer de buenos hábitos en el ciberespacio se debe volver tema fundamental en la vida cotidiana de toda persona; por ello, los expertos mencionan que la educación o cultura en seguridad informática tiene que surgir desde las escuelas hasta los puestos gubernamentales.

La seguridad informática es un tema que preocupa tanto al sector público como al privado, por lo tanto es de suma importancia que se siga generando conocimiento y material de ayuda e importancia tanto para las personas interesadas en el tema como para los expertos; de esta forma, se podrán seguir tendencias mundiales para combatir el cibercrimen y sobre todo para generar una cultura de seguridad. Los principales atrasos de las organizaciones en el ámbito de la seguridad informática son:

- a) Una cultura de seguridad poco extendida.
- b) Falta de capacitación tanto de los responsables de la seguridad de la información a nivel interno, como de algunos proveedores de soluciones relacionadas.
- c) Bajo nivel de conciencia entre directivos de las organizaciones.
- d) Carencia de presupuesto para incentivar la investigación tecnológica.
- e) Falta de una legislación clara y suficiente para la protección de datos personales.

En varios países está renuente en adoptar de forma inmediata nuevas tecnologías en seguridad informática derivado del rechazo a utilizarlas en el momento en que son puestos al mercado debido a que se etiquetan como modas.

Por lo general, se tiene la percepción de que las amenazas a la seguridad de la empresa provienen del exterior; no obstante, pueda serlo de manera interna. De ahí, que sea fundamental crear una cultura de seguridad para que los directivos y dueños, lo asuman como un factor clave en la competitividad y desarrollo de su labor cotidiana en el centro de trabajo.

La conciencia de seguridad se sigue incrementando pero este avance es más lento de lo deseable porque la seguridad de la información está íntimamente ligada a los procesos y a las políticas. Así un plan de cultura dirigida a la seguridad de la información tiene que ser completo e incluir aspectos de seguridad, reuniones con los grupos objetivos y contar con una metodología adecuada con fundamento en las certificaciones profesionales internacionales y los estándares a nivel mundial.

6.6.II *TECNOLOGÍAS DE PROTECCIÓN*

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Algunas técnicas son evidentes y otras no, incluso pueden producir una sensación de falsa seguridad.

Algunas de las vulnerabilidades estudiadas son el resultado de la implementación incorrecta de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas pero la mayoría de los agujeros de seguridad son ocasionados por los usuarios de

dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

Estas tecnologías pueden dividirse de manera independiente o en su conjunto llamado suite de seguridad. Durante los últimos años, las suites de seguridad han ganado prestigio entre los usuarios que buscan una máxima protección en un solo producto en lugar de tener que instalar todo por separado. Además, permite ser más productivo a la hora de controlar la seguridad y del consumo de recursos de los equipos informáticos. Una suite de seguridad es la suma de varios programas, los cuales son:

a) Antispyware

Ayuda a proteger a un equipo contra spyware y otro software potencialmente no deseado. Reduce sus efectos incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada. Permite a los usuarios protegerse contra los programas cuya intención es rastrear la información sobre hábitos de consumo y navegación, o peor aún, obtener contraseñas y otros datos sensibles.

b) Antivirus

Funciona mediante un escaneo de archivos la cual tiene como objetivo la detección, identificación y eliminación de malware. Además, está formado por tres principales partes (figura 6.7).



Figura 6.7. Partes de un software antivirus

1. Interfaz de usuario: Es el medio por el cual un usuario puede comunicarse e interactuar con el programa y realizar configuraciones.
2. Motor de búsqueda: Es el cerebro del programa ya que se encarga de la búsqueda y detección de malware, utilizando para ello la base de datos de definiciones de virus.
3. Base de datos de definición de virus: Contiene los archivos sobre las firmas del malware, que se actualiza periódicamente y es utilizada por el antivirus para lograr su detección.

Existen tres métodos utilizados por los programas antivirus para realizar la detección de malware, estas son:

1. *Coincidencia de firmas (Matching signature)*: Se basa en la búsqueda de coincidencias entre los archivos escaneados y los registros de las firmas de malware. El inconveniente se da si no se cuenta previamente con la firma asociada al malware para poder realizar su detección, lo cual requiere que el usuario realice actualizaciones periódicas a la base de datos de dichas firmas.
2. *Heurístico (Heuristic)*: Analiza el código de cualquier rutina o subrutina y lo compara con las firmas de comportamiento almacenadas en la base de datos (nivel estático). También puede realizar la detección de malware sin contar con la firma asociada.
3. *Verificación de integridad (Integrity checksum)*: Se realiza hasta que el malware infecta al sistema y realiza modificaciones. Las principales desventajas son la generación de falsos positivos, así como su ineficiencia hacia la detección de los macro virus o aquellos virus capaces de insertarse en la memoria.

c) *Antispam*

Previene el correo basura mediante el uso de cuatro categorías: las que requieren acciones por parte humana; las que de manera automática son los mismos correos electrónicos de los administradores; las que se automatizan por parte de los remitentes de correos electrónicos; las empleadas por los investigadores y funcionarios encargados de hacer cumplir las leyes.

d) *Control parental*

Su objetivo es bloquear, restringir o filtrar el acceso a determinada información ofensiva para los niños o personas susceptibles. Actualmente, el concepto de control parental no sólo está ligado a aplicaciones técnicas sino que corresponde a la educación, formación y comunicación entre padres e hijos para el manejo correcto de la información.

e) *Antiphishing*

Identifica el contenido que intenta suplantar la identidad contenida en páginas web y correo electrónico. A menudo se integra con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el nombre de dominio real del sitio web que el usuario visita, en un intento de evitar los sitios web fraudulentos.

6.6.III TENDENCIA EN ATAQUES

Se le llama tendencia a la inclinación o propensión hacia determinados fines. Las tendencias en ataques informáticos se dividen en dos principales: por caballos de Troya y por bots (hacen zombis a las computadoras).

Actualmente, se ha incrementado el consumo del ancho de banda debido a que los caballos de Troya se están reenviando de manera constante y los bots reciben las órdenes (activadores o desactivadores) que son usados para el envío masivo de spam por e-mail, para alojar datos ilegales o para unirse en ataques DDoS como forma de extorsión, entre otras. Por otra parte, están los ataques por phishing, los cuales defraudan a gran número de personas. Los criterios en las tendencias en ataques informáticos son:

- a) Nuevos usuarios entran al campo de la creación de programas maliciosos con el objetivo de realizar ataques y recopilar información con fines lucrativos.
- b) Los delincuentes cibernéticos atacarán con frecuencia a los usuarios corporativos dejando paulatinamente a los usuarios comunes.
- c) Las vulnerabilidades seguirán siendo el principal método para realizar ataques (su impacto y velocidad de uso crecerán de forma significativa).

Además, algunas tendencias en ataques informáticos son las siguientes:

- a) Malware (Malicious software, programa malicioso)

Tiene como objetivo infiltrarse o dañar la computadora sin el consentimiento del propietario y se dividen en: virus, gusanos, troyanos, rootkits, spyware, adware intrusivo y otros. Malware no es lo mismo que software defectuoso; éste último contiene bugs (errores) peligrosos pero no de forma intencionada. Debido al aumento de usuarios de Internet, el malware se ha programado para obtener beneficio de otros equipos de cómputo siendo de manera legal o ilegalmente.

- b) SPAM (correo basura)

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. Su principal medio de difusión es el correo electrónico aunque también se presenta en programas de mensajería instantánea o por telefonía celular. El spam representa un elevado porcentaje del tráfico de correo electrónico total. A medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el spam, los spammers modifican sus técnicas con el objetivo de evitar las contramedidas desplegadas por los usuarios.

c) Ataque Aurora

Los objetivos principales fueron: que el ataque fue motivado con el ánimo de robar información de propiedad intelectual a grandes compañías; y por el otro, la intención de robar cuentas de Gmail de activistas de derechos humanos en China.

El ataque consiste en configurar una sesión de escucha y configurar un servidor web que hospeda el código malicioso, espera que el usuario visite el sitio web para abrir una conexión entre la computadora del atacante y la del usuario. Una vez obtenida la sesión, el atacante tiene el control de la computadora.

d) 0-Day Exploits (Explotaciones Día Cero)

Busca vulnerabilidades aún desconocidas para el usuario y el fabricante del producto en las aplicaciones informáticas hasta que finalmente son encontradas y se publican en un foro. Una vulnerabilidad o exploit cuenta con un periodo de tiempo, al inicio se publica la amenaza y al final salen los parches que lo solucionan (generados y distribuidos por los propios fabricantes). En este periodo es cuando ocurren los ataques de día-cero.

e) Metasploit

Proporciona información acerca de vulnerabilidades de seguridad en el desarrollo de firmas para sistemas de detección de intrusos y para el desarrollo, prueba, mejora y penetración a diversos sistemas operativos. Trabaja con una base de datos en la cual se encuentra toda la lista de exploits y vulnerabilidades, lo único que se tiene que indicar al metasploit es la vulnerabilidad a manejar, el sistema a atacar, el tipo de ataque que se usará y los datos diversos que utilizará para atacar al host.

CAPÍTULO 7

MANUAL DE PRÁCTICAS



En el año de 1977 se creó en la Facultad de Ingeniería de la UNAM la Carrera de Ingeniería en Computación, como respuesta a la necesidad de formar profesionales de alto nivel en este campo, comprometidos con la sociedad. La última modificación de los planes y programas de estudios fue en 2005.

Ante el cambio del paradigma en el proceso de enseñanza aprendizaje de las ingenierías, las instituciones formadoras de ingenieros deben redefinir y adecuar sus programas educativos. La sociedad en el siglo XXI se caracteriza por un amplio, sostenido y cambiante uso de la tecnología, en un mercado global de enorme competencia e interdependencia, y con una capacidad de comunicación jamás imaginada.

Esto implica para los ingenieros el reto de adquirir nuevas habilidades que le permitan diseñar, construir, fabricar y operar bienes con mayor valor agregado de tecnología y más eficientes, a los menores costos posibles, además de profundizar sus conocimientos en diversas disciplinas, ampliando sus capacidades de información y desarrollando su creatividad. En síntesis, se trata de formar ingenieros aptos para la innovación tecnológica en un mundo global, interconectado y altamente competitivo, al servicio de una Nación quien debe establecer una estrategia de desarrollo nacional y la Facultad de Ingeniería debe colaborar en ello junto con otros actores esenciales como los gremios de profesionales de la ingeniería en México.

Para mantenerse a la vanguardia del conocimiento en el campo de la computación, la Facultad de Ingeniería ha estado conduciendo la modificación del plan de estudios de la carrera de Ingeniería en Computación, con el compromiso de mantener la excelencia y el liderazgo académico, conservando los valores esenciales que dan vida a nuestra Facultad y a nuestra Universidad.

7.1 MANUAL DE PRÁCTICAS¹²

El manual de prácticas se realizó para el módulo de redes y seguridad, donde se propuso la asignatura llamada *Seguridad Informática Avanzada* (aun no entra en el plan de estudios) con la nueva modalidad de contar con un laboratorio incluido, en la cual se fusionan en su mayor parte los programas de las asignaturas de Seguridad Informática I¹³ y II¹⁴ del plan 2005 y de la cual se basó para la realización del manual de prácticas. A continuación, se ven los objetivos de las asignaturas del plan 2005 en comparación con el propuesto de Seguridad Informática Avanzada.

1. SEGURIDAD INFORMÁTICA I

Objetivo(s) del curso:

El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética.

2. SEGURIDAD INFORMÁTICA II

Objetivo(s) del curso:

El alumno conocerá, identificará y aplicará los servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; conocerá, comprenderá y hará uso de las estrategias de monitoreo de los mecanismos de seguridad para administrar la seguridad dentro de una organización, a la vez que podrá controlar los sucesos e incidentes de seguridad conociendo los aspectos sociales en el área de la seguridad informática.

3. SEGURIDAD INFORMÁTICA AVANZADA

Objetivo(s) del curso:

El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, vulnerabilidades y ataques en sistemas y redes de cómputo. Asimismo, conocerá, identificará y aplicará servicios y herramientas que le permitan implementar la

¹² Para ver las prácticas véase el apéndice G

¹³ Para mayor información acerca del programa véase el apéndice D.

¹⁴ Para mayor información acerca del programa véase el apéndice E.

seguridad informática dentro de una organización; además de estrategias de monitoreo de los mecanismos de seguridad, a la vez que controle los sucesos e incidentes de seguridad conociendo y considerando los aspectos sociales en el área de seguridad informática y enmarcados en una base ética.

Tomando como referencia el programa de la materia de *Seguridad Informática Avanzada*¹⁵ se elaboró un Manual de Prácticas para el laboratorio de dicha asignatura donde se cubren las necesidades de la misma. Conforme al nuevo programa de estudios la asignatura lleva por nombre Seguridad Informática Avanzada, con clave y semestre por asignar, tiene 14 créditos, pertenece a la división de Ingeniería Eléctrica del departamento de Ingeniería en Computación, en la carrera que se imparte es Ingeniería en Computación, la asignatura es obligatoria teniendo 6 horas teóricas y 2 prácticas, siendo 8 horas por semana durante 16 semanas que da un total de 128 horas.

El manual que se realizó para el laboratorio de la asignatura de Seguridad Informática Avanzada consta de 15 prácticas que cubren los temas más relevantes del programa como se pueden observar en la siguiente tabla 7.1.

Tabla 7.1 Prácticas del manual conforme al programa de estudios

Número y nombre de la práctica	Número y nombre del tema
Practica 1 - Identificación de amenaza	2.- Amenazas y vulnerabilidades
Practica 2 - Ataques pasivos y activos Practica 3 - Phising Practica 4 - SQL Injection en PHP Practica 5 - WEP Key-cracking	3.- Identificación de ataques y técnicas de intrusión
Practica 6 - Firewall Practica 7 - Configurar una VPN en Windows Practica 8 - Configurar una VPN en Linux	6.- Implementación de la seguridad informática
Practica 9 - Detección de Intrusos Snort con Nessus Practica 10 - Detección de Intrusos Snort con NMAP	7.- Gestión de la seguridad informática
Practica 11 - Auditoría (Hardening de sistemas Linux) Practica 12 - Análisis Forense	8.- Control de la seguridad informática
Practica 13 - Impacto Social de Facebook y Twitter	9.- Entorno social, ética informática e impacto económico de la seguridad informática
Practica 14 - Ataque de día cero Aurora Practica 15 - Ataque de día cero Adobe Reader 9.3	10.- Nuevas tendencias y tecnologías

¹⁵ Para mayor información acerca del programa véase el apéndice F.

Cada práctica está diseñada para ser realizada en un máximo de dos horas que es el tiempo que dura el laboratorio y cada una consta de 7 partes, las cuales son:

- 1.- Objetivos de aprendizaje
- 2.- Conceptos teóricos (Introducción)
- 3.- Equipo y material necesario
- 4.- Desarrollo
- 5.- Preguntas
- 6.- Conclusiones
- 7.- Cuestionario Previo

A continuación se da una breve descripción del contenido de cada una de las prácticas:

Practica 1 - Identificación de amenaza

Se identificará, clasificará y explicará los distintos tipos de amenazas y vulnerabilidades presentes en el Laboratorio de Redes y Seguridad.

Practica 2 - Ataques pasivos y activos

Identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas. Explicará y clasificará los distintos tipos de ataques: pasivos y activos. Identificará la metodología que conlleva un ataque basándose en un caso. Adquirirá la habilidad para ir descubriendo las pistas que pueden estar en un informe para obtener los datos y elaborar su propia metodología.

Practica 3 - Phising

Conocerá e identificará los métodos y técnicas de ataque e intrusión a redes y sistemas. Analizará el contenido que intenta suplantar la identidad en páginas web y correo electrónico. Entenderá el uso de SET (Social Engineering Toolkit, Kit de herramientas de Ingeniería Social) y de Java Applet Attack incluidos en la suite de Backtrack. Adquirirá la habilidad para desarrollar phising contenido en páginas web para obtener el control de la computadora de la víctima de manera remota.

Practica 4 - SQL Injection en PHP

Conocerá e identificará los métodos y técnicas de ataque e intrusión a redes y sistemas en SQL injection. Identificará las partes que conforman una base de datos. Identificará cuáles son los puntos clave para que una página web sea vulnerable a un ataque de inyección SQL en PHP, esto debe hacerse únicamente con fines educativos.

Practica 5 - WEP Key-cracking

Conocerá los tipos de mecanismos de seguridad para evitar la vulnerabilidad que tiene la clave WEP. Explicará cómo funciona una clave WEP en la seguridad de las redes inalámbricas y los modos de autenticación. Determinará qué componentes son necesarios para obtener una clave WEP y esto se hará únicamente con fines educativos. Sabrá paso a paso, la forma en que debe ser *atacado* un router para obtener su clave WEP. Comparará la seguridad que brinda WEP con otros sistemas de cifrado como WPA o WPA2.

Practica 6 - Firewall

Conocerá el mecanismo de protección más usado (firewall) para cuidar la seguridad informática en una organización de manera lógica. Determinará cómo desactivar el firewall de Windows XP. Aprenderá a usar y a configurar un ataque con la herramienta de software Armitage. Distinguirá el riesgo de entrar a sitios web que tienen en la dirección url ciertos patrones específicos.

Practica 7 - Configurar una VPN en Windows

Conocerá el mecanismo de protección (VPN) para cuidar la seguridad informática en una organización de manera lógica. Analizará cómo funciona una VPN y qué elementos debe incluir. Al finalizar la práctica tendrá la capacidad de configurar una VPN así como compartir carpetas y archivos dentro de ella.

Practica 8 - Configurar una VPN en Linux

Conocerá el mecanismo de protección (VPN) para cuidar la seguridad informática en una organización de manera lógica. Analizará cómo funciona una VPN y qué elementos debe incluir. Al finalizar la práctica tendrá la capacidad de configurar una VPN así como compartir carpetas y archivos dentro de ella.

Practica 9 - Detección de Intrusos Snort con Nessus

Permitirá administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes. Desarrollará la habilidad para detectar intrusos usando la interfaz web de monitoreo Snort. Aprenderá sobre las funciones de BASE (Basic Analysis and Security Engine, Análisis básico y motor de seguridad). Identificará la metodología que conlleva configurar un escaneo de vulnerabilidades en Nessus. Analizará y conocerá sobre la importancia del resumen ejecutivo, vulnerabilidades por host y vulnerabilidades por plugin en Nessus. Conocerá la importancia de los sistemas de detección de intrusos para evitar entradas no autorizadas y las propias vulnerabilidades existentes en el entorno.

Practica 10 - Detección de Intrusos Snort con NMAP

Permitirá administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes. Aprenderá a instalar, configurar, crear reglas y administrar un detector de intrusos (Snort). Usará los programas nmap y zenmap para escanear un sistema operativo así como los comandos básicos de cada uno y las diferencias entre los mismos.

Practica 11 - Auditoría (Hardening de sistemas Linux)

Conocerá y comprenderá la utilidad de mantener el control sobre redes y dispositivos dentro de una organización a través de la realización de auditorías. Realizará y auditará el fortalecimiento de dos sistemas operativos Linux para hacerlo más seguro en cuestión de vulnerabilidades (Ubuntu 12.04 LTS y Backtrack 5 R3). Conocerá y manejará la herramienta LYNIS (Security and System Auditing Tool, Herramienta de Seguridad y Auditoría al Sistema) usado para la detección de fallas. Adquirirá la habilidad para realizar el fortalecimiento o hardening del sistema con la herramienta BASTILLE.

Practica 12 - Análisis Forense

Aprenderá e identificará los métodos y herramientas para el análisis forense en informática. Adquirirá la habilidad para capturar paquetes de red (pcap) usando la herramienta de Wireshark. Conocerá y entenderá el funcionamiento de Xplico como programa orientado al análisis del tráfico de red. Utilizará el sniffer ettercap para capturar el tráfico que circula por una LAN.

Practica 13 - Impacto Social de Facebook y Twitter

Conocerá y comprenderá los aspectos sociales y económicos en el campo de la seguridad informática. Definirá el concepto de impacto social en las redes sociales, identificando los factores que se involucran en el empleo de las mismas. Adquirirá la habilidad para analizar las consecuencias del uso de las redes sociales.

Practica 14 - Ataque de día cero Aurora

Conocerá las tendencias en ataques (Aurora) hacia sistemas y redes de cómputo. Identificará cómo se realiza un ataque de día cero. Entenderá y analizará el uso del software Metasploit Framework. Adquirirá la habilidad para detectar una vulnerabilidad contenida en una falla de software.

Practica 15 - Ataque de día cero Adobe Reader 9.3

Conocerá las tendencias en ataques hacia sistemas y redes de cómputo, en especial un ataque de día cero (Adobe Reader). Analizará el contenido dado a un archivo (documento pdf) que intenta acceder de manera remota a la computadora de la víctima. Entenderá el uso de MSFconsole (Metasploit Framework) que está incluido en la suite de Backtrack. Adquirirá la habilidad para detectar una vulnerabilidad contenida en una falla de software.

Al leer, hacer y contestar cada parte de las prácticas el lector podrá demostrar los conocimientos adquiridos en teoría, verificará que no es difícil realizar un ataque informático y por consecuente aprenderá sobre él y le resultará fácil defenderse de uno.

En lo que entra en vigor el nuevo programa de Seguridad Informática Avanzada, las practicas se pueden usar con los dos programas ya existentes (Seguridad Informática I y II) abarcando los siguientes temas de cada programa como se muestra en la siguiente tabla 7.2.

Tabla 7.2 Temas que se utilizan en ambas asignaturas del plan 2005 para el Manual de Prácticas

SEGURIDAD INFORMÁTICA I	SEGURIDAD INFORMÁTICA II
<p>2 Amenazas y vulnerabilidades</p> <p>Contenido:</p> <p>2.1 Amenazas</p> <p>2.2 Vulnerabilidades</p> <p>3 Identificación de ataques y técnicas de intrusión</p> <p>Contenido:</p> <p>3.3 Explotación y obtención de acceso a Sistemas y Redes</p> <p>3.3.2 Robo de Identidad</p> <p>3.3.3 Engaño a Firewalls y Detectores de Intrusos</p> <p>3.3.4 Vulnerabilidades en el Software</p> <p>3.3.4.5 SQL Injection</p> <p>3.3.9 Ataques a Redes Inalámbricas</p> <p>3.3.9.4 WEP key-cracking</p>	<p>1 Implementación de la seguridad informática</p> <p>Contenido:</p> <p>1.1 Sistemas y Mecanismos de Protección</p> <p>1.1.2 Seguridad Lógica</p> <p>1.3 Seguridad en Redes Inalámbricas</p> <p>1.3.3 WEP (Wired Equivalent Privacy)</p> <p>2 Monitoreo de la seguridad informática</p> <p>Contenido:</p> <p>2.2 Detección de Intrusos</p> <p>3 Control de la seguridad informática</p> <p>Contenido:</p> <p>3.1 Auditoría de Red</p> <p>3.3 Análisis Forense a Sistemas de Cómputo</p>

	<p>4 Entorno social e impacto económico de la seguridad informática</p> <p>Contenido:</p> <p>4.4 Impacto Social de la Seguridad Informática</p> <p>4.5 Impacto Económico de la Seguridad Informática</p> <p>5 Nuevas tendencias y tecnologías</p> <p>Contenido:</p> <p>5.3 Tendencias en Ataques y Nuevos Problemas de Seguridad</p> <p>5.3.3 Exploits de Días Cero</p> <p>5.3.4 Metasploits</p>
--	---

Con base a los temas que se tocan en los programas actuales de Seguridad Informática en el plan 2005, ahora corresponde entrar en detalle sobre los costos y especificaciones de las prácticas del manual y el lugar en donde se puedan desarrollar.

Al realizar el manual de prácticas para el nuevo laboratorio de la asignatura de Seguridad Informática Avanzada, uno se imagina el gran número de dificultades e inconvenientes que se tendrían que superar para lograr el objetivo.

Al empezar a trabajar en la creación del manual de prácticas para el nuevo laboratorio, el primer obstáculo al que uno se enfrenta es la asignación de un espacio donde se puedan llevar a cabo, y se pensó que se puede utilizar el laboratorio de Redes y Seguridad que está ubicado en el primer piso del edificio de Posgrado de la Facultad de Ingeniería.

Teniendo el área de trabajo, el siguiente punto es el elegir qué tipo de equipo de cómputo se va a necesitar ya que ciertas prácticas requieren de más memoria RAM, espacio en disco duro, de un buen procesador, de varios sistemas operativos instalados o de máquinas virtuales instaladas. Se propone que el nuevo laboratorio cuente con computadoras de escritorio de estas características como mínimo ya que si se usa equipos con menor rendimiento al indicado puede que no funcionen adecuadamente los sistemas operativos o no soporte las diferentes máquinas virtuales (véase figuras 7.1 y 7.2):



Modelo AM3970-MO13P: <http://www.acer.com.mx/ac/es/MX/content/model/DL.SHAAL.001>
 Precio estimado: <https://syste-mart.com/verProducto.php?cv=PC-1423>
 Costo \$ 12,977.19 pesos (IVA incluido)

Windows® 7 Home Premium - versión de 64-bit - Procesador Intel® Core™ i5-2320 (3.30GHz, 6MB cache) - 12GB DDR3 SDRAM
 - disco duro 2TB - pantalla de 21.5" (1920 x 1080) Full HD - integrados gráficos - Intel® H67 Express
 - DVD-RAM/±R/±RW - Red Gigabit Ethernet 1000 Base-T,
 Red inalámbrica 802.11b/g/n - HDMI® - USB - teclado y mouse USB - garantía limitada de 1 año

Figura 7.1. Modelo ACER AM3970-MO13P

Modelo XPS 8700
http://configure.la.dell.com/dellstore/config.aspx?oc=good1403_017&model_id=xps-8700&c=mx&l=es&s=dhs&cs=mxdhs1
 Costo \$12,499 pesos (IVA incluido)





PROCESADOR
Intel®
Core™ i5



8



8GB



1TB

Procesador
 Cuarta generación del procesador Intel® Core™ i5-4430 (6MB Caché, hasta 3.20 GHz)

Sistema operativo
 Windows 8, 64-bit, Español

Memoria
 8 GB Dos canales SDRAM DDR3 a 1600 MHz

Disco duro
 Disco Duro SATA de 1TB 7200 RPM (6.0 Gb/s)

Tarjeta de video
 AMD Radeon™ HD 7570 1GB GDDR5

Garantía
 1 Año de garantía Estándar, con Servicio en el sitio al siguiente día laborable



Figura 7.2. Modelo DELL XPS 8700

También se presenta la siguiente tabla 7.3 donde se expone el software, hardware y máquina virtual que necesita cada práctica en base a sus requerimientos específicos:

Tabla 7.3 Costos y especificaciones del manual de prácticas para la asignatura de Seguridad Informática Avanzada

NO. PRÁCTICA	NOMBRE DE LA PRACTICA	HARDWARE	SOFTWARE	NÚMERO DE MÁQUINAS VIRTUALES	
1	Identificación de amenazas y vulnerabilidades	Computadora de escritorio*			
2	Ataques pasivos y activos	Computadora de escritorio*			
3	Phishing	Computadora de escritorio*	VMware Workstation 9 Java versión 6 o 7	2	Backtrack 5 R3 Windows 7 (cualquier edición)
4	<i>SQL injection en PHP</i>	Computadora de escritorio*	VMware Workstation 9	1	Backtrack 5 R3
5	WEP key-cracking	Computadora de escritorio* Antena inalámbrica externa**	Sistema operativo Backtrack 5 R3		
6	Firewall	Computadora de escritorio*	VMware Workstation 9	1	Backtrack 5 R3
7	Configurar una VPN en Windows	Computadora de escritorio* Mini Switch Ethernet 10/100 Mbps 2 cables patch cord de Ethernet	Sistema operativo Windows 7 (Ultimate)		
8	Configurar una VPN en Linux	Computadora de escritorio* Mini Switch Ethernet 10/100 Mbps 2 cables patch cord de Ethernet	Sistema operativo Ubuntu 12.04LTS		
9	Detección de intrusos SNORT con Nessus	Computadora de escritorio*	VMware Workstation 9 Snort Nessus	1	Backtrack 3
10	Detección de intrusos SNORT con Nmap	Computadora de escritorio*	VMware Workstation 9 Snort Nmap	1	Backtrack 5 R3

11	Auditoría (Hardening de sistemas Linux)	Computadora de escritorio*	Sistema operativo Backtrack 5 R3 Sistema operativo Ubuntu 12.04LTS Lynis Bastille		
12	Análisis forense	Computadora de escritorio*	Sistema operativo Backtrack 5 R3 Sistema operativo Ubuntu 12.04LTS		
13	Impacto social de Facebook y Twitter	Computadora de escritorio*			
14	Ataques de día cero: Aurora	Computadora de escritorio*	VMware Workstation 9 Metasploit Framework 4.5.1	1	Windows XP (con Service Pack 3)
15	Ataques de día cero: Adobe Reader 9.3	Computadora de escritorio*	VMware Workstation 9 Adobe Reader 9.3	2	Backtrack 5 R3 Windows XP (con Service Pack 3)

NOTAS

* Computadora de escritorio (a elegir)

** Antena inalámbrica externa:

- a) Alfa Network, Modelo AWUS036NH + U-Mount, tiene un costo de \$480.00 pesos
- b) TP-LINK Modelo TL-WN722N, tiene un costo de \$140.00

SOFTWARE LIBRE

- **Java versión 6 o 7**, no tiene costo y se puede descargar de Internet.
- **Sistema operativo Backtrack 5 R3**, no tiene costo y se puede descargar de Internet
- **Sistema operativo Backtrack 3**, no tiene costo y se puede descargar de Internet.
- **Sistema operativo Ubuntu 12.04LTS**, no tiene costo y se puede descargar de Internet
- **Nessus**, no tiene costo en versión de estudiante y se puede descargar de Internet
- **Snort**, no tiene costo y se puede descargar de Internet
- **Lynis**, no tiene costo y se puede descargar de Internet
- **Bastille**, no tiene costo y se puede descargar de Internet
- **Metasploit Framework 4.5.1**, no tiene costo y se puede descargar de Internet
- **Adobe Reader 9.3**, no tiene costo y se puede descargar de Internet

SOFTWARE CON LICENCIA

- **VMware Workstation 9**, la licencia tiene un costo de \$ 249.00 dólares
- **Windows 7 Ultimate**, la licencia tiene un costo de \$ 4,199.00 pesos
- **Windows XP (con Service Pack 3)**, ya no se expiden licencias debido a que se retiró el soporte técnico a este sistema operativo a partir de abril del 2014

DISPOSITIVOS DE RED

- **Mini Switch Ethernet 10/100 Mbps (5 Puertos)**, tiene un costo de \$ 200.00 pesos
- **2 cables patch cord de Ethernet**, tiene un costo de \$ 30.00 pesos c/u (haciéndolos uno mismo)

CONCLUSIONES

CONCLUSIONES

El objetivo general de la tesis se cumplió satisfactoriamente porque se planearon y diseñaron 15 prácticas para el laboratorio de *Seguridad Informática Avanzada* basándose en el nuevo programa de la asignatura y que servirán de complemento para la teoría ya que tendrán una vasta retroalimentación de los conceptos teóricos al momento de ponerlos en práctica teniendo un mayor campo visual para atender este tipo de emergencias o situaciones en el ámbito laboral.

Además se lograron los siguientes resultados:

Se mostró a los participantes los diferentes métodos que existen de hackeo, como se puede apreciar en la práctica 3 (Phising), 4 (SQL Injection en PHP), 5 (WEP Key-cracking), 6 (Firewall), 14 (Ataque de día cero: Aurora) y 15 (Ataque de día cero: Adobe Reader 9.3), ya que los ataques se realizan aprovechando una vulnerabilidad en el software, lenguaje de programación y cifrado que usa la compañía con el objetivo de amenazar la seguridad de los activos. También se enseñó cómo defenderse de un ataque informático al ir tapando los huecos de seguridad como se observa en la práctica 11 (Auditoría: Hardening de sistemas Linux) ya que al instalar las actualizaciones de software estas van desapareciendo de manera gradual.

Se identificaron las posibles vulnerabilidades y amenazas que puede sufrir una organización u compañía en la seguridad física y lógica como se hace referencia en la práctica 1 (Identificación de amenaza), 2 (Ataques pasivos y activos) y 13 (Impacto Social de Facebook y Twitter) ya que los activos se pueden manejar y procesar dependiendo del grado de seguridad que se desee obtener enseñando al encargado y/o usuario a aplicar barreras y procedimientos que resguarden el acceso, se tiene como ejemplo la práctica 7 (Configurar una VPN en Windows) y 8 (Configurar una VPN en Linux) para resolver situaciones de peligro de manera eficiente, ordenada y que se pueda coordinar con sus compañeros de trabajo.

Se mostraron las mejores herramientas para proteger los diferentes activos que cuenta una organización u empresa como se visualiza en la práctica 9 (Detección de Intrusos Snort con Nessus) y 10 (Detección de Intrusos Snort con NMAP) que da los resultados en tiempo real ante cualquier anomalía de la red local al ir indicando las conexiones que se han realizado, identificando direcciones IP y programando una lista de acciones a seguir dependiendo del suceso; sí por descuido humano se llegara a vulnerar un sistema y este fuese atacado se tendría que hacer una reconstrucción de los hechos como se aprecia en la práctica 12 (Análisis Forense) que enseña a controlar y solucionar el problema tras el incidente.

CONCLUSIONES

Finalmente, para este Manual de Prácticas de Seguridad Informática Avanzada se honraría a los autores de este trabajo de tesis al abrir un laboratorio ya que está apegado al nuevo temario para la asignatura en donde se ponen en práctica los conocimientos teóricos adquiridos durante el curso. En caso de que un lector quisiera tomar este trabajo (total o parcialmente) para una investigación, proyecto o enseñarlo en el aula de clases de reconocimiento a los autores de la tesis. Además, se les invita a promover dicho manual para que pueda tener mejoras en cuestión de diseño, desarrollo, implementación y pruebas.

FIGURAS

CAPÍTULO 1

- 1.1 Red sencilla
- 1.2 Modelo OSI conformado por 7 capas
- 1.3 Modelo TCP/IP conformado por 4 capas
- 1.4 Conjunto de protocolos del modelo TCP/IP junto a la comparativa del modelo OSI
- 1.5 Estructura del protocolo SNMP
- 1.6 Estructura del protocolo FTP
- 1.7 Arquitectura 2-capas (Cliente/Servidor)
- 1.8 Comunicación entre el navegador y el servidor por el puerto 80/TCP
- 1.9 Sistema DNS
- 1.10 Funcionamiento de NAT
- 1.11 NAT estático
- 1.12 NAT dinámico
- 1.13 Clases de direcciones IP
- 1.14 Cierre de una conexión según el estándar
- 1.15 Partes del cable coaxial
- 1.16 Tipos de cables coaxial
- 1.17 Colores del par trenzado
- 1.18 Posicionamiento de estándares Wireless
- 1.19 Adaptadores y puntos de acceso de una WLAN
- 1.20 Subcapas de la capa 2 del modelo OSI

CAPÍTULO 2

- 2.1 Router inalámbrico
- 2.2 Funcionamiento de un router
- 2.3 División de frecuencias en telefónica e Internet
- 2.4 Esquema del funcionamiento de un hub
- 2.5 Funcionamiento de un switch
- 2.6 Esquema básico de un switch conectado a dos computadora y una impresora, en la cual los elementos están compartiendo los recursos en red
- 2.7 Gráfico esquemático simplificado del funcionamiento de las computadoras servidores en internet.
- 2.8 Servidor Web
- 2.9 Panel de parcheo
- 2.10 Componentes que integran al panel de parcheo
- 2.11 Contactos con marcaje numérico
- 2.12 Fotografía de un rack
- 2.13 Puerta de enlace entre diferentes arquitecturas de red
- 2.14 Función de dos puertas de enlace predeterminadas
- 2.15 Segmento TCP

FIGURAS

- 2.16 Ejemplo de varias redes LAN conectadas a varios routers
- 2.17 Se transmite un datagrama de 1420 bytes que sale del ordenador A y atraviesa la red 1 sin ningún problema ya que el MTU es de una red Ethernet y es menor a 1500
- 2.18 Fragmentación del datagrama
- 2.19 El datagrama original se divide en tres fragmentos que se convierten en un nuevo datagrama
- 2.20 El router 2 manda los fragmentos a la red 2, el ordenador B recibe y ensambla los fragmentos para tener el datagrama original
- 2.21 Ejemplo de una gráfica de comportamiento

CAPÍTULO 3

- 3.1 Flujo normal de la información
- 3.2 Flujo con interrupción
- 3.3 Flujo con intercepción
- 3.4 Flujo con modificación
- 3.5 Flujo con suplantación

CAPÍTULO 4

- 4.1 Sistema criptográfico o criptosistema
- 4.2 Algoritmo simétrico
- 4.3 Algoritmo DES
- 4.4 Proceso del algoritmo TDES
- 4.5 Estructura básica de AES (Advanced Encryption Standard)
- 4.6 Algoritmo asimétrico

CAPÍTULO 5

- 5.1 Modelo Cliente/Servidor
- 5.2 Interacción de clientes y servidores
- 5.3 Arquitectura cliente/servidor de dos capas (Two-tier)
- 5.4 Arquitectura cliente/servidor de tres capas (Three-tier)
- 5.5 Arquitectura cliente/servidor de N capas (N-tier)

CAPÍTULO 6

- 6.1 Principales ataques a una red inalámbrica
- 6.2 Nombres que puede tener un SSID
- 6.3 Esquema de una red de computadoras que utiliza un cortafuegos
- 6.4 Fase de obtención y protección de datos

FIGURAS

- 6.5 Fase de análisis de datos
- 6.6 Reporte de la investigación forense
- 6.7 Partes de un software antivirus

CAPÍTULO 7

- 7.1 Modelo ACER AM3970-MO13P
- 7.2 Modelo DELL XPS 8700

APÉNDICE A

- A.1 Partes del cable coaxial fino
- A.2 Partes del cable coaxial grueso
- A.3 Estructura del cable UTP
- A.4 Estructura del cable STP
- A.5 Cable FTP
- A.6 Transmisión de la información por medio de fibra óptica
- A.7 Refracción de la luz con un cierto ángulo θ (izquierda) y refracción de la luz con un ángulo igual o mayor que el crítico sobre el mismo medio (derecha)
- A.8 Interior de un conductor de fibra óptica
- A.9 Recorrido de los rayos ópticos reflejándose a diferentes ángulos en la fibra multimodo
- A.10 Refracción de los rayos en forma de curvas con índice graduado
- A.11 Refracción de los rayos con índice escalonado
- A.12 Interior de la fibra monomodo
- A.13 Conectores para fibra óptica

APÉNDICE B

- B.1 Ataque Spoofing
- B.2 Conexión de tres pasos
- B.3 Ataque Smurf

TABLAS

CAPÍTULO 1

- 1.1 Clasificación de las redes por topología
- 1.2 Clasificación de las redes por área geográfica
- 1.3 Opciones negociadas de Telnet
- 1.4 Ejemplos de códigos de estado

CAPÍTULO 2

- 2.1 Estándares definidos para el router
- 2.2 Estándares del hub
- 2.3 Estándares del switch
- 2.4 MTU en diferentes redes

CAPÍTULO 3

- 3.1 Historia de la seguridad informática

CAPÍTULO 4

- 4.1 Comparación del tamaño de la llave (bits) entre ECC y el RSA

CAPÍTULO 7

- 7.1 Prácticas del manual conforme al programa de estudios
- 7.2 Temas que se utilizan en ambas asignaturas del plan 2005
- 7.3 Costos y especificaciones del manual de prácticas

APÉNDICE A

- A.1 Categorías del cable coaxial banda ancha

APÉNDICE B

- B.1 Cantidad de claves generadas según el número de caracteres empleados

APÉNDICE C

- C.1 Estándares definidos para un access point

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

ACK (Acknowledgement): Acuse de recibo. En comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

AES (Advanced Data Encryption Standard): Estándar avanzado de cifrado de datos.

Amenaza: Es todo aquello que intenta, puede o pretende destruir a un activo.

AP (Access Point): Punto de acceso. Es un dispositivo que interconecta equipos de comunicación para formar una red (cableada o inalámbrica) y transmitir datos.

Applet: Es un componente de aplicación que se ejecuta en el contexto de otro programa, por ejemplo un navegador web.

AppleTalk: Es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes.

ARP (Address Resolution Protocol): Protocolo de resolución de direcciones. Es el encargado de convertir las direcciones IP en direcciones de la red física.

ASCII (American Standard Code For Information Interchange): Código Americano Estandarizado para el Intercambio de Información.

Asymmetric: Asimétrico.

ASP (Active Server Pages): Es una tecnología desarrollada por Microsoft para la creación dinámica de páginas web ofrecida junto a su servidor IIS.

Ataque: Es la realización o culminación de una amenaza.

ATM (Asynchronous Transfer Mode): Modo de Transferencia Asíncrona. Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Autenticación o autenticación: Verificación de la identidad de una persona, usuario o proceso, para así acceder a determinados recursos o poder realizar determinadas tareas.

BackDoor: Estos programas son diseñados para abrir una puerta trasera en nuestro sistema para permitir al creador del backdoor tener acceso al sistema y hacer lo que desee con él.

BFOC (Bayonet Fiber Optic Connector): Conector de bayoneta de fibra óptica.

GLOSARIO DE TÉRMINOS

Bot: Es un programa informático que realiza funciones muy diversas, imitando el comportamiento de un humano.

Bridge: Puente de red. Es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Broadcast: Difusión. Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

BSI (British Standard Institute): Instituto Británico de Estándares.

Bugs: Es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado.

CGI (Common Gateway Interface): Interfaz Común de Intercomunicación. Conjunto de medios y formatos que permite y unifica la comunicación entre la web y otros sistemas externos, como las bases de datos.

CoS (Class of Service): Clase de servicio. Es un parámetro usado en los protocolos de voz y datos para diferenciar los tipos de cargas contenidas en los paquetes cuando son transmitidos.

Cracks: Tipo de programa que realiza una modificación permanente o temporal sobre otro o en su código, para obviar una limitación o candado impuesto a propósito por el programador original.

Criptoanalista: Es la persona que sin poseer ningún permiso intenta descubrir la clave o el mensaje original utilizando para ello el criptoanálisis.

Criptografía: Son las técnicas utilizadas para cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Criptograma: Es el texto o mensaje cifrado.

Criptología: Se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.

DB (Data Base): Base de datos.

GLOSARIO DE TÉRMINOS

DCOM (Distributed Component Object Model): Modelo de Objetos de Componentes Distribuidos. Es una tecnología para desarrollar componentes software distribuidos sobre varios ordenadores y que se comunican entre sí.

Demonio: Es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario.

DES (Data Encryption Standard). Estándar de cifrado de datos.

DMZ (DeMilitarized Zone): Zona desmilitarizada. Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DNS (Domain Name System): Sistema de denominación de dominio. Es un conjunto de protocolos y servicios (base de datos distribuida) que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas.

DoS (Denial of Service): Ataque de denegación de servicio a un sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Downstream: Flujo descendente. Se refiere a la velocidad con que los datos pueden ser transferidos de un servidor a un cliente, lo que podría traducirse como velocidad de bajada (downloading).

DQDB (Distributed-Queue Dual-Bus): Bus Dual de Cola Distribuida. Es una tecnología de transmisión de paquetes entre redes de área metropolitana y redes de área extensa a alta velocidad.

DRP (Disaster Recovery Plan): Plan de recuperación de desastres.

EAP (Extensible Authentication Protocol): Protocolo de autenticación extensible.

ECDH (EC Diffie-Hellman key agreement): Intercambio de claves de curvas elípticas Diffie-Hellman.

ECDSA (EC Digital Signature Algorithm): Algoritmo de firma digital de curvas elípticas.

ELF (Extremely Low Frequency): Frecuencia Extremadamente Baja. Es la banda de radiofrecuencias comprendida entre los 3 y los 30 Hz.

E-mail (Electronic mail): Correo electrónico. Es un servicio de internet que permite el intercambio de mensajes entre usuarios.

GLOSARIO DE TÉRMINOS

Exploit: Es una pieza de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

FC (Ferrule Connector). Conector Férula. Conector usado para equipos de medición como OTDR.

FDDI (Fiber Distributed Data Interface): Interfaz de Datos Distribuida por Fibra. Es una interfaz de red en configuración simple o de doble anillo que puede ser implementada con fibra óptica, cable de par trenzado apantallado o sin apantallar.

FDX (Full Duplex): La etiqueta puede transmitir inmediatamente cuando en la presencia de un campo de activación del receptor.

Firewall: Cortafuego. Es un sistema que previene el uso y el acceso desautorizados al ordenador.

FTP (File Transfer Protocol): Protocolo de transferencia de archivos. Es un software cliente/servidor que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP.

Full Dúplex: Cualidad de los elementos que permiten la entrada y salida de datos de forma simultánea.

GAN (Global Area Network): Red de área global.

GPRS (General Packet Radio Service): Servicio General de Paquetes vía Radio. Es una técnica de conmutación de paquetes, que es integrable con la estructura actual de las redes GSM.

GSM (Global System for Mobile communications): Sistema Global para las comunicaciones Móviles.

Half Duplex: Semidúplex. Significa que el método o protocolo de envío de información es bidireccional pero no simultáneo.

Hardening: Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etcétera.

HCRMON (High Capacity Remote MONitoring): Monitoreo Remoto de redes de Alta Capacidad.

GLOSARIO DE TÉRMINOS

HDX (Half Duplex): La etiqueta debe almacenar suficiente energía cuando el campo de activación del receptor se activa para permitir que se transmita cuando el campo de activación está apagado.

Hilo: Son subprocesos que se ejecutan de manera secuencial dentro de otro proceso compartiendo así el CPU, tienen el mismo espacio de direcciones.

HTML (Hyper Text Markup Language): Lenguaje de marcación de Hipertexto.

HTTP (HyperText Transfer Protocol): Protocolo de transferencia de hipertexto. Es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un ordenador.

Hub: Concentrador. Es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás.

IANA (Internet Assigned Numbers Authority): Autoridad de Asignación de Números en Internet. Antiguo registro central de protocolos, puertos, números de protocolos y códigos de Internet. Fue sustituido en 1998 por la ICANN.

IBM (International Business Machines): Es una empresa multinacional estadounidense de tecnología y consultoría.

ICMP (Internet Control Message Protocol): Protocolo de mensajes de control de Internet. Es un protocolo que permite administrar información relacionada con errores de los equipos en red.

IDS (Intrusion Detection System): Sistema de detección de intrusos. Es un programa usado para detectar accesos no autorizados a una red o a una computadora.

IDEA (International Data Encryption Algorithm): Algoritmo Internacional de Cifrado de Datos.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de Ingenieros Eléctricos y Electrónicos.

IP (Internet Protocol): Protocolo de Internet.

IPS (Intrusion Prevention System): Sistema de Prevención de Intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

GLOSARIO DE TÉRMINOS

IPSec (Internet Protocol Security): Seguridad de protocolo Internet. Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos

ISACA (Information Systems Audit and Control Association): Asociación de Auditoría y Control de Sistemas de la Información.

ISDN (Integrated Services Digital Network): Red de datos de servicios integrados. Está diseñada para transportar datos (voz, imágenes, faxes, etcétera), además de señalar información.

ISO (International Organization for Standardization): Organización Internacional para la Estandarización.

ISP (Internet Service Provider): Proveedor de servicios de Internet.

ITU (International Telecommunication Union): Unión Internacional de Telecomunicaciones.

JDBC (Java Data Base Connectivity): Conectividad a la Base de Datos de Java.

JDK (Java Development Kit): Es un software que provee herramientas de desarrollo para la creación de programas en Java. Puede instalarse en una computadora local o en una unidad de red.

jFlow: Es un flujo de tráfico IP de tecnología de muestreo utilizado por los routers y switch.

Kernel: Núcleo. Es el encargado de que el software y el hardware del ordenador puedan trabajar juntos.

Keygens (key generator): Generador de claves. Es un programa informático que al ejecutarse genera un código (serial) para que un determinado programa de software de pago en su versión de prueba (Trial) pueda ofrecer los contenidos completos del programa.

LAN (Local Area Network): Red de área local.

LC (Lucent Connector o Local Connector): Conector más pequeño y sofisticado, usado en transceivers y equipos de comunicación de alta densidad de datos.

GLOSARIO DE TÉRMINOS

LLC (Logical Link Control): Control de enlace lógico. Define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores. Es la más alta de las dos subcapas de enlace de datos definidas por el IEEE y la responsable del control de enlace lógico.

Log: Es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

MAC (Medium Access Control): Control de Acceso al Medio. Es el mecanismo encargado del control de acceso de cada estación al medio. Puede realizarse de forma distribuida cuando todas las estaciones cooperan para determinar cuál es y cuándo debe acceder a la red. También se puede realizar de forma centralizada utilizando un controlador.

Malware (malicious software): También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

MAN (Metropolitan Area Network): Red de área metropolitana.

MD5 (Message-Digest Algorithm 5): Algoritmo de Resumen del Mensaje 5. Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Metasploit: Es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en pruebas de penetración y en el desarrollo de firmas para sistemas de detección de intrusos.

MIB (Management Information Base): Base de Información Gestionada. Es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol de todos los dispositivos gestionados en una red de comunicaciones.

MTU (Maximum Transmission Unit): Unidad Máxima de Transmisión. Es el tamaño máximo que puede ocupar un paquete de información en el protocolo IP.

MT-RJ (Mechanical Transfer Registered Jack). Conector dúplex plástico de pequeño tamaño con mecanismo de fijación rápido.

NAT (Network Address Translation): Traducción de Dirección de Red. Es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP.

NetBIOS (Network Basic Input/Output System): Es un programa que permite la comunicación entre aplicaciones en diferentes ordenadores dentro de una LAN.

GLOSARIO DE TÉRMINOS

Netflow: Es un protocolo de red para recolectar información sobre tráfico IP.

NFS (Network File System): Sistema de archivos de red. Permite a los hosts remotos montar sistemas de archivos sobre la red e interactuar con esos sistemas de archivos como si estuvieran montados localmente. Esto permite a los administradores de sistemas consolidar los recursos en servidores centralizados en la red.

NIC (Network Interface Card): Tarjeta de interfaz de red. Es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras.

NIST (National Institute for Standards and Technology): Instituto Nacional de Estándares y Tecnología.

ODBC (Open Data Base Connectivity): Abrir una Conexión a la Base de Datos.

OSI (Open System Interconnection): Modelo de interconexión de sistemas abiertos. Es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos.

P2P (Peer to peer): Red de pares o red punto a punto. Es una red de computadoras permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados.

PAN (Personal Area Network): Red de área personal.

PC (Personal Computer): Computadora personal.

PES (Proposed Encryption Standard): Estándar de cifrado propuesto.

PGP (Pretty Good Privacy): Privacidad bastante buena. Es un programa desarrollado por Phil Zimmermann cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Políticas de seguridad: Es un enunciado formal de las reglas que deben cumplir los usuarios que acceden a los recursos de la red de una organización.

QoS (Quality of Service): Calidad de servicio. Son las tecnologías que permiten aplicar un tratamiento específico a un determinado tipo de tráfico.

QUIT: Orden básica de SMTP para cerrar la sesión.

GLOSARIO DE TÉRMINOS

RADIUS AUTHENTICATION (Remote Authentication Dial In User Service): Autenticación remota telefónica de servicio de usuario.

RARP (Reverse Address Resolution Protocol): Protocolo de Resolución de Direcciones Inverso. Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dada (como una dirección Ethernet).

RC4: Es un sistema de cifrado de flujo utilizado en algunos protocolos como TLS/SSL (para proteger el tráfico de Internet) y WEP (para añadir seguridad en las redes inalámbricas).

RCPT: Orden básica de SMTP para indicar el destinatario del mensaje.

Red de Feistel: Es un método de cifrado en bloque con una estructura particular. Debe su nombre al criptógrafo de IBM Horst Feistel.

RFC (Request for Comments): Petición de comentarios. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RG (Radio Grade): Es un cable especial blindado para la utilización de altas frecuencias ya que aísla las radiofrecuencias externas que pueden provocar mal funcionamiento y a su vez no deja interferir con otros dispositivos cercanos. Las designaciones de RG se utilizan sobre todo para identificar a los conectores compatibles que se ajustan a los interiores del conductor, dieléctrico y a las dimensiones de los jackets de los antiguos cables de series RG.

RIPEMD-160 (acrónimo RACE Integrity Primitives Evaluation Message Digest): Primitivas de integridad del resumen del mensaje. Es un algoritmo del resumen del mensaje de 160 bits (y función criptográfica de hash) desarrollado en Europa por Hans Dobbertin, Antoon Bosselaers y Bart Preneel, y publicados en 1996. Es una versión mejorada de RIPEMD, que estaba basado sobre los principios del diseño del algoritmo MD4, y es similar en seguridad y funcionamiento al SHA-1.

RMON (Remote MONitoring): Protocolo de Monitoreo Remoto. Es un protocolo de red que permite que la información de una red sea recolectada por una sola estación de trabajo.

RTT (Round-Trip delay Time): Tiempo Aproximado de Viaje. Tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.

GLOSARIO DE TÉRMINOS

Router: Es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

SAP (Source Access Point): Punto de acceso al servicio. Ubicación de la fuente de servicios de un nivel hacia el siguiente.

SC (Subscriber Connector). Conector de Suscriptor. Conector de bajas pérdidas, muy usado en instalaciones de SM y aplicaciones de redes y CATV.

Seal: Es un generador de secuencia diseñado en 1993 para IBM basado en un proceso inicial en el que se calculan los valores para unas tablas a partir de la clave, de forma que el cifrado propiamente dicho puede llevarse a cabo de una manera rápida.

Servlet: Es una clase Java usada para extender la capacidad de aplicaciones basadas en el modelo cliente-servidor y que utilizan el protocolo HTTP basado en la interacción de ambos extremos por medio de una petición y una respuesta.

sFlow: Es una tecnología de red de monitoreo, inalámbrica y de dispositivos host.

SHA-1 (Secure Hash Algorithm): Algoritmo de Hash Seguro. Es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el NIST.

SMDS (Switched Multimegabit Data Service): Servicio de datos conmutados multimegabit. Es capaz de proporcionar un transporte de datos transparente *no orientado a conexión* entre locales de abonado utilizando accesos de alta velocidad a redes públicas dorsales.

SMTP (Simple Mail Transfer Protocol): Protocolo Simple de Transferencia de Correo.

SMS (Short Message Service): Servicio de Mensajes Cortos. Permite el envío de mensajes cortos entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano.

SNAT (source NAT): Cambio de origen. Es cuando alteramos el origen del primer paquete cambiando el lugar de donde viene la conexión.

Sniffer: Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

SNMP (Simple Network Management Protocol): Protocolo Simple de Administración de Red. Es un protocolo que permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red.

GLOSARIO DE TÉRMINOS

Snooping: Su objetivo es obtener información de una red a la que está conectado sin modificarla.

Social Engineering Toolkit: Kit de herramientas de Ingeniería Social. Permite realizar ataques automatizados por medio de ingeniería social.

Sockets: Es un método para la comunicación entre un programa del cliente y un programa del servidor en una red. Además, se define como el punto final en una conexión.

SSID (Service Set Identifier): Identificador de conjunto de servicios.

SSL (Secure Sockets Layer): Capa de conexión segura. Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Stealth scan o TCP Half scan: Permite a un atacante determinar qué puertos están abiertos en un host de destino, sin ser detectado por el sistema operativo host.

ST (Straight Tip): Punta recta. Es el conector más usado especialmente en terminaciones de cables MM y para aplicaciones de redes.

STM (Synchronous Transport Module): Módulo de Transporte Síncrono.

STP (Spanning-Tree Protocol): Es un estándar utilizado en la administración de redes, basado en el algoritmo de árbol abarcador, para describir cómo los puentes y conmutadores pueden comunicarse para evitar bucles en la red.

Tampering: Modificación no autorizada de los datos del software instalado en el sistema de la víctima, incluye el borrado de los archivos.

TCP (Transmission Control Protocol): Protocolo de Control de Transmisión.

TCP/IP: Transmission Control Protocol / Internet Protocol.

TDES, Triple DES, 3DES: Algoritmo que realiza el triple cifrado tipo DES para hacerlo más seguro que el cifrado DES simple. Fue desarrollado por IBM en el año 1978.

TELNET (Telecommunication Network): Red de Telecomunicaciones.

TFTP (Trivial File Transfer Protocol): Protocolo trivial de transferencia de archivos. Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. Se utiliza para transferir pequeños archivos entre ordenadores en una red.

TKIP (Temporal Key Integrity Protocol): Protocolo de clave temporal.

GLOSARIO DE TÉRMINOS

UDP (User Datagram Protocol): Protocolo de Datagrama de Usuario.

UHF (Ultra High Frequency): Frecuencia ultra alta. Es una banda del espectro electromagnético que ocupa el rango de frecuencias de 300 MHz a 3 GHz.

USM (User-Based Security Model): Modelo de seguridad orientado a usuarios.

URL (Uniform Resource Locator): Localizador de recursos uniforme. Es una secuencia de caracteres, de acuerdo con un formato modélico y estándar usado para nombrar recursos en Internet para su localización o identificación.

UTP (Unshielded twisted pair): Par trenzado no blindado.

VACM (View-Based Access Control Model): Modelo de configuración orientado en vistas.

VAF: Verificación automática de firmas. Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud. La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo.

VPN (Virtual Private Network): Red privada virtual.

WAN (Metropolitan Area Network): Red de área metropolitana.

WEP (Wired Equivalent Privacy): Privacidad equivalente al cable.

WEP2: Esta mejora de WEP fue presentada tras los primeros modelos 802.11i. Usa cifrado y vector de iniciación de 128-bits. Se esperaba que eliminase la deficiencia del duplicado de IV así como ataques a las claves por fuerza bruta. Sin embargo, como todavía se basaba en el algoritmo de cifrado RC4, aún mantenía las mismas vulnerabilidades que WEP.

Wi-Fi (Wireless Fidelity): Fidelidad inalámbrica. Consiste en estándares para redes que no requieren de cables, y que funcionan con base en ciertos protocolos previamente establecidos.

WiMAX (Worldwide Interoperability for Microwave Access): Interoperabilidad mundial para acceso por microondas. Diseñado como una alternativa wireless al acceso de banda ancha DSL y cable y una forma de conectar nodos Wi-Fi en una red de área metropolitana.

WLAN (Wireless Local Area Network): Red de área local inalámbrica.

GLOSARIO DE TÉRMINOS

WPA (Wifi Protect Access): Acceso Wi-Fi protegido. Es un sistema para proteger las redes inalámbricas (Wi-Fi) y creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP).

WPA2 (Wi-Fi Protected Access 2): Acceso Protegido Wi-Fi 2. Es un sistema para proteger las redes inalámbricas (Wi-Fi) y creado para corregir las vulnerabilidades detectadas en WPA.

WPAN (Wireless Personal Area Networks): Red Inalámbrica de Área Personal. Es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

WPS (Wi-Fi Protected Setup): Es un estándar de 2007, promovido por la Wi-Fi Alliance para facilitar la creación de redes WLAN. En otras palabras, no es un mecanismo de seguridad por sí, se trata de la definición de diversos mecanismos para facilitar la configuración de una red WLAN segura con WPA2, pensados para minimizar la intervención del usuario en entornos domésticos o pequeñas oficinas (SOHO).

WWW: World Wide Web.

APÉNDICE A

1. MEDIOS DE TRANSMISIÓN

Terrestres

A) Cable coaxial

El cable coaxial puede ser utilizado para redes Ethernet, siendo en este caso, de dos modelos diferentes:

I. CABLE COAXIAL (BANDA BASE)

1. Coaxial fino (thin)

Tiene un diámetro de 0.2 pulgadas de 50 ohms que pueden abarcar una distancia de 185m. Este tipo de cable coaxial es denominado comúnmente Cheapernet debido al bajo costo en su instalación, se aprecia en la figura A.1.

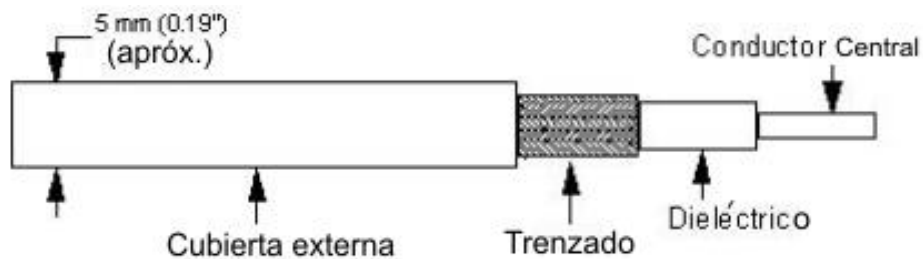


Figura A.1 Partes del cable coaxial fino

2. Coaxial grueso (thick)

Tiene un diámetro de 0.4 pulgadas de 50 ohms que puede abarcar una distancia de 500m. Es caro y difícil de instalar, pero permite conectar un mayor número de nodos y alcanzar mayores distancias. Véase figura A.2.

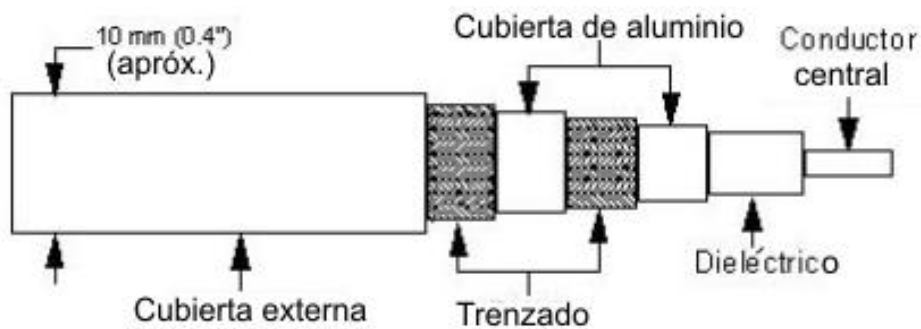


Figura A.2 Partes del cable coaxial grueso

Cable coaxial (banda base) ventajas y desventajas

Ventajas:

- Diseñados principalmente para las comunicaciones de datos, pero pueden acomodar aplicaciones de voz pero no en tiempo real.
- Tiene un bajo costo, simple de instalar y bifurcar.
- Banda ancha con una capacidad de 10 Mbps.
- Tiene un alcance de 1 a 10 kms.

Desventajas:

- Transmite una señal simple en HDX (half duplex).
- No hay modelación de frecuencias.
- Es un medio pasivo donde la energía es provista por las estaciones del usuario.
- Hace uso de contactos especiales para la conexión física.
- Se usa solo en topología bus y árbol, raramente en anillo.
- Ofrece poca inmunidad a los ruidos, puede mejorarse con filtros.
- El ancho de banda puede transportar solamente un 40 % del total de su carga para permanecer estable.

TIPO DE CONEXIÓN DEL CABLE COAXIAL BANDA BASE (thin y thick)

- ✓ El conector de cable BNC (Bayonet Neill-Concelman) está soldado o incrustado en el extremo de un cable.
- ✓ El conector BNC T se conecta a la tarjeta de red (NIC) del equipo con el cable de la red.
- ✓ Conector acoplador (barrel) BNC se utiliza para unir dos cables Thinnet para obtener uno de mayor longitud.
- ✓ Terminador BNC cierra el extremo del cable del bus para absorber las señales perdidas.

II. CABLE COAXIAL (BANDA ANCHA)

Es utilizado generalmente para señales de televisión y para transmisiones de datos de alta velocidad a distancias de varios kilómetros, de hasta 100 Mbps; pero a mayor velocidad de transmisión, menor distancia podemos cubrir porque el periodo de la señal es menor, y por tanto se atenúa antes. En la tabla A.1 se encuentran los diferentes tipos del cable coaxial banda ancha.

APÉNDICE A

Tabla A.1 Categorías del cable coaxial banda ancha

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mbps. Segmentos: máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mbps. Segmentos: máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos: máximo de 3600 metros. Velocidad de transmisión: 10 Mbps.
100-BASE-X	Fast Ethernet. Velocidad de transmisión: 100 Mbps.

Ventajas:

- Es el mismo tipo de cable que se utiliza en las redes de Tv por cable (catv).
- Es posible transmitir voz, datos y video simultáneamente.
- Todas las señales son HDX pero usando 2 canales se obtiene una señal FDX.
- Se usan amplificadores y no repetidoras.
- Se considera un medio activo, ya que la energía se obtiene de los componentes de soporte de la red y no de las estaciones del usuario conectado.

Desventajas:

- ✓ Su costo es relativamente caro, se necesitan moduladores en cada estación de usuarios, lo que aumenta su costo y limita su velocidad de transmisión.

B) Par trenzado (TWISTER-PAIR CABLING)

Existen tres tipos de par trenzado los cuales son divididos de acuerdo con sus características físicas, teniendo así, diferentes características de alcance.

2. UTP (Unshielded Twister Pair, Par Trenzado Sin Blindaje)

Únicamente depende de trenzar los cables sin necesidad de un recubrimiento externo a ellos, como se observa en la figura A.3. La distancia máxima sin necesidad de repetidores es de 100m. UTP es clasificado por el número de *trenzados* que se realizan por la unidad de medición pie. El conector más usado es el RJ45 pero también se puede usar el RJ11, DB25 o DB11 dependiendo del adaptador de red.

APÉNDICE A

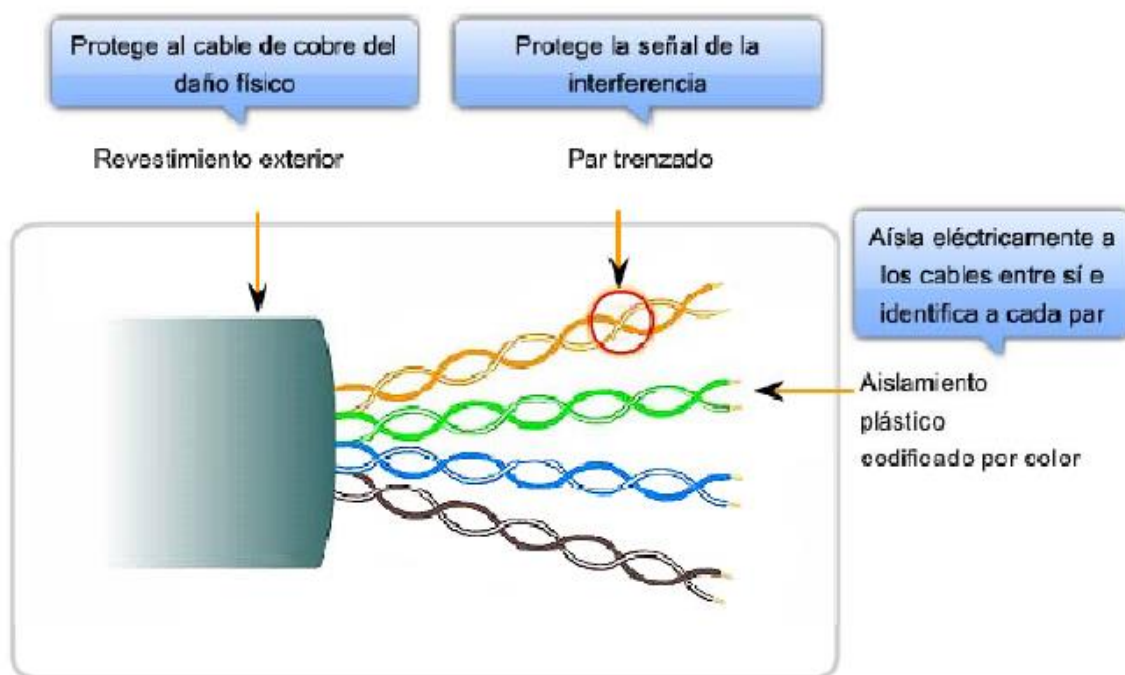


Figura A.3 Estructura del cable UTP

Categorías del cable UTP

En las diferentes categorías que hay se especifican las características eléctricas, atenuación, capacidad de la línea e impedancia; actualmente existen 11 categorías dentro del cable UTP.

- a) Categoría 1: Diseñado para redes telefónicas; empleado para transmitir voz y datos a baja capacidad. Alcanzan como máximo velocidades de hasta 4 Mbps.
- b) Categoría 2: De características similares al cable de categoría 1; con los cables normalizados al transmitir a 1 MHz.
- c) Categoría 3: Cable formado por 3 pares trenzados. Transmite a 16MHz y es utilizado en redes Ethernet a 10Mbps y Token Ring a 4Mbps.
- d) Categoría 4: Cable formado por 4 pares trenzados. Transmite a 20MHz y es utilizado en redes Token Ring a 16Mbps.
- e) Categoría 5: Cable formado por 4 pares trenzados. Transmite a 100MHz y es utilizado en redes Fast Ethernet.

APÉNDICE A

- f) Categoría 5e: Es una categoría 5 mejorada al minimizar la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque sí esta diferenciada por los diferentes organismos.
- g) Categoría 6: Es un estándar de cables para Gigabit Ethernet. Transmite a 250 MHz y es utilizado en redes 10GBASE-T, 100BASE-TX y 1000BASE-TX.
- h) Categoría 6a: No está estandarizada pero lleva el sello del fabricante, en algunos sitios ya está utilizándose. Puede llegar a transmitir hasta 550 MHz y es utilizado en redes 10GBASE-T Ethernet.
- i) Categoría 7: No está definida y mucho menos estandarizada. Transmitirá a 600 MHz. Tiene conectores Giga Gate-45 (es compatible con el RJ-45) y el TERA, al combinarse puede transmitir a la frecuencia ya mencionada.
- j) Categoría 7a: Para servicios de telefonía y televisión por cable Ethernet 1000BASE-T. Tiene 4 pares trenzados de cobre. Puede llegar a transmitir hasta 1200 MHz. Tiene conectores Giga Gate-45 (es compatible con el RJ-45) y el TERA, al combinarse puede transmitir a la frecuencia ya mencionada.
- k) Categoría 8: No está definida pero sigue en desarrollo. No tiene todavía una aplicación.

3. STP (Shielded Twister Pair, Par Trenzado Blindado)

Cable de par trenzado de 150 ohm en donde existe un recubrimiento de aluminio alrededor, de tal manera que impide interferencias eléctricas sobre los cables logrando así una inmunidad hacia el ruido, véase figura A.4. La distancia máxima sin necesidad de repetidores es de 200m. STP fue desarrollado por IBM, no se usa en redes Ethernet pero puede adaptarse a 10Base-T, 100Base-TX y 100Base-T2 aunque casi siempre es usado en redes Token Ring.



Figura A.4 Estructura del cable STP

4. FTP (Foiled Twisted Pair, Par trenzado con pantalla global)

Es como el cable UTP pero sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas. Su impedancia característica típica es de 120 Ohmios y sus propiedades de transmisión son más parecidas a las del UTP. Además, puede utilizar los mismos conectores RJ45. Tiene un precio intermedio entre el UTP y STP. La figura A.5 representa al cable FTP.



Figura A.5 Cable FTP

Conectores del par trenzado

- RJ45: Conector modular que puede contener hasta cuatro pares de cables. Es el más común para cableado de par trenzado sin blindaje (UTP), se utiliza en instalación de redes LAN.
- RJ11: Conector modular que puede contener hasta tres pares de cables. Es el más común para enlaces telefónicos; se utiliza en casas y oficinas.
- Armarios o Racks de Distribución: Crean sitio para los cables en aquellos lugares donde no hay mucho espacio libre en el suelo. Su uso ayuda a organizar una red que tiene muchas conexiones.
- Paneles de Conexiones Ampliables: Hay diferentes versiones que admiten hasta 96 puertos y alcanzan velocidades de transmisión de hasta 100 Mbps.
- Clavijas: Se usan los RJ-45 dobles o simples para conectarse en paneles de conexiones y placas de pared ya que alcanzan velocidades de datos de hasta 100 Mbps.
- Placas de pared: Permiten dos o más enganches.

APÉNDICE A

Par trenzado: ventajas y desventajas

Ventajas

- Bajo costo en su contratación.
- Alto número de estaciones de trabajo por segmento.
- Facilidad para el rendimiento y la solución de problemas.
- Puede estar previamente cableado en un lugar o en cualquier parte.

Desventajas

- Altas tasas de error a altas velocidades.
- Ancho de banda limitado.
- Baja inmunidad al ruido.
- Baja inmunidad al efecto crosstalk (diafonía)
- Alto costo de los equipos.

C) Fibra óptica (OPTICAL FIBER)

Si se conecta una fuente de luz en un extremo de la fibra y un detector en el otro se tiene un sistema de transmisión para datos unidireccionales que acepta una señal eléctrica que la convierte y transmite por pulsos de luz para después reconvertirla a una señal eléctrica en el extremo receptor. Este proceso puede observarse en la figura A.6.

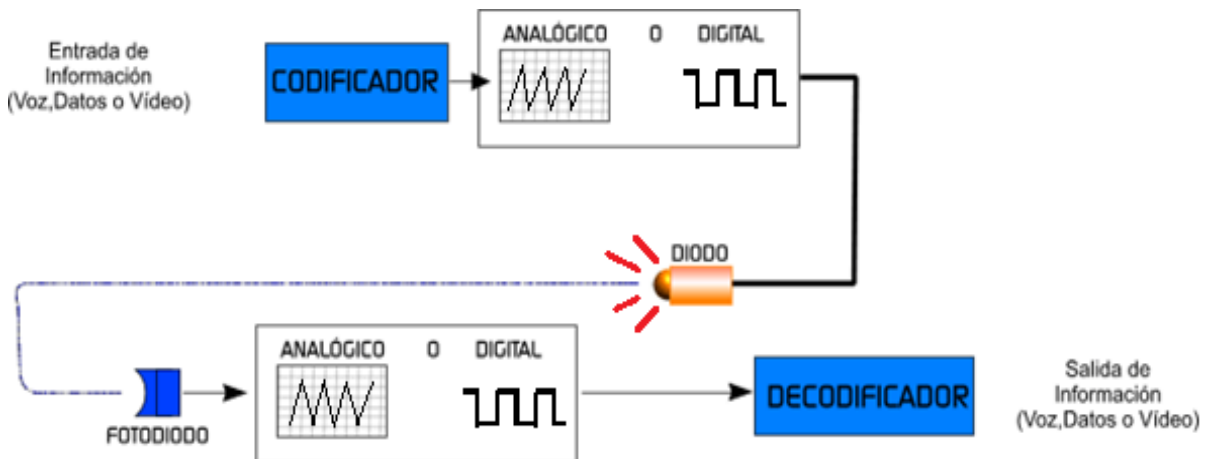


Figura A.6 Transmisión de la información por medio de fibra óptica

APÉNDICE A

Para que el sistema funcione debe seguir el principio de la física:

Cuando un rayo de luz pasa de un medio a otro, el rayo de luz se refracta con un cierto ángulo g . Como el ángulo de refracción depende de las propiedades de los dos medios (en particular, de sus índices de refracción), para ángulos de incidencia por encima de un cierto valor crítico, la luz se refracta sobre el mismo medio. Así, un rayo incidente con un ángulo igual o mayor que el crítico queda atrapado dentro del medio. Este principio se representa en la figura A.7.

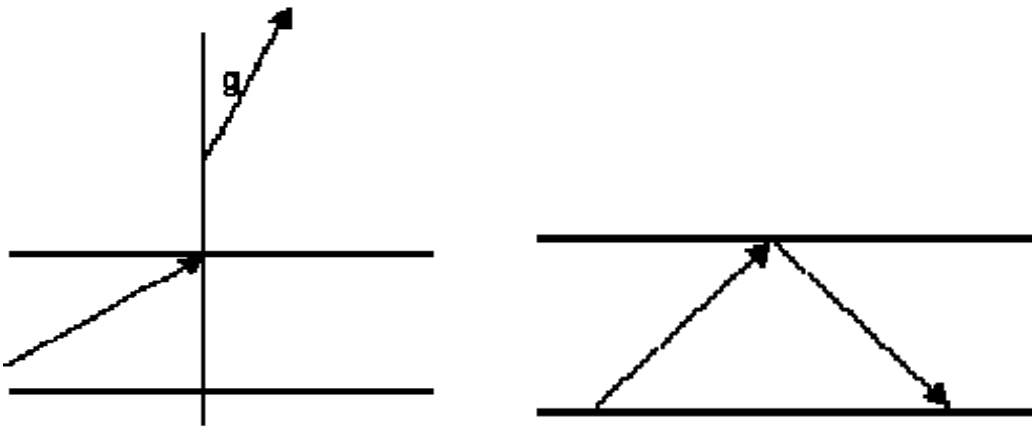


Figura A.7 Refracción de la luz con un cierto ángulo g (izquierda) y refracción de la luz con un ángulo igual o mayor que el crítico sobre el mismo medio (derecha)

La diferencia entre sus índices de refracción (indicados con n) es lo que hace que el haz de luz se mantenga dentro del núcleo (siempre que el haz haya entrado con el ángulo apropiado y el n del núcleo sea mayor que el del revestimiento).

La fibra óptica está formada por un núcleo rodeado de revestimiento, los cuales pueden ser de 3 maneras:

- Núcleo y revestimiento de plástico
- Núcleo de vidrio y revestimiento de plástico
- Núcleo y revestimiento de vidrio

Los conductores de fibra óptica comúnmente utilizados en transmisión de datos son de un grosor comparable a un cabello, variando el núcleo entre los 8 y los 100 μm (micrones), y el revestimiento entre 125 y 140 μm . Véase en la figura A.8.

APÉNDICE A

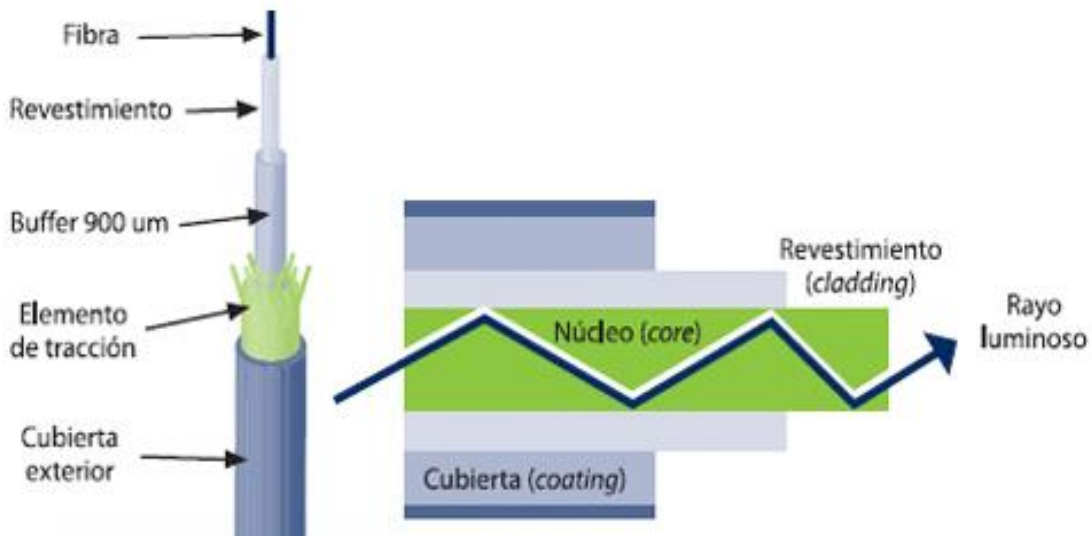


Figura A.8 Interior de un conductor de fibra óptica

1. Fibra Multimodo

Viajan varios rayos ópticos reflejándose a diferentes ángulos, los diferentes rayos ópticos recorren diferentes distancias y se separan al viajar dentro de la fibra (figura A.9). La distancia a la que se puede transmitir está limitada.

Las principales características de la fibra multimodo son:

- Usa láser
- El recubrimiento es anaranjado
- Usado en redes LAN

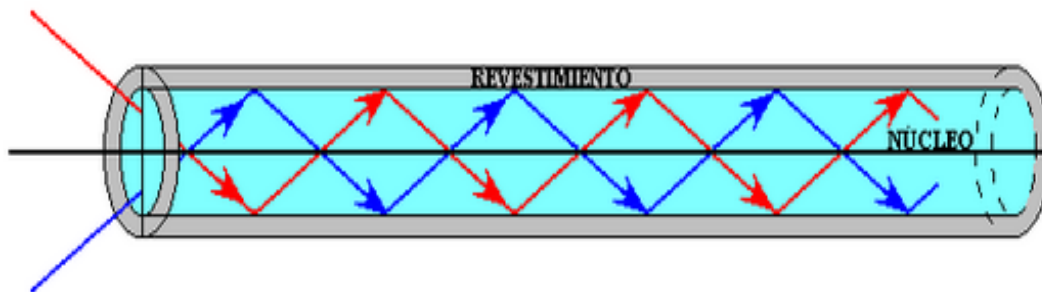


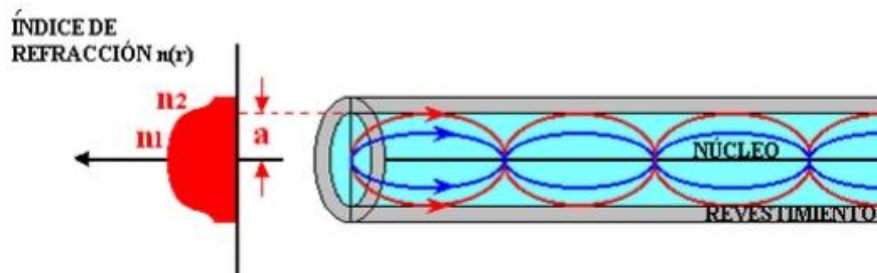
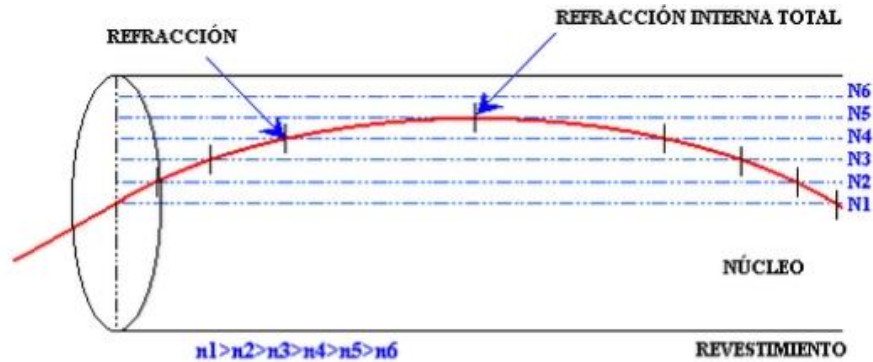
Figura A.9 Recorrido de los rayos ópticos reflejándose a diferentes ángulos en la fibra multimodo

2. Fibra Multimodo con índice graduado

El núcleo está hecho de varias capas concéntricas de material óptico con diferentes índices de refracción. Los rayos se propagan en trayectorias curvas (figura A.10). En esta

APÉNDICE A

fibra el número de rayos ópticos diferentes que viajan es menor. Tienen una banda de paso que llega hasta los 500 MHz por kilómetro.



LOS RAYOS SIGUEN TRAYECTORIAS CURVAS

Figura A.10 Refracción de los rayos en forma de curvas con índice graduado

3. Fibra Multimodo de índice escalonado

Están fabricadas a base de vidrio con una atenuación de 30 dB/km o plástico con una atenuación de 100 dB/km. Tienen una banda de paso que llega hasta los 40 MHz por kilómetro. En esta fibra, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea. El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice por lo cual se llama índice escalonado (figura A.11).

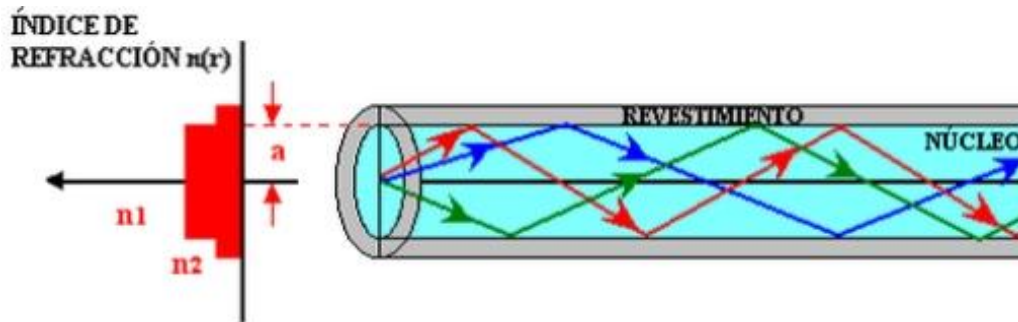


Figura A.11 Refracción de los rayos con índice escalonado

APÉNDICE A

4. Fibra Monomodo

Es de menor diámetro y solamente permite viajar al rayo óptico central (figura A.12), ofrece la mayor capacidad de transporte de información ya que una banda de paso del orden de 100 GHz/km. No sufre del efecto de las otras pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mayores.

Las principales características de la fibra monomodo son:

- Usa led
- El recubrimiento es amarillo o azul.
- Mayor potencia que el multimodo.
- Permite transmisión a grandes distancias.



Figura A.12 Interior de la fibra monomodo

Las velocidades que alcanza la fibra óptica:

- STM-1 150 Mbps
- STM-4 622 Mbps
- STM-16 2.5 Gbps
- STM-64 10 Gbps
- STM-256 40 Gbps

Conectores para fibra óptica:

- ST (Straight Tip, Punta recta). Se sujeta a la fibra por medio de una aguja y un cilindro que son cerámicos, aunque los hay de metal o plástico.
- SC (Subscriber Connector, Conector de precisión). Conector utilizado en enlaces más delicados, es un conector muy confiable pero costoso. Conector de forma cuadrada.
- FC (Ferrule Connector, Conector de virola). Se usa en la transmisión de datos y en telecomunicaciones.

APÉNDICE A

- FDDI (Fiber Distributed Data Interface, Interfaz de Datos de Fibra Distribuida), se usa para redes de fibra óptica.
- LC (Lucent Connector o Local Connector, Conector Local) y MT-RJ (Mechanical Transfer Registered Jack, Transferencia Mecánica del Registro de Jack) que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC (Bayonet Fiber Optic Connector, Conector de Bayoneta de Fibra Óptica) se usa en redes de edificios y en sistemas de seguridad.

En la siguiente figura A.13, se aprecian los conectores para fibra óptica:



Figura A.13 Conectores para fibra óptica

Fibra óptica ventajas y desventajas

Ventajas:

- Alta velocidad de propagación.
- Poca atenuación a largas distancias.
- Resistencia a la corrosión.
- Se puede instalar en medios explosivos.
- Inviolabilidad a la conexión.
- Insensibilidad a la interferencia electromagnética.

APÉNDICE A

- Las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada.
- Carencia de señales eléctricas en la fibra.
- Livianidad y reducido tamaño del cable capaz de llevar un gran número de señales.
- Sin puesta a tierra de señales, como ocurre con alambres de cobre que quedan en contacto con ambientes metálicos.
- Compatibilidad con la tecnología digital.
- Fácil de instalar.

Desventajas:

- El costo es elevado.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.

Fibra óptica en aplicaciones comerciales

- Portadores comunes telefónicos y no telefónicos.
- Televisión por cable.
- Enlaces y bucles locales de estaciones terrestres.
- Automatización industrial.
- Controles de procesos.
- Aplicaciones de computadora.
- Aplicaciones militares.

APÉNDICE B

1. AMENAZAS

Ejemplos de amenazas según su clasificación dependiendo de las fuentes que las generan:

a) Factor humano

1. Curiosos: Se trata de personas que entran a los sistemas (en algunos casos de manera accidental) a los que no están autorizados, motivados por la curiosidad, por el desafío personal, o por el deseo de aprender o averiguar. Generalmente este tipo de intruso no tiene el conocimiento apropiado para lograr causar daño, pero no por eso se les debe ignorar sin tomar las precauciones necesarias.
2. Intruso remunerado: Se encarga de penetrar a los sistemas a cambio de un pago ya que se trata de personas que poseen los conocimientos, experiencia y herramientas necesarias para penetrar en los sistemas, incluso aquellos que tienen un nivel alto de seguridad.
3. Personal enterado: Se trata de personas que tienen acceso autorizado o conocen la estructura del sistema de cierta organización. Por lo general, son el mismo personal interno o un ex empleado, sus motivaciones van desde revanchas personales hasta ofertas y remuneraciones de organizaciones rivales.
4. Terroristas: Tienen como objetivo causar daños con diferentes fines, por ejemplo proselitistas o religiosos.
5. Robo: Se refiere a la extracción física de la información por medio de unidades de almacenamiento, robo físico de los componentes de hardware del sistema e incluso también se considera como robo el usar los equipos para actividades diferentes a las asignadas por la organización.
6. Sabotaje: Consiste en reducir la funcionalidad del sistema por medio de acciones deliberadas dirigidas a dañar los equipos, logrando la interrupción de los servicios e incluso la destrucción completa del sistema. Puede ser perpetuada por el personal interno o por opositores externos.
7. Fraude: Esta actividad no tiene como prioridad ponerle fin al sistema sino aprovechar los recursos que se manejan para obtener beneficios ajenos a los objetivos de la organización.

APÉNDICE B

8. Ingeniería social: Es la práctica de obtener información confidencial a través de la manipulación del usuario legítimo llevándolo a revelar información sensible o bien a violar las políticas de seguridad. Generalmente se está de acuerdo con que *los usuarios son el eslabón débil* en seguridad; éste es el principio por el que se rige la ingeniería social.
9. Ingeniería social inversa: Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en la ingeniería social.

b) Errores de hardware

1. Mal diseño: Es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios.
2. Errores de fabricación: Es cuando las piezas de hardware son adquiridas con defectos de fabricación y posteriormente fallan al momento de intentar usarse.
3. Suministro de energía: Las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos para que no se acorte su vida útil.
4. Desgaste: El uso constante del hardware produce un desgaste considerado como normal, con el tiempo este desgaste reduce el funcionamiento óptimo del dispositivo hasta dejarlo inutilizable.
5. Descuido y mal uso: Todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor que trae como consecuencia descomposturas prematuras y reducción del tiempo de vida útil de los recursos.

c) Errores de la red

1. Topología seleccionada: Dependiendo el alcance y recursos compartidos en una red, puede ser más conveniente seleccionar una topología sobre otra, pero debe tomarse en cuenta que las desventajas de cada arquitectura no solo limitan la comunicación, incluso pueden dejar la red fuera de servicio.
2. Sistema operativo: Aunque el modelo OSI permite la comunicación entre equipos con diferentes sistemas operativos, se dan casos en los que ciertas opciones de operación difieren entre sistemas operativos, haciendo difícil el compartir ciertos recursos.

3. Incumplimiento de las normas de instalación de la red: La instalación del cableado físico de las redes de datos, debe seguir ciertas normas y estándares de diseño conocido como cableado estructurado. No tomar en cuenta estos puntos puede resultar en fallas de diseño que causen problemas de transmisión de datos, inoperabilidad o indisponibilidad de los recursos de red.

d) Software

1. Software de aplicación: No fue creado específicamente para realizar ataques, pero tiene características que pueden ser usadas de manera maliciosa para atacar un sistema.
2. Código malicioso: Es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas para modificar, obtener control o perjudicar.
3. Virus: Es un tipo de código malicioso que tiene como principal característica la capacidad de duplicarse a sí mismo usando recursos del sistema infectado, propagándose rápidamente; además, reemplaza archivos ejecutables por otros infectados con el código de éste.
4. Troyanos: En sentido estricto, un troyano no es un virus, aunque se considere como tal. Realmente es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.
5. Gusanos: Es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él y aprovecha los recursos del sistema infectado.
6. Errores de programación y diseño: Ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos ya que no fue diseñado para dar soporte a una organización. Los errores y fallas más generales que tiene una aplicación también representa una amenaza.

2. CLASIFICACIÓN DE ATAQUES

Algunos ejemplos de ataques de este tipo son:

a) Ataques de suplantación o contra la autenticación

1. Spoofing-Looping: Se traduce como hacerse pasar por otro, el objetivo de esta técnica es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, luego utiliza este para entrar en otro y así sucesivamente. Este proceso tiene la finalidad de *evaporar* la identificación y la ubicación del atacante.
2. Spoofing: Para realizar este ataque es necesario tener conocimiento del protocolo en el que se va a basar el ataque. Los ataques más conocidos son el IP Spoofing, DNS Spoofing, Web Spoofing, utilización de BackDoors, obtención de contraseñas y uso de diccionarios.
3. IP Spoofing: El atacante genera paquetes que proveerán de Internet con una dirección de red falsa en el campo origen, que será aceptada por el destinatario del paquete. Su uso más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima *observa* un ataque proveniente de esa tercera red y no la dirección real del intruso. El esquema con dos puentes es el siguiente (figura B.1):

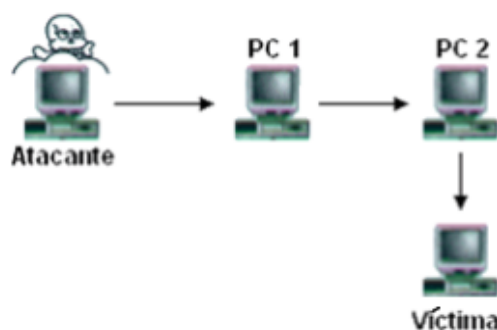


Figura B.1 Ataque Spoofing. Si la víctima descubre el ataque verá a la PC 2 como su atacante y no al verdadero origen.

4. DNS Spoofing: Se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el DNS. Si se permite el método de recursión en la resolución de *Nombre/Dirección IP* en el DNS, es posible controlar algunos aspectos del DNS remoto.

APÉNDICE B

5. Web Spoofing: El atacante crea un sitio web falso similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las contraseñas, números de tarjeta de créditos, etcétera. El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.
6. BackDoors: Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. Se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales.
7. Obtención de Contraseñas: Comprende la obtención por fuerza bruta de las claves que permiten ingresar a los sistemas, aplicaciones y cuentas de los atacados. Generalmente las contraseñas de acceso son obtenidos fácilmente porque involucran el nombre u otro dato familiar del usuario y esta rara vez se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y *diccionarios* que prueban millones de posibles claves hasta encontrar la contraseña correcto.
8. Uso de diccionarios: Es un archivo con millones de palabras, las cuales pueden ser posibles contraseñas de los usuarios. Este archivo es utilizado para descubrir dicha contraseña en pruebas de fuerza bruta. El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, compara la palabra encriptada contra el archivo de contraseñas del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada. En la tabla B.1, podemos observar el tiempo de búsqueda de una clave de acuerdo con su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100,000 contraseñas por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

APÉNDICE B

Tabla B.1 Cantidad de claves generadas según el número de caracteres empleados

Cantidad de Caracteres	26–Letras minúsculas	36–Letras y dígitos	52–Mayúsculas y minúsculas	96–Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

b) Ataques de interceptación o contra la confidencialidad

1. Syn Flood: Es un ataque de denegación de servicio y se basa en un *saludo* incompleto entre los dos hosts. El cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el host hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna), el servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.
2. Eavesdropping–packet sniffing: Muchas redes son vulnerables al Eavesdropping o a la pasiva interceptación (sin modificación) del tráfico de red. Un sniffer consiste en colocar en la tarjeta de red un modo llamado *promiscuo*, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta tarjeta (computadora donde está instalado el sniffer).
3. Snooping downloading: Esta categoría tiene el mismo objetivo que el sniffing: obtener información sin modificarla. Sin embargo, los métodos son diferentes. En este caso, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.
4. TCP SYN scanning: La identificación del servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto que depende para la conexión. El cliente establece la conexión con el servidor a través del puerto disponible para luego intercambiar datos. El establecimiento de dicha conexión se realiza mediante Three-Way Handshake (conexión en tres pasos) ya que intercambian tres segmentos. En forma esquemática se representa en la figura B.2:

APÉNDICE B

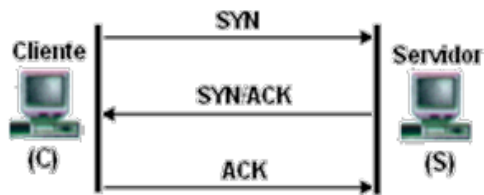


Figura B.2 Conexión de tres pasos

5. TCP FIN scanning– stealth port scanning: Hay veces que incluso el escaneo SYN no es lo suficientemente limpio. Algunos sistemas (firewalls y filtros de paquetes) monitorean la red en busca de paquetes SYN a puertos restringidos. Para solucionar este inconveniente los paquetes FIN podrán ser capaces de pasar sin ser advertidos. Este tipo de escaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

c) Ataques de interrupción o contra la disponibilidad

1. Jamming o Flooding: Desactiva o satura los recursos del sistema ya que un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico que sature la red o el sistema con mensajes que requieren establecer conexión con la finalidad de que nadie más pueda utilizarla.
2. Smurf o Broadcast Storm: Consiste en recolectar una serie de direcciones broadcast para mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima). Este paquete maliciosamente manipulado, será repetido en difusión broadcast a cientos o miles de hosts que mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP (figura B.3).

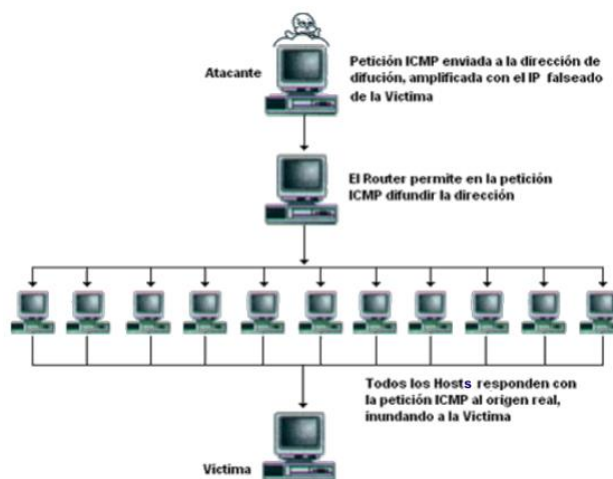


Figura B.3 Ataque Smurf

3. Land Attack: Consiste en un bug (error) en la implementación de la pila TCP/IP de las plataformas Windows. Se realiza mandando a algún puerto abierto de un servidor (generalmente al NetBIOS con puertos 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.
4. OOB Supernuke o winnuke: Es un ataque para los equipos con Windows ya que éstos van a escuchar por el puerto NetBIOS sobre TCP/UDP 137 a 139, quedando fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados. Generalmente se envían fragmentos de paquetes Out Of Band (fuera de banda), que la máquina víctima detecta como inválidos pasando a un estado inestable. Al configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido. Este ataque puede prevenirse instalando los parches adecuados suministrado por el fabricante del sistema operativo afectado o teniendo instalado un filtro que garantice la detección de una inundación de bits Urgentes.
5. E-Mail Bombing–Spamming: Consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario. El spamming, en cambio se refiere a enviar un e-mail a miles de usuarios, hayan solicitado el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.

d) Ataques de modificación o contra la integridad

1. Teardrop I y II-Newtear-bonk-boink: Estos ataques afectan a los fragmentos de los paquetes ya que no se vuelven a armar correctamente los fragmentos que se superponen, haciendo que el sistema se cuelgue. Windows NT 4.0 de Microsoft es especialmente vulnerable a este ataque.
2. Tampering o data diddling: Es la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Cuando la persona que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. El administrador va a necesitar dar de baja el sistema por horas o días hasta checar y tratar de recuperar aquella información que haya sido alterada o borrada.
3. Borrado de huellas: Las huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo. Los archivos logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

Es una de las tareas más importantes que debe realizar el intruso después de ingresar a un sistema, ya que, si se detecta su ingreso, el administrador buscará cómo conseguir *tapar el hueco* de seguridad, evitar ataques futuros e incluso rastrear al atacante.

4. Hoaxes, jokes o bulos: Son bromas que asemejan ser virus, pero no lo son. Normalmente una persona conocida recibe una *alarma* de un supuesto virus y *hace el favor* de notificar para que se tomen precauciones en el equipo. El objetivo de la persona que inició el rumor o hoax se ha cumplido, al preocupar al usuario con la broma y que, en muchos casos, puede hacer al usuario auto eliminar algún supuesto archivo contaminado, lo cual podría afectar realmente al funcionamiento del sistema, llegando incluso a tener que reinstalarlo.
5. Parásito Informático: Tipo de malware en el que se adhieren archivos (especialmente ejecutables), como lo haría un parásito. Ese archivo ejecutable es denominado portador (o host) y el parásito lo utiliza para propagarse. Si el programa es ejecutado, lo primero que se ejecuta es el parásito informático, y luego, para no levantar sospechas, se ejecuta el programa original. Muchas veces es aquí donde los parásitos fallan, porque hay programas que detectan estas modificaciones y lanzan errores (incluso errores de advertencias de presencia de malware).

3. SEGURIDAD FÍSICA

A continuación se analizan los peligros más importantes que se corren en un centro de cómputo; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

1. Incendios

Son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas, el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad ya que es considerado el enemigo número uno de las computadoras al destruir fácilmente los archivos de información y programas.

Los sistemas antifuego en muchas de las ocasiones dejan mucho que desear porque causan casi el mismo daño que lo haría el fuego, sobre todo a los elementos electrónicos.

APÉNDICE B

Al usar dióxido de carbono que es una alternativa para no usar agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

Los factores para reducir los riesgos de un incendio en un centro de cómputo son:

- a) El área en la que se encuentran las computadoras debe estar en un lugar que no sea combustible o inflamable.
- b) El lugar no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- c) Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- d) Deben tener un piso falso instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- e) No debe estar permitido fumar en el área de proceso.
- f) Deben emplearse muebles incombustibles y cestos metálicos para papeles.
- g) Deben evitarse los materiales plásticos e inflamables.
- h) El piso y el techo en el centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos solo sea para uso del personal autorizado. Es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados, como son:

- a) Proteger el sistema contra daños causados por el humo.
- b) La temperatura no debe sobrepasar los 18°C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- c) Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- d) Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores). El personal designado para usar extinguidores debe ser entrenado en su uso.
- e) Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.
- f) Suministrar información del centro de cómputo al departamento local de bomberos antes de que ellos sean llamados en una emergencia para que estén conscientes de las particularidades y vulnerabilidades del sistema, por las excesivas cantidades de agua y la conveniencia de una salida para el humo.

2. Inundaciones

Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por la falta de drenaje ya sea natural o artificial.

Esta es una de las causas de mayores desastres en los centros de cómputo. En las causas naturales de inundaciones puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se puede tomar en cuenta la siguiente medida: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

3. Condiciones climatológicas

Normalmente en la radio o la televisión se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tomadas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

Los terremotos son fenómenos sísmicos que pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba.

4. Señales de radar

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiado desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro o mayor. Esto podría ocurrir solo si la antena respectiva fuera visible desde una ventana del centro de cómputo y en algún momento estuviera apuntando directamente hacia dicha ventana.

5. Instalaciones eléctricas

Al usar computadoras implica trabajar con electricidad, por lo tanto ésta es una de las principales áreas a considerar en la seguridad física. En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos pero favorecer la escucha electrónica.

Los cables que se suelen utilizar para construir las redes locales van desde el cable telefónico normal hasta el cable coaxial o la fibra óptica.

Los riesgos más comunes del cableado son:

- a) Interferencia: son modificaciones que pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración de los datos que viajan a través de él.
- b) Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- c) Daños en el cable: los daños normales con el uso pueden afectar el apantallamiento que preserva la integridad de los datos transmitidos lo que hace que las comunicaciones dejen de ser fiables. El cable de red puede ser atacado por un intruso que intenta acceder a los datos para desviar o estableciendo una conexión no autorizada en la red. Un sistema de administración y procedimiento de identificación de acceso adecuado hará difícil que se puedan obtener privilegios de usuario en la red.

Las redes con cables de alto nivel de seguridad son recomendadas para instalaciones con un grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreo de la información que circula por el cable. Consta de un sistema de tubos herméticamente cerrados por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

APÉNDICE B

La mayoría de los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser alojados en los pisos de placas extraíbles que están arriba del piso de concreto.

Todo cuarto de cómputo debe tener un sistema de aire acondicionado que se dedique de forma exclusiva a la calefacción y ventilación de equipos. Teniendo en cuenta que los aparatos de aire acondicionado son una causa potencial de incendios e inundaciones es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Las emisiones electromagnéticas con baja frecuencia que generan algunos periféricos son dañinas para el ser humano. Se recomienda tener filtros adecuados al rango de las radiofrecuencias para que éstas sean totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

6. Ergometría

Es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible. Entre los fines de su aplicación se encuentra fundamentalmente la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro. Los principales trastornos son:

- a) Óseos y/o muscular: Una manera de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural. Al usar el teclado y mouse de una computadora se hacen movimientos repetitivos y continuos, el teclado tiene un distribución ineficiente en las teclas así como un diseño antinatural, por tal motivo se tiene un potencial riesgo de enfermedades o lesiones en los músculos, nervios y huesos de manos y brazos.
- b) Visual: Los ojos son la parte más afectada por el trabajo con computadora ya que la pantalla es una fuente de luz que incide directamente sobre el ojo del operador provocando después de periodos largos de exposición cansancio visual, irritación y lagrimeo, cefalea y visión borrosa. Para prevenir los trastornos visuales en los operadores podemos tomar en cuenta:

APÉNDICE B

- I. Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
 - II. Usar pantallas antirreflejo o anteojos con protección para el monitor, es una medida preventiva importante y de bajo costo.
- c) Salud mental: El trabajo informático disminuye los desplazamientos de los trabajadores y las tareas requieren un menor esfuerzo muscular y dinámico pero aumenta al mismo tiempo la carga estática de las posturas inadecuadas asumidas. El estrés informático se está convirtiendo en una nueva enfermedad profesional que se relaciona con el trabajo al provocar una carga mental y psíquica inherente a la operación de los nuevos equipos. Los efectos del estrés pueden ser:
- I. Efectos fisiológicos inmediatos: caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardiaca, etcétera. Estos efectos hacen referencia a la tensión, irritabilidad, cólera, agresividad. Los sentimientos pueden inducir ciertos efectos en el comportamiento tales como el consumo de alcohol y psicofármacos, el hábito de fumar, etcétera.
 - II. Existen consecuencias médicas a largo plazo como enfermedades coronarias, hipertensión arterial, úlceras pépticas, agotamiento; mientras que las consecuencias psicológicas a largo plazo pueden señalar neurosis, insomnio, estados crónicos de ansiedad y/o depresión, etcétera.
 - III. La apatía es una sensación de insatisfacción ante la vida, la pérdida de la propia estima, alteran profundamente la vida personal, familiar y social del trabajador llevándolo, eventualmente, al aislamiento, al ausentismo laboral y la pérdida de la solidaridad social.
- d) Ambiente luminoso: las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.
- e) Ambiente climático: la temperatura de una oficina con computadoras debe estar entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. El ambiente sonoro se recomienda que no supere los 55 decibeles sobre todo cuando trabajan muchas personas en un mismo espacio.

7. Robo

Las computadoras son posesiones valiosas de las empresas y están expuestas de la misma forma que lo están las piezas de stock e incluso el dinero. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información a los que dan menor protección que la

APÉNDICE B

que otorgan a una máquina de escribir o una calculadora. El software es una propiedad fácilmente sustraíble, las cintas y discos son fácilmente copiados sin dejar ningún rastro.

8. Fraude

Cada año millones de dólares son sustraídos de empresas y en muchas ocasiones las computadoras han sido utilizadas como instrumento para dichos fines. Debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etcétera.), tienen algo que ganar sino que más bien pierden prestigio y no se da ninguna publicidad a este tipo de situaciones ya que afectarían directamente a la empresa.

9. Sabotaje

El peligro más temido en los centros de cómputo de datos es el sabotaje. Las empresas han intentado que implementar programas de seguridad de alto nivel y han encontrado que la protección contra el saboteador es uno de los retos más duros. Éste puede ser un empleado o un sujeto ajeno a la propia empresa. De manera física los imanes son las herramientas a las que más recurren los atacantes ya que con una ligera pasada la información desaparece aunque las cintas estén almacenadas en el interior de su funda protectora.

10. Utilizar guardias

El servicio de vigilancia es el encargado del control de acceso de todas las personas del edificio. Este servicio se encarga de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal. Cualquier persona ajena a la planta se le solicitará completar un formulario de datos personales donde se pide: *los motivos de la visita, hora de ingreso y de egreso.*

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa. La desventaja del uso de credenciales es que las tarjetas pueden ser copiadas, robadas, permitiendo ingresar a cualquier persona que la posea. Las credenciales se pueden clasificar de la siguiente manera:

- a) Normal o definitiva: Para el personal permanente de planta.
- b) Temporaria: Para personal recién ingresado.
- c) Contratistas: Personas ajenas a la empresa que por razones de servicio deben ingresar a la misma.
- d) Visitas.

APÉNDICE B

El personal puede acceder a las instalaciones de la empresa mediante una contraseña que se solicitará a su ingreso. La desventaja de este método es que generalmente se eligen contraseñas sencillas o bien se olvidan, las bases de datos pueden ser alterada o robadas por personas no autorizadas.

La principal desventaja de tener personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr tener acceso a sectores donde no esté habilitado, así como ingresar o egresar de la planta con materiales no autorizados. Esta situación de soborno es muy frecuente por lo que es recomendable utilizar sistemas biométricos para el control de acceso.

Si se utiliza un control vehicular para el ingreso y egreso de autos el personal de vigilancia debe anotar en una planilla los datos personales de los ocupantes, la marca y modelo del vehículo así como la hora de ingreso y egreso de la empresa.

11. Detectores de metales

Es un elemento sumamente práctico para la revisión de personas ofreciendo grandes ventajas sobre el sistema de palpación manual. La sensibilidad del detector es regulable permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma. La utilización de este tipo de detectores debe hacerse conocer a todo el personal para que actúe como elemento disuasivo.

12. Sistemas biométricos

Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Las principales ventajas de este método son:

- a) Pueden eliminar la necesidad de poseer una tarjeta para acceder.
- b) Utilizando un dispositivo biométrico los costos de administración son más pequeños al solo tener que realizar el mantenimiento del lector y solo una persona se encarga de mantener la base de datos actualizada. Las características biométricas de una persona son intransferibles a otra.

Los diferentes sistemas biométricos son:

- a) Emisión de calor: Mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

APÉNDICE B

- b) Huella digital: Se basa en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos (llamados minucias), dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.
- c) Verificación de voz: La dicción de una o más frases es grabada y el acceso se compara a la voz (entonación, diptongos, agudeza). Tiene la desventaja que es muy sensible a factores externos como el ruido, el estado de ánimo, enfermedades de la persona y el envejecimiento.
- d) Verificación de patrones oculares: se basa en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos ya que en 200 millones de personas la probabilidad de coincidencia es casi 0. La principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en las mismas enfermedades que en ocasiones se prefiere mantener en secreto.

13. Verificación automática de firmas (VAF)

Es posible para un falsificador producir una buena copia visual de una firma pero es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud. La VAF usa emisiones acústicas toma datos del proceso dinámico de firmar o de escribir, así la secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo costo y robusto, consta de un bloque de metal y una computadora barata.

14. Seguridad con animales

Sirven para cubrir grandes extensiones de terreno ya que tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo, generalmente el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema. Posee la desventaja de que los animales pueden ser engañados para tener el acceso deseado.

15. Protección electrónica

Su nombre proviene de la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Dichas centrales están conectadas a los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Si un sensor detecta una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información

APÉNDICE B

recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Los métodos más usados son:

- a) Barreras Infrarrojas y de Micro-Ondas: Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Las barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa. Si el haz es interrumpido, se activa el sistema de alarma y luego vuelve al estado de alerta. Las barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire.

Las invisibles barreras fotoeléctricas llegan a cubrir hasta 150 metros de longitud (distancias exteriores). La principal ventaja es la capacidad de atravesar ciertos materiales como el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

- b) Detector ultrasónico: Utiliza ultrasonidos para crear un campo de ondas y así cualquier movimiento que realice un cuerpo dentro del espacio protegido generará una perturbación en dicho campo que accionará la alarma. El circuito posee un refinado sistema que elimina las falsas alarmas y su cobertura máxima es de 40 metros cuadrados.
- c) Detectores pasivos sin alimentación: Los elementos no requieren alimentación extra de ningún tipo, solo van conectados a la central de control de alarmas para mandar la información de control. Los detectores más usados son:
- I. Detector de aberturas: Contactos magnéticos externos o de embutir.
 - II. Detector de roturas de vidrios: Inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable.
 - III. Detector de vibraciones: Detecta golpes o manipulaciones extrañas sobre la superficie controlada.
- d) Sonorización y dispositivos luminosos: Los elementos de sonorización son las sirenas, campanas, timbres. Los dispositivos luminosos son los faros rotativos, balizas, luces intermitentes. Éstos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

- e) Circuito cerrado de televisión: Controla todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad y las cámaras pueden estar a la vista (siendo utilizada como medida disuasiva) u ocultas (evitando que el intruso sepa que está siendo captado por el personal de seguridad). Estos elementos poseen un control contra sabotaje de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

- f) Edificios inteligentes: Es una estructura que facilita a los usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Propone la integración de todos los sistemas existentes dentro del edificio como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción y aire acondicionado) y todas las formas de administración de energía. La característica principal es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

4. HERRAMIENTAS DE MONITOREO

Algunas herramientas para el monitoreo de redes son:

- a) *NetSupport Manager 10.5*

Esta herramienta puede monitorear cualquier tipo de red, es compatible con los sistemas operativos: Linux, Windows, Solaris, Mac, etcétera. Permite ver qué hacen las demás personas y tener el control del equipo remoto. Mejora la seguridad, comunicación o transferencia de datos. Sus principales características son:

1. Autenticación de tarjetas inteligentes (SmartCards).
2. Directorio activo.
3. Internet gateway (tiene acceso a Internet sin hacer cambios en el firewall local).
4. Transferencia de archivos.
5. Miniaturas ampliables (soportan sistemas con múltiples monitores).
6. NetSupport School (solución completa de control remoto).
7. NetSupport Manager (proporciona soporte a los sistemas operativos).
8. TotemGuard (aumenta los niveles de productividad, reduce recursos económicos y asegura los sistemas más críticos del negocio).

APÉNDICE B

b) *PRTG Network Monitor*

Asegura el funcionamiento de los sistemas informáticos y evita fallos en la red. Ayuda a optimizar la red ya que facilita la información detallada sobre el uso de la banda ancha y otros recursos de la red. PRTG ayuda a optimizar la infraestructura de la red y sus principales características son:

1. Evita las pérdidas causadas por fallos en la red sin detectar.
2. Reduce los costos del ancho de banda y hardware según las necesidades reales.
3. Mejora el rendimiento y el monitoreo de red que ayuda a evitar la saturación de la red

c) *Observer*

Es un analizador de protocolos para Ethernet, Inalámbricos 802.11b y 802.11a, Token Ring y FDDI. Además, mide, captura y predice tendencias de las redes. Se ejecuta en Windows. Monitorea y sirve como herramienta para resolver problemas que se presentan en las redes.

d) *Expert Observer*

Analiza y monitorea redes en tiempo real al manejar los datos para predecir tendencias y posibles escenarios de solución. De manera automática manda una serie de eventos de alertas para tomar decisiones a tiempo.

e) *Observer Suite*

Rastrea múltiples dispositivos SNMP, la información del análisis y modelaje experto se despliega en reportes vía web. La herramienta analiza, monitorea, predice tendencias de un solo segmento de su red o de todas sus redes LAN o WLAN.

f) *Observer Probes*

Los probes o examinadores se basan en software que permite un análisis y monitoreo remoto de redes: 10/100 Ethernet, 802.11 a/b/g Wireless, Token Ring y FDDI. Este examinador (probes) se basa en hardware que reporta a las consolas Observer Suite la información de la actividad de la red que analizan y monitorea sin la necesidad de desplazarse a otra ubicación, está disponible para redes wire-speed (velocidad de cable), full-duplex Gigabit y T1/E1.

APÉNDICE B

g) *Agente de Tráfico Internet (Internet Traffic Agent) 2.6*

Monitorea el tráfico de Internet de manera detallada sobre cualquier dirección IP al mostrar la ubicación geográfica (país) y el nombre del servidor, guarda un historial de las páginas que ha visitado el usuario, crea estadísticas del tráfico diario local, de Internet y HTTP, captura todos los paquetes IP en la red de área local, mide el tráfico de Internet, LAN o de un usuario específico, detecta a los usuarios con mayor actividad y monitorea su propia actividad de red.

h) *WhatsUp Gold Syslog Server 1*

Guarda, observa o reenvía fácilmente los mensajes de syslog desde cualquier punto de la red. Sus principales características son:

1. Muestra mensajes en tiempo real.
2. Se pueden configurar 10 usuarios con perfiles destacados.
3. Creación de reglas flexibles de procesamiento de mensajes.
4. Configurable rotación de archivos de registro.
5. Recibe y procesa mensajes en formatos RFC 3164, 5424 y UNIX.
6. Recibe mensajes desde varios dispositivos a través de protocolos UDP y TCP.
7. Reenvía mensajes utilizando los protocolos UDP y TCP.
8. Arranca como un servicio de Windows o en modalidad de aplicación.

i) *Monitoreo de redes de AthTek - Edición para Empresas (AthTek NetWalk Enterprise Edition) 2.0.15*

Captura paquetes y analiza el tráfico para poder administrar cualquier tipo de red. Crea representaciones gráficas del estado de la red usando capturas avanzadas de paquetes. Los filtros de paquetes integrados ayudan en la detección de intrusos y tienen soporte para todos los protocolos. Sus características principales son:

1. Navegación inteligente.
2. Mejora la captura de paquetes en todos los protocolos.
3. Agrega varias reglas de filtrado integradas como MSN y Yahoo Messenger.
4. Optimiza la interfaz y soporta completamente IPv6.
5. Soporta análisis de tráfico durante la captura de paquetes.
6. Se integra con Wireshark y logra un rendimiento mayor a éste.

APÉNDICE B

j) *AthTek NetWalk Edición Gratuita (AthTek NetWalk Free Edition) 2.0.15*

La herramienta puede analizar paquetes, gestiona la red doméstica, tiene una interfaz gráfica flexible, permite trazar la ruta desde la fuente de tráfico, soporta casi todos los tipos de protocolos de red incluyendo IPv6, los filtros de tráfico permiten identificar fácilmente las intrusiones para denegarles el acceso. Tiene las mismas características que el programa anterior (*Monitoreo de Redes de AthTek*).

k) *Verificador para red - Alertador limitado (Checklan Alerter Limited) 5.2.2*

Gestiona, actúa de forma remota en todos los contadores de rendimiento, procesos, impresoras, sockets, unidades, distribuciones, evita las interrupciones en servidores, evalúa las aplicaciones, repara automáticamente scripts y verifica todo lo concerniente a una dirección IP, proporciona informes en web o gráficos, no utiliza más memoria que la de su navegador local de Internet, genera registros y alarmas en informes simples que manda al correo electrónico. Gestiona los servicios de estado, arranque, parada y apagado remoto.

l) *Cisco Network Magic PRO*

Es un gestor de redes para usuarios inexpertos en administración, encuentra y corrige errores de configuración, mide la velocidad de conexión, protección de la conexión WiFi, administra los recursos compartidos: archivos, impresoras, unidades de disco duro, etcétera, controla el acceso a los diferentes contenidos de Internet permitiendo obtener el historial de navegación.

m) *Net Tools*

Monitorea y controla máquinas en red, controla los tiempos de respuestas, realiza inventarios de software y de hardware de estaciones remotas, lista los servicios locales, mide el ancho de banda, programa alarmas, traza rutas, localiza servidores DNS y escanea puertos; puede descubrir si alguien cambió su IP para simular que es otro ordenador o si han cambiado el nombre de la conexión de otro ordenador y verifica qué computadoras están en línea, cuál es su IP y su MAC.

n) *Net Control 2*

Controla y administra de manera remota cualquier red local doméstica, escolar, oficinas. Permite administrar múltiples ordenadores simultáneamente. Sus principales características son:

APÉNDICE B

1. Escritorio remoto: Controla el escritorio de cualquier equipo de la red como si se estuviera delante de él.
2. Administra programas: Ejecuta y finaliza programas, especifica restricciones para que no se puedan abrir ciertas aplicaciones.
3. Administra archivos: Todas las operaciones comunes de manejo de archivos.
4. Administra el apagado de equipos: Todas las acciones de encendido, apagado, reinicio, cierres de sesión, hibernación.
5. Administra el acceso a Internet: Es un cortafuego interno que está incluido.
6. Administra las restricciones del sistema: Determina a qué elementos y áreas del sistema se puede acceder y a cuáles no.
7. Mensajería instantánea y chat: Comunica de diversas formas con todos los equipos (mensajes de texto, sonidos, mensajería instantánea entre usuarios y administrador).

Las principales herramientas de seguridad son:

a) *Tcpdump*

Es una herramienta para el monitoreo y la adquisición de datos en redes. El programa permite volcar (un archivo, la pantalla, etcétera) el tráfico que presenta una red. Puede ser usado para imprimir los encabezados de los paquetes en una interfaz de red (network interface) que concuerden con una cierta expresión. Se puede usar esta herramienta para seguir problemas en la red, detectar los ataques de ping o para monitorear las actividades de una red.

b) *Abacus Portsentry*

Usa un demonio para la detección de barrido de puertos; además, tiene la habilidad de detectar estos barridos (incluyendo stealth scans) en la interfaz de red de la máquina. Como medida de alarma, puede bloquear al atacante por medio de la denegación al host, bloqueando el ruteo hacia la máquina hostil o por medio de reglas de firewall.

c) *DSniff*

Comprueba la integridad de archivos y directorios.

d) *Tripwire*

Ayuda a los administradores y usuarios de sistemas a monitorear alguna posible modificación en un set de archivos. Si se usa regularmente en los archivos de sistema puede notificar a los administradores del sistema si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo.

APÉNDICE B

e) *IP Filter*

Es un filtro de paquetes de TCP e IP adaptable para usarlo junto con un firewall. Puede ser utilizado como un módulo de kernel o incorporarlo al kernel de UNIX; Viene junto con scripts para instalarlo y parchar archivos de sistema si se requiere.

f) *Firewalk*

Es una técnica desarrollada por MDS y DHG que emplea técnicas del estilo de traceroute para determinar las reglas de filtrado que se están usando en un dispositivo de transporte de paquetes.

g) *Crack / Cracklib*

Es una versión de actualización del cracker local de contraseñas, permite a cualquier usuario de un sistema crackear el archivo `/etc/passwd` y determinar las contraseñas de otros usuarios (incluso la de root) en el sistema. Los sistemas modernos requieren de acceso a `/etc/shadow` para poder lograr esto. Sirve a los administradores que corren el cracker de vez en cuando para verificar que todos los usuarios tienen contraseñas fuertes.

h) *Nemesis*

Está diseñado para ser una pila de IP (IP stack) humana, portable y basada en línea de comandos para UNIX y Linux. El set está separado por protocolos y debería permitir crear scripts útiles desde un shell.

i) *Lids*

Es un sistema de detección y defensa de intrusión en Linux. El objetivo es proteger al sistema Linux para prevenir intrusiones a nivel de root, deshabilitando algunas llamadas al sistema del kernel mismo.

j) *IPLog*

Es una herramienta de registro de tráfico TCP e IP. Es capaz de registrar tráfico TCP, UDP, e ICMP.

APÉNDICE C

APÉNDICE C

1. ACCESS POINT (PUNTO DE ACCESO)

Características generales

- a) Permiten la conexión de dispositivos inalámbricos a la WLAN, como: Teléfonos celulares, Netbook, laptop, PDA e inclusive otros access point para ampliar las redes.
- b) Tiene un puerto RJ-45 que permite interconectarse con un switch inalámbrico y formar grandes redes entre dispositivos convencionales e inalámbricos.
- c) Se comunica a base de ondas de radio que son capaces de traspasar muros; sin embargo, entre cada obstáculo esta señal pierde fuerza y se reduce la cobertura.
- d) Puede ampliar la cobertura de la red y ser usado como un expansor de rango.
- e) En promedio la cobertura del radio empieza desde los 30 hasta más de 100 metros.
- f) Tiene una antena externa para la emisión y recepción de ondas.

Un access point funciona con los estándares o protocolos de las redes Wi-Fi e incluso en redes Bluetooth, los más usados pueden verse en la tabla C.1.

Tabla C.1 Estándares definidos para un access point

Estándar	Características	Velocidad (Mbps)
IEEE 802.11b (Wireless B)	Es uno de los primeros estándares populares que aún se utiliza.	1 / 2 / 5.5 / 11 Mbps
IEEE 802.11g (Wireless G) / Super G	Trabaja en la banda de frecuencia de 2.4 GHz solamente.	11 / 22 / 54 / 108 Mbps
IEEE 802.11n (Wireless N)	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.	Hasta 300 Mbps
Bluetooth	Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio de corto alcance (1, 20 y 100 m a la redonda dependiendo la versión). Las ondas pueden incluso ser capaces de cruzar cierto tipo de materiales, incluyendo muros.	Hasta 1 Mbps

2. WEP (WIRED EQUIVALENT PRIVACY, PRIVACIDAD EQUIVALENTE AL CABLE)

Algoritmo RC4

RC4 es un algoritmo de flujo y no de bloques, fue creado en 1987 por Ronald Rivest y publicado el 13 de Septiembre de 1994 usando remailers (repetidores de correo) anónimos en un grupo de noticias llamado *sci.crypt*. Tiene una clave que va desde 1 a 256 bytes (8 a 1024 bits), inicializando una tabla de estados. Esta tabla se usa para generar una lista de bytes pseudo-aleatorios, los cuales se combinan mediante la función XOR con el texto en claro; el resultado es el texto cifrado.

Este algoritmo tiene claves de 64 bits que se forman por 24 bits que corresponden al vector de inicialización más 40 bits de la clave secreta. Estos 40 bits son los que se deben distribuir manualmente. El vector de inicialización es generado dinámicamente y deberá ser diferente en cada trama para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y termine deduciendo la clave.

3. 802.11(X)

Las especificaciones del estándar definido por el IEEE denominado 802.11X, donde X comprende letras que definen las variantes de la norma 802.11a, 802.11b, 802.11g o 802.11n. Cada letra final corresponde aún uso específico del estándar, como es:

- a) 802.11: Usa la frecuencia de 2.4 GHz con una velocidad de 1 a 2 Mbps.
- b) 802.11a: Usa las frecuencias de 5.1-5.3 y de 5.7-5.8 GHz a una velocidad de 54 Mbps.
- c) 802.11b: Usa las frecuencias de 2.4-2.485 GHz a una velocidad de 11 Mbps.
- d) 802.11c: Añade soporte MAC para operaciones de puente (Bridges).
- e) 802.11d: Múltiples dominios reguladores (restricciones según países).
- f) 802.11e: Calidad de servicio (QoS) de la interfaz IEEE WLAN de radio.
- g) 802.11f: Protocolo de conexión entre puntos de acceso (AP) y el protocolo IAPP.
- h) 802.11g: Usa las frecuencias de 2.4-2.485 GHz a una velocidad de 36 ó 54 Mbps.
- i) 802.11h: Tiene un espectro de banda de 5GHz usado solo para Europa y Asia.
- j) 802.11i: Seguridad en protocolos de autenticación y codificación.
- k) 802.11j: Armoniza los estándares IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).
- l) 802.11n: Usa las frecuencias de 2.4 o 5 GHz a una velocidad de 540 Mbps.
- m) 802.11m: Usado para mantenimiento de redes inalámbricas. Las más usadas son: 802.11b, 802.11g, 802.11a.

4. NUEVAS TECNOLOGÍAS DE SEGURIDAD

802.16

Las variantes del estándar 802.16 son:

- a) 802.16: Utiliza un espectro licenciado en el rango de 10 a 66 GHz, necesita una línea de visión directa con una capacidad de hasta 134 Mbps en distancias de 3.22 a 8.05 kilómetros. Soporta calidad de servicio (QoS).
- b) 802.16a: Ampliación del estándar 802.16, las bandas son de 2 a 11 GHz, con sistemas NLOS (Non Line Of Sight, Sin Línea De Vista) y LOS (Line Of Sight, Línea De Visión), y protocolo PTP (Point To Point, Punto a Punto) y PTMP (Point To MultiPoint, Punto a MultiPunto).
- c) 802.16b: Delimita redes de área metropolitana inalámbricas en bandas de frecuencia desde 10 a 60 GHz.
- d) 802.16c: Ampliación del estándar 802.16 para definir las características y especificaciones en la banda de 10-66 GHz.
- e) 802.16d: Revisión del 802.16 y 802.16a para añadir los perfiles aprobados por el WiMAX Forum. Aprobado como 802.16-2004 (la última versión del estándar).
- f) 802.16e: Extensión del estándar 802.16, incluye la conexión de banda ancha para elementos portables (ordenadores portátiles, PDA, móviles, etcétera).

Actualmente, se usan dos estándares:

- a) El estándar 802.16d que pertenece a la conexiones WiMAX fijas que funciona mediante una antena fija (similar a la de TV) con una frecuencia de 2 a 11 GHz a una velocidad de hasta 75 Mbps y un rango de hasta 10 Km.
- b) El estándar 802.16e que pertenece a las conexiones WiMAX móviles que trabaja en la frecuencia de 2 a 6 GHz con una velocidad de hasta 30 Mbps y un rango de hasta 3.5 Km.

5. SISTEMAS DETECTORES DE INTRUSOS (IDS)

En el campo de la seguridad informática los tres IDS más usados son:

- a) IDS basado en host: Analiza las diferentes áreas para determinar qué actividades pueden ser maliciosas o abusivas dentro de la red y verifica que no haya ninguna intrusión o violaciones de seguridad desde afuera. Este IDS consulta los diferentes registros de archivos (kernel, sistema, servidores, red, cortafuegos, etcétera.) y compara los registros contra una base de datos interna de peculiaridades comunes sobre ataques conocidos.
- b) IDS basado en la red: Escanea los paquetes de red a nivel del enrutador o host y posteriormente audita la información de los paquetes, busca cualquier paquete que pueda ser sospechoso y lo marca como un archivo de registro extendido, para que después pueda ser enviado al host específico. Este IDS se considera incompleto ya que muchos hosts en un ambiente móvil dan el servicio de escaneo y protección de paquetes de red.
- c) IDS distribuidos: Es un esquema de varios IDS desplegados a lo largo de una red, los cuales centralizan la información. Este tipo de esquemas puede ser útil en redes de gran tamaño, pero debido a la gran cantidad de información que implica, necesita un monitoreo y mantenimiento constante.

6. ENTORNO SOCIAL E IMPACTO ECONÓMICO DE LA SEGURIDAD INFORMÁTICA

Efecto de las computadoras sobre los individuos

Aplicaciones positivas

- a) *Nueva oportunidad de trabajo*: Se han creado cientos de nuevos empleos en áreas como la programación, operación de computadoras y la administración de sistemas de información.
- b) *Mayor satisfacción en el trabajo*: Los científicos e ingenieros pueden resolver problemas complicados que no habían podido solucionar sin la ayuda de las computadoras.
- c) *Uso en los negocios*: Evita el desperdicio y mejora la eficiencia. Se obtienen precios más bajos del producto y un mejor servicio a los clientes.
- d) *Uso en las organizaciones públicas*: Disminuye la pérdida de tiempo y proporciona un mejor rendimiento en las oficinas del gobierno, escuelas y hospitales.
- e) *Uso en el hogar*: Son usados con fines de entretenimiento, diversión, educativo y para el control del presupuesto familiar.

Implicaciones potenciales

- a) *Amenaza del desempleo*: Al emplear computadoras en el trabajo, una persona puede ser considerada como obsoleta y en consecuencia ser despedida.
- b) *Uso de ciertas prácticas dudosas de procesamiento de datos*: Las organizaciones pueden capturar datos de los ciudadanos pero en ocasiones los recopilan personas que no tienen permiso para realizarlo.
- c) *Tendencias a la despersonalización*: Se pierde la identidad del individuo debido a que la computadora lo identifica como un número.
- d) *El problema de seguridad de los sistemas*: Es la falta de control en la seguridad de los datos de un sistema de cómputo, debido a personas no autorizadas (tengan acceso accidental o intencionalmente).
- e) *La cuestión de la privacidad*: Es la falta de control en el almacenamiento, recuperación y transmisión de datos que ha permitido que se abuse del derecho de mantener en forma confidencial los hechos, creencias y sentimientos del individuo.


Existen ciertas modalidades de piratería que deberían ser clasificadas como delitos y otras no, por ejemplo:

- a) Copias caseras: Son las fabricadas por los usuarios. No constituyen delitos porque por lo general no existe un fin de lucro.
- b) Copia corporativa: Se adquiere un ejemplar original para asegurar la asistencia técnica en caso de ser necesario y a partir de ésta se fabrican copias para ser instaladas en todas las computadoras existentes pero no constituye un delito.
- c) Comunidad de usuarios: Una persona compra un ejemplar original y a su vez, hace varias copias del mismo para venderlas a un costo más bajo, así dicho usuario obtendrá ganancias. Al haber un fin de lucro hay acción delictiva.
- d) Suministro de copias como estímulo de venta de computadoras: Los comercios o empresas que venden hardware cargan en el disco duro del comprador copias piratas que el usuario no tiene que comprar y así abaratan el precio final para éste. Por tal razón, sí hay acción delictiva.
- e) Fabricación y venta de copias en comercio: Sí hay acción delictiva.
- f) Copiado de fuentes: Consiste en que empleados de una empresa obtienen una copia de un determinado software hecho a medida de ésta, lo modifican y lo venden como si fuera un desarrollo propio. También deberá ser considerado delito.

APÉNDICE D

**PROGRAMA DE ESTUDIO
DE LA ASIGNATURA:
SEGURIDAD INFORMÁTICA I**

APÉNDICE D

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE INGENIERÍA			
PROGRAMA DE ESTUDIO <small>Aprobado por el Consejo Técnico de la Facultad de Ingeniería en su sesión ordinaria del 15 de octubre de 2008</small>			
SEGURIDAD INFORMÁTICA I	0880	8°, 9°	06
Asignatura	Clave	Semestre	Créditos
Ingeniería Eléctrica	Ingeniería en Computación	Ingeniería en Computación	
División	Departamento	Carrera en que se imparte	
Asignatura: Obligatoria <input type="checkbox"/> Optativa de elección <input checked="" type="checkbox"/>		Horas: Teóricas <input type="text" value="3.0"/> Prácticas <input type="text" value="0.0"/>	
		Total (horas): Semana <input type="text" value="3.0"/> 16 Semanas <input type="text" value="48.0"/>	
Modalidad: Curso.			
Asignatura obligatoria antecedente: Ninguna.			
Asignatura obligatoria consecuente: Seguridad Informática II.			
Objetivo(s) del curso: El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética.			
<hr/> Temario			
NÚM.	NOMBRE	HORAS	
1.	Fundamentos teóricos	9.0	
2.	Amenazas y vulnerabilidades	7.5	
3.	Identificación de ataques y técnicas de intrusión	10.5	
4.	Políticas de seguridad informática de la organización	7.5	
5.	Análisis del riesgo	7.5	
6.	Ética informática	6.0	
		48.0	
Prácticas de laboratorio		0.0	
Total		48.0	



1 Fundamentos teóricos

Objetivo: El alumno conocerá los conceptos, objetivos y antecedentes históricos de la Seguridad informática, así como el de los modelos de seguridad que le permitan adoptar los Estándares destinados a planificar un esquema de seguridad en una organización.

Contenido:

- 1.1 Introducción
 - 1.1.1 Concepto de la Seguridad Informática
 - 1.1.2 Evolución histórica de la Seguridad Informática
 - 1.1.3 Objetivos y misión de la Seguridad Informática
 - 1.1.4 Amenazas a las redes y sistemas computacionales
- 1.2 Normatividad de la Seguridad Informática
 - 1.2.1 Normas de Seguridad a través de la Historia
 - 1.2.1.1 TCSEC / Libro Naranja
 - 1.2.1.2 ITSEC
 - 1.2.1.3 CTCPEC
 - 1.2.1.4 FC-ITS
 - 1.2.2 Criterios Comunes / ISO 15408
 - 1.2.3 ISO 17799
 - 1.2.4 Nuevas Tendencias
 - 1.2.4.1 OCTAVE
- 1.3 Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección
 - 1.3.1 Definición y propósito
 - 1.3.2 Estructura
 - 1.3.2.1 Introducción
 - 1.3.2.2 Descripción del objeto de evaluación
 - 1.3.2.3 Entorno de seguridad
 - 1.3.2.4 Hipótesis
 - 1.3.2.5 Amenazas
 - 1.3.2.6 Políticas de la organización
 - 1.3.2.7 Nivel de Garantía general requerido
 - 1.3.2.8 Objetivos de Seguridad
 - 1.3.2.9 Requerimientos Funcionales y de Garantía
 - 1.3.2.10 Justificación
- 1.4 Servicios de Seguridad
 - 1.4.1 Confidencialidad
 - 1.4.2 Autenticación
 - 1.4.3 Integridad
 - 1.4.4 No repudio
 - 1.4.5 Control de Acceso
 - 1.4.6 Disponibilidad



2 Amenazas y vulnerabilidades

Objetivo: El alumno conocerá, identificará y explicará los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.

Contenido:

- 2.1 Amenazas
 - 2.1.1 Definición
 - 2.1.2 Fuentes de amenaza
 - 2.1.2.1 Factor humano
 - 2.1.2.1.1 Tipos: ingeniería social, robo, fraude, sabotaje, personal enterado, terroristas, curiosos, intrusos remunerados, etc.
 - 2.1.2.1.2 Hardware
 - 2.1.2.1.3 Tipos: mal diseño, errores de fabricación, suministro de energía, etc.
 - 2.1.2.2 Red de datos
 - 2.1.2.2.1 Tipos: topología seleccionada, sistema operativo, sistema de administración, monitoreo, etc.
 - 2.1.2.3 Software
 - 2.1.2.3.1 Tipos: software de desarrollo, software de aplicación, código malicioso, virus, etc.
 - 2.1.2.4 Desastres naturales
 - 2.1.2.4.1 Tipos: inundaciones, terremotos, fuego, viento, tormentas eléctricas, etc.
- 2.2 Vulnerabilidades
 - 2.2.1 Definición
 - 2.2.2 Tipos de Vulnerabilidades
 - 2.2.2.1 Física
 - 2.2.2.2 Natural
 - 2.2.2.3 Hardware
 - 2.2.2.4 Software
 - 2.2.2.5 Red

3 Identificación de ataques y técnicas de intrusión

Objetivo: El alumno conocerá, identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas; a su vez conocerá los mecanismos y herramientas para evitarlos.

Contenido:

- 3.1 Reconocimiento y Obtención de Información
 - 3.1.1 Bases de Datos Públicas
 - 3.1.2 WEB
 - 3.1.3 DNS
 - 3.1.4 Keyloggers
 - 3.1.5 Ingeniería Social
 - 3.1.6 Otros
- 3.2 Identificación de Vulnerabilidades
 - 3.2.1 Ataques a Redes Telefónicas
 - 3.2.2 Ataques a la Telefonía Inalámbrica
 - 3.2.3 Barrido de Puertos



- 3.2.4** Identificación de Firewalls
 - 3.2.4.1** Interpretación de reglas y filtros
- 3.2.5** Identificación de Sistemas Operativos / Fingerprinting
 - 3.2.5.1** Métodos de Identificación
- 3.2.6** Escaneo a Redes Inalámbricas
- 3.2.7** Instalaciones Físicas
- 3.2.8** Configuración de Servicios y Servidores
- 3.2.9** Software
- 3.2.10** Otros
- 3.3** Explotación y obtención de acceso a Sistemas y Redes
 - 3.3.1** Promiscuidad en Redes
 - 3.3.2** Robo de Identidad
 - 3.3.3** Engaño a Firewalls y Detectores de Intrusos
 - 3.3.4** Vulnerabilidades en el Software
 - 3.3.4.1** Buffer Overflows
 - 3.3.4.2** Heap Overflows
 - 3.3.4.3** Formato de Cadena
 - 3.3.4.4** Race Conditions
 - 3.3.4.5** SQL Injection
 - 3.3.4.6** Cross-Site & Cross-Domain Scripting
 - 3.3.4.7** Virus y Gusanos
 - 3.3.4.8** Otros
 - 3.3.5** Ataques a Contraseñas
 - 3.3.6** Debilidad de los Protocolos de Red
 - 3.3.7** Ataques a Servicios
 - 3.3.8** Negación de Servicio
 - 3.3.9** Ataques a Redes Inalámbricas
 - 3.3.9.1** Denegación de Servicio
 - 3.3.9.2** Ataque de Hombre en Medio
 - 3.3.9.3** ARP Poisoning
 - 3.3.9.4** WEP key-cracking
 - 3.3.9.5** Nuevos Métodos de Ataque en Redes Inalámbricas
- 3.4** Mantener el Acceso a Sistemas Comprometidos
 - 3.4.1** Puertas Traseras
 - 3.4.2** Caballos de Troya
 - 3.4.3** Rootkits
 - 3.4.4** Otros
- 3.5** Eliminación de Evidencias
 - 3.5.1** Edición de bitácoras
 - 3.5.2** Ocultar Información
 - 3.5.3** Estenografía
 - 3.5.4** Nuevos métodos



4 Políticas de seguridad informática de la organización

Objetivo: El alumno entenderá, explicará, valorará y adquirirá la capacidad para desarrollar políticas de seguridad informática así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad en una organización.

Contenido:

- 4.1 Políticas de Seguridad Informática
 - 4.1.1 Objetivo de una política de seguridad
 - 4.1.2 Misión, visión y objetivos de la organización
 - 4.1.3 Principios fundamentales de las políticas de seguridad
 - 4.1.3.1 Responsabilidad individual
 - 4.1.3.2 Autorización
 - 4.1.3.3 Mínimo privilegio
 - 4.1.3.4 Separación de obligaciones
 - 4.1.3.5 Auditoría
 - 4.1.3.6 Redundancia
 - 4.1.4 Políticas para la confidencialidad
 - 4.1.5 Políticas para la integridad
 - 4.1.6 Modelos de Seguridad: abstracto, concreto, de control de acceso y de flujo de información
 - 4.1.7 Desarrollo de políticas orientadas a servicios de seguridad
 - 4.1.8 Publicación y Difusión de las Políticas de Seguridad
- 4.2 Procedimientos y Planes de Contingencia
 - 4.2.1 Procedimientos Preventivos
 - 4.2.2 Procedimientos Correctivos
 - 4.2.3 Planes de Contingencia
 - 4.2.3.1 Objetivos y Características de un Plan de Contingencias
 - 4.2.3.2 Fases del Plan de Contingencia
 - 4.2.3.2.1 Análisis y Diseño
 - 4.2.3.2.2 Desarrollo de un plan de contingencias
 - 4.2.3.2.3 Pruebas y Mantenimiento

5 Análisis del riesgo

Objetivo: El alumno conocerá, identificará, seleccionará y aplicará las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.

Contenido:

- 5.1 Terminología básica
 - 5.1.1 Activos
 - 5.1.2 Riesgo
 - 5.1.3 Aceptación
 - 5.1.4 Análisis del riesgo
 - 5.1.5 Manejo del riesgo
 - 5.1.6 Evaluación
 - 5.1.7 Impacto
 - 5.1.8 Pérdida esperada



- 5.1.9 Vulnerabilidad
- 5.1.10 Amenaza
- 5.1.11 Riesgo residual
- 5.1.12 Controles
- 5.2 Análisis cuantitativo
- 5.3 Análisis cualitativo
- 5.4 Pasos del análisis de riesgo
 - 5.4.1 Identificación y evaluación de los activos
 - 5.4.2 Identificación de amenazas
 - 5.4.3 Identificación de vulnerabilidades
 - 5.4.4 Impacto de la ocurrencia de una amenaza
 - 5.4.5 Controles en el lugar
 - 5.4.6 Riesgos residuales
 - 5.4.7 Identificación de los controles adicionales
 - 5.4.8 Preparación de un informe del análisis del riesgo.
- 5.5 Análisis costo-beneficio

6 Ética informática

Objetivo: El alumno comprenderá y conocerá la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.

Contenido:

- 6.1 Concepto de Ética Informática
- 6.2 Códigos Deontológico en Informática
- 6.3 Contenidos de la Ética Informática
- 6.4 Actualidad de la Ética Informática
- 6.5 Psicología del Intruso
- 6.6 Códigos de Ética
- 6.7 Casos de Estudio

Bibliografía básica:

Temas para los que se recomienda

ANONYMOUS
Maximun Security
4rd. Edition
U.S.A.
Sams Publishing, 2003.

Todos

FACCIN, Stefano, et al.
IP in Wireless Networks
U.S.A.
Prentice Hall, 2003.

Todos

APÉNDICE D

SEGURIDAD INFORMÁTICA I	(7/8)	
FLICKENGER, Rob <i>Linux Server Hacks</i> U.S.A. O'Reilly, 2003.	Todos	
GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene. <i>Practical UNIX & Internet Security</i> 3rd. Edition U.S.A. O'Reilly, 2003.	Todos	
KING, Todd <i>Security + Training Guide</i> U.S.A. Que, 2003.	Todos	
SUMMERS, Rita <i>Secure Computing, Threats and Safeguards</i> U.S.A. McGraw Hill, 1997	Todos	
LOPEZ, Jaquelina y QUEZADA, Cintia <i>Apuntes de Seguridad Informática</i> México Facultad de Ingeniería – UNAM, 2005	Todos	
McCARHY, Linda <i>IT security: risking the corporation</i> U.S.A. Prentice Hall, 2003.	Todos	
Bibliografía complementaria:		
BHASKAR, K. <i>Threats and countermeasures</i> England NCC Blackwell, 1993	2, 4 y 5	
ELEGIDO M., Juan <i>Fundamentos de Ética de Empresa</i> México IPADE, 1998.	5	

APÉNDICE D

SEGURIDAD INFORMÁTICA I

(8 / 8)



FACCIN, Stefano, et al.
IP in Wireless Networks
U.S.A.
Prentice Hall, 2003.

2

FOGIE, Seth; PEIKARI, Cyrus
Maximum Wireless Security
U.S.A.
Sams Publishing, 2002.

2

Sugerencias didácticas:

Exposición oral	<input checked="" type="checkbox"/>
Exposición audiovisual	<input checked="" type="checkbox"/>
Ejercicios dentro de clase	<input checked="" type="checkbox"/>
Ejercicios fuera del aula	<input checked="" type="checkbox"/>
Seminarios	<input checked="" type="checkbox"/>

Lecturas obligatorias	<input checked="" type="checkbox"/>
Trabajos de investigación	<input checked="" type="checkbox"/>
Prácticas de taller o laboratorio	<input checked="" type="checkbox"/>
Prácticas de campo	<input type="checkbox"/>
Otras	<input type="checkbox"/>

Forma de evaluar:

Exámenes parciales	<input checked="" type="checkbox"/>
Exámenes finales	<input checked="" type="checkbox"/>
Trabajos y tareas fuera del aula	<input checked="" type="checkbox"/>

Participación en clase	<input checked="" type="checkbox"/>
Asistencias a prácticas	<input checked="" type="checkbox"/>
Otras	<input type="checkbox"/>


Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente de las carreras: Ingeniero en Computación, Ingeniero en Electrónica, Ingeniero en Telecomunicaciones, Licenciado en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en seguridad en informática, desarrollo de esquemas de seguridad y aplicaciones de seguridad informática.

APÉNDICE E

**PROGRAMA DE ESTUDIO
DE LA ASIGNATURA:
SEGURIDAD INFORMÁTICA II**

APÉNDICE E

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO FACULTAD DE INGENIERÍA			
PROGRAMA DE ESTUDIO Aprobado por el Consejo Técnico de la Facultad de Ingeniería en su sesión ordinaria del 15 de octubre de 2008			
SEGURIDAD INFORMÁTICA II	0916	8º, 9º	06
Asignatura	Clave	Semestre	Créditos
Ingeniería Eléctrica	Ingeniería en Computación	Ingeniería en Computación	
División	Departamento	Carrera en que se imparte	
Asignatura:		Horas:	
Obligatoria <input type="checkbox"/>	Teóricas <input type="text" value="3.0"/>	Total (horas):	
Optativa <input checked="" type="checkbox"/>	Prácticas <input type="text" value="0.0"/>	Semana <input type="text" value="3.0"/>	
de elección		16 Semanas <input type="text" value="48.0"/>	
Modalidad: Curso			
Asignatura obligatoria antecedente: Seguridad Informática I			
Asignatura obligatoria consecuente: Ninguna			
<p>Objetivo(s) del curso: El alumno conocerá, identificará y aplicará los servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; conocerá, comprenderá y hará uso de las estrategias de monitoreo de los mecanismos de seguridad para administrar la seguridad dentro de una organización, a la vez que podrá controlar los sucesos e incidentes de seguridad conociendo los aspectos sociales en el área de la seguridad informática.</p>			
Temario			
NÚM.	NOMBRE	HORAS	
1.	Implementación de la seguridad informática	12.0	
2.	Monitoreo de la seguridad informática	12.0	
3.	Control de la seguridad informática	12.0	
4.	Entorno social e impacto económico de la seguridad informática	6.0	
5.	Nuevas tendencias y tecnologías	6.0	
		48.0	
	Prácticas	0.0	

APÉNDICE E

Total

48.0





1 Implementación de la seguridad informática

Objetivo: El alumno conocerá, explicará y aplicará los mecanismos y herramientas de protección para cuidar de la seguridad informática en una organización de manera física y lógica.

Contenido:

- 1.1 Sistemas y Mecanismos de Protección
 - 1.1.1 Seguridad Física
 - 1.1.1.1 Protección del hardware
 - 1.1.1.1.1 Acceso Físico
 - 1.1.1.1.2 Desastres Naturales
 - 1.1.1.2 Contratación de Personal
 - 1.1.2 Seguridad Lógica
 - 1.1.2.1 Identificación y Autenticación
 - 1.1.2.2 Modalidad de Acceso
 - 1.1.2.3 Control de Acceso Interno
 - 1.1.2.3.1 Contraseñas
 - 1.1.2.3.2 Listas de Control de Acceso
 - 1.1.2.3.3 Cifrado
 - 1.1.2.4 Control de Acceso Externo
 - 1.1.2.4.1 Dispositivos de Control de Puertos
 - 1.1.2.4.2 Firewalls
 - 1.1.2.4.2.1 Selección del Tipo de Firewall
 - 1.1.2.4.2.2 Integración de las Políticas de Seguridad al Firewall
 - 1.1.2.4.2.3 Revisión y Análisis del Mercado
 - 1.1.2.4.3 Proxies
 - 1.1.2.4.4 Integridad del Sistema
 - 1.1.2.4.5 VPN (Virtual Private Networks)
 - 1.1.2.4.6 DMZ (Zona Desmilitarizada)
 - 1.1.2.4.7 Herramientas de Seguridad
- 1.2 Seguridad en Redes de Datos
 - 1.2.1 Amenazas y Ataques a Redes
 - 1.2.2 Elementos Básicos de Protección
 - 1.2.3 Introducción a la Criptografía
 - 1.2.4 Seguridad de la Red a nivel:
 - 1.2.4.1 Aplicación
 - 1.2.4.2 Transporte
 - 1.2.4.3 Red
 - 1.2.4.4 Enlace
 - 1.2.5 Monitoreo
- 1.3 Seguridad en Redes Inalámbricas
 - 1.3.1 Seguridad en el Access Point
 - 1.3.2 SSID (Service Set Identifier)
 - 1.3.3 WEP (Wired Equivalent Privacy)
 - 1.3.4 Filtrado de MAC Address
 - 1.3.5 RADIUS Authentication
 - 1.3.6 WLAN VPN
 - 1.3.7 Seguridad sobre 802.11(x)



- 1.3.8 Nuevas Tecnologías de Seguridad para redes Inalámbricas
- 1.4 Seguridad en Sistemas
 - 1.4.1 Riesgos de Seguridad en Sistemas
 - 1.4.2 Arquitectura de los Sistemas
 - 1.4.3 Problemas Comunes de Seguridad
 - 1.4.4 Instalación Segura de Sistemas
 - 1.4.5 Administración de Usuarios y controles de acceso
 - 1.4.6 Administración de Servicios
 - 1.4.7 Monitoreo
 - 1.4.8 Actualización de los Sistemas
 - 1.4.9 Mecanismos de Respaldo

2 Monitoreo de la seguridad informática

Objetivo: El alumno conocerá y aplicará las técnicas que le permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

Contenido:

- 2.1 Administración de la Seguridad Informática
 - 2.1.1 Administración de cumplimiento de Políticas
 - 2.1.2 Administración de Incidentes
 - 2.1.3 Análisis de nuevas Vulnerabilidades en la Infraestructura
 - 2.1.4 Monitoreo de los Mecanismos de Seguridad
- 2.2 Detección de Intrusos
 - 2.2.1 Sistemas Detectores de Intrusos
 - 2.2.2 Falsos Positivos
 - 2.2.3 Falsos Negativos
 - 2.2.4 Métodos de Detección de Intrusos
 - 2.2.4.1 Análisis de Tráfico
 - 2.2.4.2 HIDS (Host Intrusión Detection System)
 - 2.2.4.3 NIDS (Network Intrusión Detection System)
 - 2.2.4.4 Nuevos métodos de detección
 - 2.2.5 Identificación de Ataques
 - 2.2.6 Análisis del Tiempo de Respuesta de los IDS

3 Control de la seguridad informática

Objetivo: El alumno conocerá y comprenderá la utilidad de mantener el control sobre redes y dispositivos dentro de una organización a través de la realización de auditorías; así mismo aprenderá y conocerá los métodos y herramientas para el análisis forense en informática que le permitan comprender los mecanismos y técnicas que utilizan los intrusos para vulnerar los sistemas.

Contenido:

- 3.1 Auditoría de Red
 - 3.1.1 Concepto de Auditoría sobre la Red
 - 3.1.2 Herramientas de Auditoría
 - 3.1.3 Mapeo de la Red
 - 3.1.4 Monitores de Red
 - 3.1.5 Auditoría a Firewalls



- 3.1.6 Pruebas de Penetración sobre redes
- 3.1.7 Análisis de la Información y Resultados
- 3.2 Auditoría a Sistemas
 - 3.2.1 Checklist de Seguridad
 - 3.2.2 Baseline del Sistema
 - 3.2.3 Auditoría a las Políticas del Sistema
 - 3.2.4 Auditoría a usuarios
 - 3.2.5 Comandos del Sistema
 - 3.2.6 Herramientas para realizar Auditoría
 - 3.2.7 Auditoría a los Registros y Bitácoras del Sistema
 - 3.2.8 Auditoría a la Configuración del Sistema
 - 3.2.9 Auditoría a la Capacidad de Recuperación ante Desastres
 - 3.2.10 Análisis de la Información y Resultados
- 3.3 Análisis Forense a Sistemas de Cómputo
 - 3.3.1 Introducción al Análisis Forense en Sistemas de Cómputo
 - 3.3.2 Obtención y Protección de la Evidencia
 - 3.3.3 Análisis Forense sobre Sistemas
 - 3.3.3.1 Imágenes en Medios de Almacenamiento
 - 3.3.3.2 Revisión de Bitácoras
 - 3.3.3.3 Revisión del Sistema de Archivos
 - 3.3.3.3.1 Tiempos de Modificación, Acceso y Creación
 - 3.3.3.4 Revisión de Procesos
 - 3.3.3.5 Herramientas y Técnicas del Análisis Forense
 - 3.3.4 Herramientas para Obtener información de la Red
 - 3.3.5 Análisis de la Información y Resultados
 - 3.3.6 Sistemas de Detección de Intrusos
 - 3.3.6.1 Aplicación de los Sistemas de Detección de Intrusos en la Seguridad Informática
 - 3.3.6.2 Tipos de Sistemas de Detección de Intrusos
 - 3.3.6.3 Nivel de Interacción de los Sistemas de Detección de Intrusos
- 3.4 Respuesta y Manejo de Incidentes
 - 3.4.1 Respuesta a Incidentes
 - 3.4.2 Creación de un Equipo de Respuesta a Incidentes de Seguridad Informática

4 Entorno social e impacto económico de la seguridad informática

Objetivo: El alumno conocerá y comprenderá los aspectos sociales y económicos en el campo de la seguridad informática.

Contenido:

- 4.1 Legislación Mexicana
 - 4.1.1 Acceso Ilícito a Sistemas
 - 4.1.1 Código Penal
 - 4.1.2 Derechos de Autor
 - 4.1.3 Actualidad de la legislación sobre delitos informáticos
- 4.2 Ley Modelo (CNUDMI)
- 4.3 Legislaciones Internacionales
 - 4.3.1 Legislación de Estados Unidos de América en Materia Informática
 - 4.3.2 Legislación de Australia en Materia Informática
 - 4.3.3 Legislación de España en Materia Informática
 - 4.3.4 Otras Legislaciones



- 4.4 Impacto Social de la Seguridad Informática
- 4.5 Impacto Económico de la Seguridad Informática

5 Nuevas tendencias y tecnologías

Objetivo: El alumno conocerá las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías que puedan minimizar estas amenazas.

Contenido:

- 5.1 Cultura de la Seguridad Informática
- 5.2 Nuevas Tecnologías de Protección
- 5.3 Tendencias en Ataques y Nuevos Problemas de Seguridad
 - 5.3.1 SPAM
 - 5.3.2 Malware
 - 5.3.3 Exploits de Días Cero
 - 5.3.4 Metasploits
 - 5.3.5 Otros

Bibliografía básica:

Temas de la asignatura para los que se recomienda

ANONYMOUS
Maximum Security
Fourth Edition
USA
Sams Publishing, 2003

Todos

BELLOVIN, Steven, CHESWICK, William, RUBIN, Aviel
Firewalls and Internet Security: Repelling the Wily Hacker
Second Edition
USA
Addison Wesley, 2003

Todos


GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene
Practical UNIX & Internet Security
Third Edition
USA
O'Reilly, 2003

Todos

KING, Todd
Security + Training Guide
USA
Que, 2003

Todos

APÉNDICE E

SEGURIDAD INFORMÁTICA II	(7/8)	
LISKA, Allan <i>The Practice of Network Security: Deployment Strategies for Production Enviroments</i> USA Prentice Hall, 2002	Todos	
Bibliografía complementaria:		
FINE, LEONARD H. <i>Seguridad en Centros de Cómputo, Políticas y Fundamentos</i> Segunda Edición México Trillas, 1997	2	
KOZIOL, Jack <i>Intrusion Detection with Snort</i> USA Que, 2003	2	
PEIKARI Cyrus, FOGIE Seth <i>Maximum Wireless Security</i> USA Sams Publishing, 2002	1, 3	
PATIL, Basavaraj, SAIFULLAH, Yousuf, FACCIN, STEFANO, MONOMEN Risto <i>IP in Wireless Networks</i> USA Prentice Hall, 2003	1, 3	
SKOUDIS, ED; ZELTSER, Lenny <i>Malware Fighting Malicious Code</i> First Edition USA Prentice may, 2004	5	
DRIMES Roger A. <i>Malicious Mobile Code</i> USA O'Reilly, 2001	5	

APÉNDICE E

SEGURIDAD INFORMÁTICA II

(8/8)



Sugerencias didácticas:

Exposición oral	<input checked="" type="checkbox"/>
Exposición audiovisual	<input checked="" type="checkbox"/>
Ejercicios dentro de clase	<input checked="" type="checkbox"/>
Ejercicios fuera del aula	<input checked="" type="checkbox"/>
Seminarios	<input checked="" type="checkbox"/>

Lecturas obligatorias	<input checked="" type="checkbox"/>
Trabajos de investigación	<input checked="" type="checkbox"/>
Prácticas de taller o laboratorio	<input checked="" type="checkbox"/>
Prácticas de campo	<input type="checkbox"/>
Otras	<input type="checkbox"/>

Forma de evaluar:

Exámenes parciales	<input checked="" type="checkbox"/>
Exámenes finales	<input checked="" type="checkbox"/>
Trabajos y tareas fuera del aula	<input checked="" type="checkbox"/>

Participación en clase	<input checked="" type="checkbox"/>
Asistencias a prácticas	<input checked="" type="checkbox"/>
Otras	<input type="checkbox"/>

Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente maestría de las siguientes carreras; Ingeniería en computación, Ingeniería en Comunicaciones y Electrónica, Ingeniería en Telecomunicaciones, Ingeniería en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en redes de computadoras, seguridad informática, desarrollo de proyectos y aplicaciones de la seguridad informática.

APÉNDICE F

**PROGRAMA DE ESTUDIO
DE LA ASIGNATURA:
SEGURIDAD INFORMÁTICA
AVANZADA**

APÉNDICE F

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO



SEGURIDAD INFORMÁTICA AVANZADA				14
Asignatura		Clave	Semestre	Créditos
INGENIERÍA ELÉCTRICA	INGENIERÍA EN COMPUTACIÓN	INGENIERÍA EN COMPUTACIÓN		
División	Departamento	Carrera(s) en que se imparte		
Asignatura:	Horas:	Total (horas):		
Obligatoria <input checked="" type="checkbox"/>	Teóricas <input type="text" value="6.0"/>	Semana <input type="text" value="8.0"/>		
Optativa <input type="checkbox"/>	Prácticas <input type="text" value="2.0"/>	16 Semanas <input type="text" value="128.0"/>		

Asignatura(s) precedente(s): Redes de datos seguras

Asignatura(s) subsecuente(s): Arquitecturas cliente/servidor, Praxis de redes y seguridad

Objetivo(s) del curso: El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, vulnerabilidades y ataques en sistemas y redes de cómputo. Asimismo, conocerá, identificará y aplicará servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; además de estrategias de monitoreo de los mecanismos de seguridad, a la vez que controle los sucesos e incidentes de seguridad conociendo y considerando los aspectos sociales en el área de seguridad informática y enmarcados en una base ética.

APÉNDICE F

SEGURIDAD INFORMÁTICA AVANZADA



Temario

NÚM.	NOMBRE	HORAS
1.	Fundamentos teóricos	10
2.	Amenazas y vulnerabilidades	8
3.	Identificación de ataques y técnicas de intrusión	14
4.	Políticas de seguridad informática de la organización	8
5.	Análisis y gestión de los riesgos	10
6.	Implementación de la seguridad informática	10
7.	Gestión de la seguridad informática	10
8.	Control de la seguridad informática	10
9.	Entorno social, ética informática e impacto económico de la seguridad informática	10
10.	Nuevas tendencias tecnológicas	6
	Teóricas	96
	Prácticas de laboratorio	32
	Total	128



1 Fundamentos teóricos

Objetivo: El alumno conocerá los conceptos, objetivos y antecedentes históricos de la Seguridad informática, así como el de los modelos de seguridad que le permitan adoptar los estándares destinados a planificar un esquema de seguridad en una organización

Contenido:

1.1 Introducción

- 1.1.1 Concepto de la Seguridad Informática
- 1.1.2 Evolución histórica de la Seguridad Informática
- 1.1.3 Objetivos de la Seguridad Informática
- 1.1.4 Principio de profundidad

1.2 Normatividad de la Seguridad Informática

- 1.2.1 Normas de Seguridad a través de la Historia
 - 1.2.1.1 TCSEC / Libro Naranja
 - 1.2.1.2 ITSEC
 - 1.2.1.3 CTCPEC
- 1.2.2 Criterios Comunes / ISO 15408
- 1.2.3 COBIT
- 1.2.4 Serie ISO 27000
 - 1.2.4.1 Antecedentes: BS7799 e ISO/IEC 17799
 - 1.2.4.2 Sistema de Gestión de Seguridad de la Información
 - 1.2.4.3 ISO 27001
 - 1.2.4.4 ISO 27002
 - 1.2.4.5 ISO 27003, 27004....

1.3 Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección

- 1.3.1 Definición y propósito
- 1.3.2 Estructura
 - 1.3.1.1 Introducción
 - 1.3.1.2 Descripción del objeto de evaluación
 - 1.3.1.3 Entorno de seguridad
 - 1.3.1.4 Hipótesis
 - 1.3.1.5 Amenazas
 - 1.3.1.6 Políticas de la organización
 - 1.3.1.7 Nivel de Garantía general requerido
 - 1.3.1.8 Objetivos de Seguridad
 - 1.3.1.9 Requerimientos Funcionales y de Garantía
 - 1.3.1.10 Justificación

1.4 Servicios de Seguridad

- 1.4.1 Confidencialidad
- 1.4.2 Autenticación
- 1.4.3 Integridad
- 1.4.4 No repudio
- 1.4.5 Control de Acceso
- 1.4.6 Disponibilidad



2 Amenazas y vulnerabilidades

Objetivo: El alumno conocerá, identificará y explicará los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.

Contenido:

2.1 Amenazas

- 2.1.1 Definición
- 2.1.2 Fuentes de amenaza
 - 2.1.2.1 Factor humano
 - 2.1.2.2 Hardware
 - 2.1.2.3 Red de datos
 - 2.1.2.4 Software
 - 2.1.2.5 Desastres naturales

2.2 Vulnerabilidades

- 2.2.1 Definición
- 2.2.2 Tipos de Vulnerabilidades
 - 2.1.2.6 Física
 - 2.1.2.7 Natural
 - 2.1.2.8 Hardware
 - 2.1.2.9 Software
 - 2.1.2.10 Red
 - 2.1.2.11 Humana

3 Identificación de ataques y técnicas de intrusión

Objetivo: El alumno conocerá, identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas; a su vez conocerá los tipos de mecanismos de seguridad para evitarlos.

Contenido:

3.1 Ataques

- 3.1.1 Definición
- 3.1.2 Ataques inherentes a las redes
 - 3.1.2.1 Interrupción
 - 3.1.2.2 Intercepción
 - 3.1.2.3 Interrupción
 - 3.1.2.4 Suplantación
- 3.1.3 Tipos
 - 3.1.3.1 Pasivos
 - 3.1.3.2 Activos
- 3.1.4 Etapas de un ataque



- 3.1.4.1 Planteamiento o preparación
- 3.1.4.2 Activación
- 3.1.4.3 Ejecución
- 3.2 Reconocimiento y Obtención de Información
 - 3.2.1 Bases de Datos Públicas
 - 3.2.2 WEB
 - 3.2.3 DNS
 - 3.2.4 Keyloggers
 - 3.2.5 Ingeniería Social
 - 3.2.6 Otros
- 3.3 Identificación de Vulnerabilidades
 - 3.3.1 Ataques a Redes Telefónicas
 - 3.3.2 Ataques a la Telefonía Inalámbrica
 - 3.3.3 Barrido de Puertos
 - 3.3.4 Identificación de Firewalls
 - 3.3.4.1 Interpretación de reglas y filtros
 - 3.3.5 Identificación de Sistemas Operativos / Fingerprinting
 - 3.3.5.1 Métodos de Identificación
 - 3.3.6 Escaneo a Redes Inalámbricas
 - 3.3.7 Instalaciones Físicas
 - 3.3.8 Configuración de Servicios y Servidores
 - 3.3.9 Software
 - 3.3.10 Otros
- 3.4 Explotación y obtención de acceso a Sistemas y Redes
 - 3.4.1 Introducción a Metasploit
 - 3.4.2 Metodología OSSSTM v.3
 - 3.4.3 Pentesting
 - 3.4.3.1 A redes (ético y no ético)
 - 3.4.3.2 A sistemas (ético y no ético)
 - 3.4.3.3 A bases de datos (ético y no ético)
 - 3.4.4 Manejo de exploits y análisis de vulnerabilidades en la red
 - 3.4.5 Promiscuidad en Redes
 - 3.4.6 Robo de Identidad
 - 3.4.7 Engaño a Firewalls y Detectores de Intrusos
 - 3.4.8 Vulnerabilidades en el Software
 - 3.4.8.1 Buffer Overflows
 - 3.4.8.2 Heap Overflows
 - 3.4.8.3 Formato de Cadena
 - 3.4.8.4 Race Conditions
 - 3.4.8.5 SQL Injection
 - 3.4.8.6 Cross-Site & Cross-Domain Scripting
 - 3.4.8.7 Virus y Gusanos
 - 3.4.8.8 Otros
 - 3.4.9 Ataques a Contraseñas
 - 3.4.10 Debilidad de los Protocolos de Red
 - 3.4.11 Ataques a Servicios



- 3.4.12 Negación de Servicio
- 3.4.13 Ataques a Redes Inalámbricas
 - 3.4.13.1 Denegación de Servicio
 - 3.4.13.2 Ataque de Hombre en Medio
 - 3.4.13.3 ARP Poisoning
 - 3.4.13.4 WEP key-cracking
 - 3.4.13.5 WPA cracking
- 3.5 Mantener el Acceso a Sistemas Comprometidos
 - 3.5.1 Puertas Traseras
 - 3.5.2 Caballos de Troya
 - 3.5.3 Rootkits
 - 3.5.4 Otros
- 3.6 Eliminación de Evidencias
 - 3.6.1 Edición de bitácoras
 - 3.6.2 Ocultar Información
 - 3.6.3 Estenografía
 - 3.6.4 Nuevos métodos
- 3.7 Mecanismos de seguridad
 - 3.7.1 Definición y objetivos
 - 3.7.2 Tipos de mecanismos de seguridad
 - 3.7.2.1 Por el servicio de seguridad que implementan
 - 3.7.2.2 Generalizados y específicos
 - 3.7.2.3 Disuasivos, preventivos, detectores, correctivos
 - 3.7.2.4 Requeridos y discrecionales

4 Políticas de seguridad informática de la organización

Objetivo: El alumno entenderá, explicará, valorará y adquirirá la capacidad para desarrollar políticas de seguridad informática, así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad en una organización.

Contenido:

- 4.1 Políticas de Seguridad Informática
 - 4.1.1 Objetivo de una política de seguridad
 - 4.1.2 Misión y visión de la organización
 - 4.1.3 Principios fundamentales de las políticas de seguridad
 - 4.1.3.1 Responsabilidad individual
 - 4.1.3.2 Autorización
 - 4.1.3.3 Mínimo privilegio
 - 4.1.3.4 Separación de obligaciones
 - 4.1.3.5 Auditoría
 - 4.1.3.6 Redundancia
 - 4.1.4 Modelos de Seguridad: abstracto, concreto, de control de acceso, de integridad y de flujo de información
 - 4.1.5 Desarrollo de políticas orientadas a servicios de seguridad
 - 4.1.6 Publicación y Difusión de las Políticas de Seguridad



4.2 Procedimientos y Planes de Contingencia

4.2.1 Procedimientos Preventivos

4.2.2 Procedimientos Correctivos

4.2.3 Planes de Contingencia

4.2.3.1 Objetivos y Características de un Plan de Contingencias

4.2.3.2 Fases del Plan de Contingencia

4.2.3.3 Análisis y Diseño

4.2.3.4 Desarrollo de un plan de contingencias

4.2.3.5 Pruebas y Mantenimiento

5 Análisis y gestión de los riesgos

Objetivo: El alumno conocerá, identificará, seleccionará y aplicará las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.

Contenido:

5.1 Terminología básica

5.1.1 Activos

5.1.2 Riesgo

5.1.3 Aceptación

5.1.4 Análisis del riesgo

5.1.5 Manejo del riesgo

5.1.6 Evaluación

5.1.7 Impacto

5.1.8 Pérdida esperada

5.1.9 Vulnerabilidad

5.1.10 Amenaza

5.1.11 Riesgo residual

5.1.12 Controles

5.2 Análisis cuantitativo

5.3 Análisis cualitativo

5.4 Pasos del análisis de riesgo

5.4.1 Identificación y evaluación de los activos

5.4.2 Identificación de amenazas

5.4.3 Identificación de vulnerabilidades

5.4.4 Impacto de la ocurrencia de una amenaza

5.4.5 Controles en el lugar

5.4.6 Riesgos residuales

5.4.7 Identificación de los controles adicionales

5.4.8 Preparación de un informe del análisis del riesgo.

5.5 Análisis costo-beneficio

5.5.1 Metodologías certificables



6 Implementación de la seguridad informática

Objetivo: El alumno conocerá, explicará y aplicará los mecanismos y herramientas de protección para cuidar de la seguridad informática en una organización de manera física y lógica.

Contenido:

6.1 Sistemas y Mecanismos de Protección

6.1.1 Seguridad Física

- 6.1.1.1 Protección del hardware
- 6.1.1.2 Acceso Físico
- 6.1.1.3 Desastres Naturales
- 6.1.1.4 Contratación de Personal

6.1.2 Seguridad Lógica

- 6.1.2.1 Identificación y Autenticación
- 6.1.2.2 Modalidad de Acceso
- 6.1.2.3 Control de Acceso Interno
 - 6.1.2.3.1 Contraseñas
 - 6.1.2.3.2 Listas de Control de Acceso
 - 6.1.2.3.3 Cifrado
- 6.1.2.4 Control de Acceso Externo
 - 6.1.2.4.1 Dispositivos de Control de Puertos
 - 6.1.2.4.2 Firewalls
 - 6.1.2.4.2.1 Selección del Tipo de Firewall
 - 6.1.2.4.2.2 Integración de las Políticas de Seguridad al Firewall
 - 6.1.2.4.2.3 Revisión y Análisis del Mercado
 - 6.1.2.4.3 Proxies
 - 6.1.2.4.4 Integridad del Sistema
 - 6.1.2.4.5 VPN (Virtual Private Networks)
 - 6.1.2.4.6 DMZ (Zona Desmilitarizada)
 - 6.1.2.4.7 Herramientas de Seguridad

6.2 Seguridad en Redes de Datos

- 6.2.1 Amenazas y Ataques a Redes
- 6.2.2 Elementos Básicos de Protección
- 6.2.3 Introducción a la Criptografía
- 6.2.4 Seguridad de la Red a nivel:
 - 6.2.4.1 Aplicación
 - 6.2.4.2 Transporte
 - 6.2.4.3 Red
 - 6.2.4.4 Enlace
- 6.2.5 Monitoreo

6.3 Seguridad en Redes Inalámbricas

- 6.3.1 Seguridad en el Access Point
- 6.3.2 SSID (Service Set Identifier)
- 6.3.3 WEP (Wired Equivalent Privacy)
- 6.3.4 WPA y WPA2
- 6.3.5 Filtrado de MAC Address



- 6.3.6 Portales cautivos
- 6.3.7 RADIUS Authentication
- 6.3.8 WLAN VPN
- 6.3.9 Seguridad sobre 802.11(x)
- 6.3.10 Nuevas Tecnologías de Seguridad para redes Inalámbricas
- 6.4 Seguridad en Sistemas
 - 6.4.1 Riesgos de Seguridad en Sistemas
 - 6.4.2 Arquitectura de los Sistemas
 - 6.4.3 Problemas Comunes de Seguridad
 - 6.4.4 Instalación Segura de Sistemas
 - 6.4.5 Administración de Usuarios y controles de acceso
 - 6.4.6 Administración de Servicios
 - 6.4.7 Monitoreo
 - 6.4.8 Actualización de los Sistemas
 - 6.4.9 Mecanismos de Respaldo

7 Gestión de la seguridad informática

Objetivo: El alumno conocerá y aplicará las técnicas que le permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

Contenido:

- 7.1 Administración de la Seguridad Informática
 - 7.1.1 Administración de cumplimiento de Políticas
 - 7.1.2 Administración de Incidentes
 - 7.1.3 Análisis de nuevas Vulnerabilidades en la Infraestructura
 - 7.1.4 Monitoreo de los Mecanismos de Seguridad
- 7.2 Detección de Intrusos
 - 7.2.1 Sistemas Detectores de Intrusos
 - 7.2.2 Falsos Positivos
 - 7.2.3 Falsos Negativos
 - 7.2.4 Métodos de Detección de Intrusos
 - 7.2.4.1 Análisis de Tráfico
 - 7.2.4.2 HIDS (Host Intrusión Detection System)
 - 7.2.4.3 NIDS (Network Intrusión Detection System)
 - 7.2.4.4 Nuevos métodos de detección
 - 7.2.5 Identificación de Ataques
 - 7.2.6 Análisis del Tiempo de Respuesta de los IDS



8 Control de la seguridad informática

Objetivo: El alumno conocerá y comprenderá la utilidad de mantener el control sobre redes y dispositivos dentro de una organización a través de la realización de auditorías; así mismo aprenderá y conocerá los métodos y herramientas para el análisis forense en informática que le permitan comprender los mecanismos y técnicas que utilizan los intrusos para vulnerar los sistemas.

Contenido:

- 8.1 Auditoría de Red
 - 8.1.1 Concepto de Auditoría sobre la Red
 - 8.1.2 Herramientas de Auditoría
 - 8.1.3 Mapeo de la Red
 - 8.1.4 Monitores de Red
 - 8.1.5 Auditoría a Firewalls
 - 8.1.6 Pruebas de Penetración sobre redes
 - 8.1.7 Análisis de la Información y Resultados
- 8.2 Auditoría a Sistemas
 - 8.2.1 Checklist de Seguridad
 - 8.2.2 Baseline del Sistema
 - 8.2.3 Auditoría a las Políticas del Sistema
 - 8.2.4 Auditoría a usuarios
 - 8.2.5 Comandos del Sistema
 - 8.2.6 Herramientas para realizar Auditoría
 - 8.2.7 Auditoría a los Registros y Bitácoras del Sistema
 - 8.2.8 Auditoría a la Configuración del Sistema
 - 8.2.9 Auditoría a la Capacidad de Recuperación ante Desastres
 - 8.2.10 Análisis de la Información y Resultados
- 8.3 Análisis Forense a Sistemas de Cómputo
 - 8.3.1 Introducción al Análisis Forense en Sistemas de Cómputo
 - 8.3.2 Obtención y Protección de la Evidencia
 - 8.3.3 Análisis Forense sobre Sistemas
 - 8.3.3.1 Imágenes en Medios de Almacenamiento
 - 8.3.3.2 Revisión de Bitácoras
 - 8.3.3.3 Revisión del Sistema de Archivos
 - 8.3.3.3.1 Tiempos de Modificación, Acceso y Creación
 - 8.3.3.4 Revisión de Procesos
 - 8.3.3.5 Herramientas y Técnicas del Análisis Forense
 - 8.3.4 Herramientas para Obtener información de la Red
 - 8.3.5 Análisis de la Información y Resultados
 - 8.3.6 Sistemas de Detección de Intrusos
 - 8.3.6.1 Aplicación de los Sistemas de Detección de Intrusos en la Seguridad Informática
 - 8.3.6.2 Tipos de Sistemas de Detección de Intrusos
 - 8.3.6.3 Nivel de Interacción de los Sistemas de Detección de Intrusos
- 8.4 Respuesta y Manejo de Incidentes
 - 8.4.1 Respuesta a Incidentes
 - 8.4.1.1 Equipo de respuesta a incidentes



- 8.4.1.2 Verificación del incidente
- 8.4.1.3 Estrategia de contención
- 8.4.1.4 Aislamiento del incidente
- 8.4.1.5 Proceso de cadena de custodia
- 8.4.1.6 Ejecución del plan de contingencia
- 8.4.2 Creación de un Equipo de Respuesta a Incidentes de Seguridad Informática

9 Entorno social, ética informática e impacto económico de la seguridad informática

Objetivo: El alumno conocerá y comprenderá los aspectos sociales y económicos en el campo de la seguridad informática, así como la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.

Contenido:

- 9.1 Delito informático
- 9.2 Marco legal mexicano
 - 9.2.1 Acceso Ilícito a Sistemas
 - 9.2.2 Código Penal
 - 9.2.3 Derechos de Autor
 - 9.2.3.1 Protección de licencias
 - 9.2.3.1.1 Bussiness Software Alliance
 - 9.2.4 Actualidad de la legislación sobre delitos informáticos
 - 9.2.5 Protección de la información
 - 9.2.6 Instituto Federal de Acceso a la Información
- 9.3 Ley Modelo (CNUDMI)
- 9.4 Legislaciones Internacionales
 - 9.4.1 Legislación de Estados Unidos de América en Materia Informática
 - 9.4.2 Legislación de Australia en Materia Informática
 - 9.4.3 Legislación de España en Materia Informática
 - 9.4.4 Otras Legislaciones
 - 9.4.4.1 Ley HIPAA
 - 9.4.4.2 Ley Sarbanes-Oaxley
- 9.5 Ética informática
 - 9.5.1 Concepto de Ética Informática
 - 9.5.2 Códigos Deontológico en Informática
 - 9.5.3 Contenidos de la Ética Informática
 - 9.5.4 Actualidad de la Ética Informática
 - 9.5.5 Psicología del Intruso
 - 9.5.6 Códigos de Ética
- 9.6 Impacto Social de la Seguridad Informática
- 9.7 Impacto Económico de la Seguridad Informática



10 Nuevas tendencias y tecnologías

Objetivo: El alumno conocerá las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías que puedan minimizar estas amenazas.

Contenido:

- 10.1 Cultura de la Seguridad Informática y cultura organizacional
- 10.2 La seguridad informática como servicio
- 10.3 Nuevas Tecnologías de Protección y vectores de ataque
- 10.4 Tendencias en Ataques y Nuevos Problemas de Seguridad

Bibliografía básica:

Títulos

Temas de la materia para los que se recomienda

GÓMEZ, ÁLVARO

Todos

Enciclopedia De La Seguridad Informática

Alfaomega, México, 2007

DALTABUIT, ENRIQUE.

Todos

La Seguridad De La Información

Limusa, México, 2007

LOPEZ, JAQUELINA; QUEZADA, CINTIA

Todos

Fundamentos De Seguridad Informática

Facultad de Ingeniería – UNAM, México, 2005

ALEXANDER, ALBERTO G.

1

Diseño De Un Sistema De Gestión De Seguridad De

Información Óptica ISO 27001:2005

Alfaomega, México, 2007

ANONYMOUS

Todos

Maximun Security

4th. Edition

Sams Publishing, U.S.A. , 2003.

FLICKENGER, ROB

Todos

Linux Server Hacks

O'Reilly, U.S.A., 2003.

GARFINKEL, SIMSON; SCHWARTZ, ALAN;

Todos

SPAFFORD, GENE.

APÉNDICE F

Practical UNIX & Internet Security

3rd. Edition

O'Reilly, U.S.A., 2003.

KING, TODD

Todos

Security + Training Guide

Que, U.S.A., 2003.

SUMMERS, RITA

Todos

Secure Computing, Threats and Safeguards

McGraw Hill, U.S.A., 1997

LISKA, Allan

Todos

The Practice of Network Security: Deployment

Strategies for Production Enviroments

Prentice Hall, U.S.A., 2002

Bibliografía complementaria:

Bibliografía básica:

Títulos

Temas de la materia para los que se recomienda

APELLIDO Y NOMBRE DE AUTORES CON MAYÚSCULAS "Título del Libro en altas y bajas y en Itálicas" Editorial, País, Año	Número del capítulo o capítulos En caso de ser todos los capitulos poner la palabra TODOS
FACCIN, STEFANO, et al. <i>IP in Wireless Networks</i> Prentice Hall, U.S.A., 2003.	2,6,8
BHASKAR, K. <i>Threats And Countermeasures</i> NCC Blackwell, England, 1993	2, 4, 5
ELEGIDO M., JUAN <i>Fundamentos de Ética de Empresa</i> IPADE, México, 1998.	5
FOGIE, SETH; PEIKARI, CYRUS <i>Maximum Wireless Security</i> Sams Publishing, U.S.A., 2002.	2
FINE, LEONARD H. <i>Seguridad en Centros de Cómputo. Políticas y Fundamentos</i> Segunda Edición Trillas, México, 1997	7
KOZIOL, JACK	7

APÉNDICE F

<p><i>Intrusion Detection with Snort</i> Que, U.S.A., 2003</p> <p>PEIKARI CYRUS, FOGIE SETH <i>Maximum Wireless Security</i> Sams Publishing, U.S.A., 2002</p> <p>SKOUDIS, ED; ZELTSER, LENNY <i>Malware Fighting Malicious Code</i> First Edition Prentice may, U.S.A., 2004</p> <p>DRIMES ROGER A. <i>Malicious Mobile Code</i> O'Reilly, U.S.A., 2001</p>	<p>6, 8</p> <p>10</p> <p>10</p>
--	---------------------------------

Sugerencias didácticas:

Exposición oral	<input checked="" type="checkbox"/>
Exposición audiovisual	<input checked="" type="checkbox"/>
Ejercicios dentro de clase	<input checked="" type="checkbox"/>
Ejercicios fuera del aula	<input checked="" type="checkbox"/>
Seminarios	<input checked="" type="checkbox"/>

Lecturas obligatorias	<input checked="" type="checkbox"/>
Trabajos de investigación	<input checked="" type="checkbox"/>
Prácticas de taller o laboratorio	<input checked="" type="checkbox"/>
Prácticas de campo	<input type="checkbox"/>
Otras	<input type="checkbox"/>

Forma de evaluar:

Exámenes parciales	<input checked="" type="checkbox"/>
Exámenes finales	<input checked="" type="checkbox"/>
Trabajos y tareas fuera del aula	<input checked="" type="checkbox"/>

Participación en clase	<input checked="" type="checkbox"/>
Asistencias a prácticas	<input checked="" type="checkbox"/>
Otras	<input checked="" type="checkbox"/>

Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente maestría de las siguientes carreras: Ingeniería en Computación, Ingeniería en Comunicaciones y Electrónica, Ingeniería en Telecomunicaciones, Licenciatura en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en redes de computadoras, seguridad en informática, desarrollo de esquemas de seguridad, desarrollo de proyectos y aplicaciones de seguridad informática

REFERENCIAS

REFERENCIAS

BIBLIOGRAFÍA

- Aldrete, A. (1998). *Telecomunicaciones, Redes de datos*. Mexico: McGraw-Hill.
- Beaver, K. (2007). *Hacking for dummies*. Estados Unidos: Wiley Publishing.
- Berrera Teron, A. (2000). *Microsoft fundamentos de redes plus, Curso oficial de certificación de MCSE*. España: McGraw-Hill Interamericana.
- Black, U. (1997). *Redes de computadores, Protocolos, normas e interfaces*. México: Alfaomega.
- Comer, D. E. (1995). *Internetworking with TCP/IP, Vol I: Principles, Protocolos, and Architecture*. Estados Unidos: Prentice-Hall Inc.
- Díaz, J. M. (2005). *Fundamentos de seguridad de redes, Especialista en Firewall Cisco*. España: Gráficas Rogar S.A.
- Domínguez, A. (2001). *Academia de Networking de Cisco Systems, Guía del primer año*. España: Pearson Educación.
- Domínguez, A. (2001). *Academia de Networking de Cisco Systems, Guía del segundo año*. España: Pearson Educación.
- Ford, M. (1998). *Tecnologías de Interconectividad de Redes*. México: Prentice Hall Hispanoamericana.
- Groff, J. R. (1990). *Using SQL*. Estados Unidos: McGraw-Hill.
- López Barrientos, M. J. (2009). *Criptografía*. México: Facultad de Ingeniería, Universidad Nacional Autónoma de México.
- López González, Á. (2000). *Protocolos de Internet*. Colombia: Alfaomega S.A.
- Mason, A. G. (2002). *Redes privadas virtuales de Cisco Secure*. España: Pearson Educación S.A.
- Nombela, J. J. (1997). *Seguridad Informática*. España: Paraninfo.
- Quezada Reyes, C. (2006). *Fundamentos de seguridad informática*. México: Facultad de Ingeniería, Universidad Nacional Autónoma de México.
- Scambray, J. (2003). *Hackers de sitios web*. España: McGraw-Hill Interamericana de España S.A.U.

REFERENCIAS

- Solórzano Palomares, F. (2003). Tomo I, Panorama histórico de la computación. México: Facultad de Ingeniería, Universidad Nacional Autónoma de México.
- Tanenbaum, A. S. (1996). Computer Networks. Estados Unidos: Prentice-Hall Inc.
- Taylor, A. G. (2006). *SQL for dummies*. Estados Unidos: Wiley Publishing.
- Whitehead, P. (1997). *Aprenda redes virtualmente*. Costa Rica: Trejos Hermanos.

REFERENCIAS ELECTRÓNICAS

Última Revisión (23.06.2014)

- ¿Cómo capturar el tráfico de red con monitor de red?* (s.f.). Obtenido de <http://support.microsoft.com/kb/148942/es>
- ¿Cómo utilizar ARP?* (s.f.). Obtenido de <http://www.alcancelibre.org/staticpages/index.php/como-arp>
- ¿Qué es el IPv6?* (s.f.). Obtenido de <http://www.maestrosdelweb.com/principiantes/evolucionando-hacia-el-ipv6/>
- ¿Qué es IP Fija y Dinámica?* (s.f.). Obtenido de http://www.publispain.com/adsl/que_es_ip_fija_y_que_es_ip_dinamica.html
- ¿Qué es un servidor proxy?* (s.f.). Obtenido de http://java.com/es/download/help/proxy_server.xml
- ¿Qué es un servidor web?* (s.f.). Obtenido de <http://www.ordenadores-y-portatiles.com/servidor-web.html>
- ¿Qué es un servidor?* (s.f.). Obtenido de <http://www.masadelante.com/faqs/servidor>
- ¿Qué software de seguridad usas?* (s.f.). Obtenido de <http://www.shellsec.net/articulo/que-software-seguridad-usas/>
- 50 Herramientas Top de seguridad informática.* (s.f.). Obtenido de http://www.zonagratis.com/a-cursos/utilidades/50_herramientas_top.htm
- Access point, características y capacidades.* (s.f.). Obtenido de http://www.informaticamoderna.com/Access_point.htm

REFERENCIAS

- Acuse de recibo* . (s.f.). Obtenido de <http://es.wikipedia.org/wiki/ACK>
- AES*. (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/aes.php>
- AES*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Advanced_Encryption_Standard
- Ajuste de la fragmentación de paquetes en una WLAN*. (s.f.). Obtenido de <http://www.ansat.es/soporte/docs/fragmentacion/fragmentacion.htm>
- Algoritmo de cifrado: MD5*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/MD5>
- Algoritmo de cifrado: PGP*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/PGP>
- Algoritmo de cifrado: RC4*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/RC4>
- Algoritmo de cifrado: RIPEMD-160*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/RIPEMD-160>
- Algoritmo de hash seguro*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Secure_Hash_Algorithm
- Algoritmo Diffie-Hellman*. (s.f.). Obtenido de http://triptico.com/docs/diffie_hellman.html
- Amenazas y vulnerabilidades*. (s.f.). Obtenido de <http://ingwebsu.wordpress.com/2008/11/18/53-amenazas-y-vulnerabilidades/>
- Amenazas y vulnerabilidades*. (s.f.). Obtenido de http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/
- Amenazas y vulnerabilidades*. (s.f.). Obtenido de <http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html>
- Análisis de tráfico con Wireshark*. (s.f.). Obtenido de http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf
- Análisis de tráfico de red*. (s.f.). Obtenido de <http://www.acis.org.co/memorias/JornadasSeguridad/IJNSI/trficored.ppt>
- Análisis forense*. (s.f.). Obtenido de <http://www.idg.es/pcworldtech/mostrarArticulo.asp?id=194718&seccion=seguridad>
- Análisis forense*. (s.f.). Obtenido de <http://es.scribd.com/doc/37134020/Analisis-forense>

REFERENCIAS

- Análisis y monitoreo de redes.* (s.f.). Obtenido de <http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html>
- Antiphishing.* (s.f.). Obtenido de http://en.wikipedia.org/wiki/Anti-phishing_software
- Antispam.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Antispam>
- Antispyware.* (s.f.). Obtenido de <http://revista.seguridad.unam.mx/numero-04/antispyware-protegi%C3%A9ndote-de-los-esp%C3%AD>
- Antivirus.* (s.f.). Obtenido de <http://revista.seguridad.unam.mx/numero-04/antivirus-una-herramienta-indispensable-para-nuestra-seguridad>
- Applet.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Applet>
- AppleTalk.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/AppleTalk>
- Arquitectura cliente servidor-Oposiciones TIC.* (s.f.). Obtenido de <http://oposicionestic.blogspot.com/2011/06/arquitectura-cliente-servidor.html>
- Arquitectura cliente-servidor.* (s.f.). Obtenido de <http://www.desarrolloweb.com/articulos/arquitectura-cliente-servidor.html>
- Arquitectura Cliente-Servidor.* (s.f.). Obtenido de <http://www.juansa.net/Admin2003/cliser.htm>
- Arquitectura cliente-servidor Socket.* (s.f.). Obtenido de <http://www.rhernando.net/modules/tutorials/doc/redes/cliente.html>
- Arquitectura de la administración de redes.* (s.f.). Obtenido de <http://html.rincondelvago.com/arquitectura-de-la-administracion-de-redes.html>
- ASCII.* (s.f.). Obtenido de <http://www.portalplanetasedna.com.ar/ascii.htm>
- ASP.* (s.f.). Obtenido de <http://www.programacion.com/asp/>
- Ataque de denegación de servicio.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
- Ataques.* (s.f.). Obtenido de <http://www.segu-info.com.ar/ataques/ataques.htm>
- Auditor de firewall.* (s.f.). Obtenido de <http://www.firewallauditor.com/HowDoesItWork/>
- Auditoría.* (s.f.). Obtenido de <http://www.infopeople.com/aaii/seguridad/auditoria.htm>

REFERENCIAS

- Auditoría de redes.* (s.f.). Obtenido de <http://www.slideshare.net/cryspaul/auditoria-de-redes>
- Autenticación.* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/autenticacion.php>
- Backdoor.* (s.f.). Obtenido de <http://www.segu-info.com.ar/malware/backdoor.htm>
- Base de datos.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/DB>
- Broadcast.* (s.f.). Obtenido de [http://es.wikipedia.org/wiki/Broadcast_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Broadcast_(inform%C3%A1tica))
- Bus dual de cola distribuida.* (s.f.). Obtenido de <http://www.angelfire.com/md2/dqdb/Paginas/INTRODUCCION.htm>
- Cabecera IP.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Cabecera_IP
- Cable coaxial.* (s.f.). Obtenido de <http://html.rincondelvago.com/cable-coaxial.html>
- Cable coaxial.* (s.f.). Obtenido de <http://modul.galeon.com/aficiones1366312.html>
- Cable coaxial.* (s.f.). Obtenido de http://www.angelfire.com/cantina/la_guayaba_asesina/coaxial.htm
- Cable coaxial.* (s.f.). Obtenido de <http://www.movvam.com/tech/Oth/Coaxial%20cable.pdf>
- Cable de par trenzado.* (s.f.). Obtenido de <http://modul.galeon.com/aficiones1366306.html>
- Cable de par trenzado.* (s.f.). Obtenido de <http://www.hispazone.com/Guia/54/Cable-de-par-trenzado.html>
- Cableado estructurado.* (s.f.). Obtenido de <http://www.microsis.com.mx/servicios/cableado2.htm>
- Capa de enlace de datos.* (s.f.). Obtenido de <http://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r56452.DOC>
- Capa de enlace de datos.* (s.f.). Obtenido de <http://es.scribd.com/doc/13980265/CAPITULO-7-Capa-de-Enlace-de-Datos>
- Capa de transporte.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Nivel_de_transporte

REFERENCIAS

- Características de un servidor web.* (s.f.). Obtenido de <http://www.josecriado.com/hosting-alojamiento-web/caracteristicas-de-un-servidor-web/>
- Cifrado de Feistel.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Cifrado_de_Feistel
- Cifrado El Gamal.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Cifrado_ElGamal
- Clasificación de redes.* (s.f.). Obtenido de <http://es.scribd.com/doc/30693991/Clasificacion-de-Redes-Por-Distribucion-y-por-Forma-de-trabajo>
- Cliente/Servidor.* (s.f.). Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/marquez_a_bm/capitulo5.pdf
- Códigos de estado HTTP.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Anexo:C%C3%B3digos_de_estado_HTTP
- Compartir recursos a través de una red de ordenadores.* (s.f.). Obtenido de <http://html.rincondelvago.com/compartir-recursos-a-traves-de-una-red-de-ordenadores.html>
- Componentes de una red.* (s.f.). Obtenido de <http://www.slideshare.net/yaretzidelangel/componentes-de-una-red-presentation-818060>
- Computo forense.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/C%C3%B3mputo_forense
- Concentrador.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Concentrador>
- Control de acceso interno.* (s.f.). Obtenido de <http://www.seguinfo.com.ar/logica/accesointerno.htm>
- Control parental.* (s.f.). Obtenido de http://www.cantv.net/ciencia/seguridadeninternet/control_parental_info.asp
- Control, administración e integridad de logs.* (s.f.). Obtenido de http://www.wikilearning.com/monografia/control_administracion_e_integridad_de_logs-que_es_un_log/3485-2
- Cortafuego.* (s.f.). Obtenido de <http://www.masadelante.com/faqs/cortafuegos>

REFERENCIAS

Criptoanálisis. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Criptoan%C3%A1lisis>

Criptografía. (s.f.). Obtenido de http://www.matem.unam.mx/~rajsbaum/cursos/web/presentacion_seguridad_1.pdf

Criptografía . (s.f.). Obtenido de <http://es.kioskea.net/contents/crypto/crypto.php3>

Criptografía - Fundamentos. (s.f.). Obtenido de www.freewebs.com/patricklonga/Presentacion2_PUCP_Longa.pps

Criptografía de clave secreta. (s.f.). Obtenido de http://digital.csic.es/bitstream/10261/24545/1/Flujo_1.pdf

Criptología. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Criptolog%C3%ADa>

Criptología y seguridad. (s.f.). Obtenido de <http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-4.pdf>

Cultura de la ciberseguridad. (s.f.). Obtenido de <http://seguinfo.wordpress.com/2007/02/25/la-cultura-de-la-ciberseguridad/>

Definición de arquitectura cliente servidor. (s.f.). Obtenido de <http://www.monografias.com/trabajos24/arquitectura-cliente-servidor/arquitectura-cliente-servidor.shtml>

Definición de cliente servidor. (s.f.). Obtenido de http://docente.ucol.mx/sadany/public_html/bd/cs.htm

Definición de gateway. (s.f.). Obtenido de <http://www.mastermagazine.info/termino/5120.php>

Definición de gateway (telecomunicaciones). (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/gateway%20telecomunicaciones.php>

Definición de hub. (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/hub.php>

Definición de radius. (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/radius.php>

Definición de router. (s.f.). Obtenido de <http://definicion.de/router/>

Definición de servidor. (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/servidor.php>

Definición de servidor web. (s.f.). Obtenido de <http://www.masadelante.com/faqs/servidor-web>

REFERENCIAS

- Definición de switch.* (s.f.). Obtenido de <http://definicion.de/switch/>
- Delitos informáticos.* (s.f.). Obtenido de <http://www.slideshare.net/pallanur/delitos-informticos-anlisis-forense-1217854>
- Demonio.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Demonio_%28inform%C3%A1tica%29
- DES.* (s.f.). Obtenido de <http://es.kioskea.net/contents/crypto/des.php3>
- Descripción de los puertos UDP.* (s.f.). Obtenido de <http://support.microsoft.com/kb/136403/es>
- Detección de intrusos.* (s.f.). Obtenido de <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html>
- Dilemas éticos de la informática.* (s.f.). Obtenido de <http://www.revistaciencias.com/publicaciones/EkpuFEVpVpdivwIXpH.php>
- Dirección MAC.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC
- DMZ.* (s.f.). Obtenido de <http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3>
- DMZ.* (s.f.). Obtenido de <http://www.solusan.com/que-es-una-dmz.html>
- DNS Dinámicos.* (s.f.). Obtenido de <http://www.desarrolloweb.com/articulos/dns-dinamico.html>
- Domain Name System.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Domain_Name_System
- Downstream .* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/downstream.php>
- El DNS.* (s.f.). Obtenido de <http://www.dcc.uchile.cl/~jpiquer/Internet/DNS/node2.html>
- El estándar VoIP.* (s.f.). Obtenido de <http://www.monografias.com/trabajos33/estandar-voip/estandar-voip.shtml>
- El mejor monitoreo de libre descarga.* (s.f.). Obtenido de http://www.freedownloadmanager.org/es/downloads/monitoreo_de_red_gratis/
- El protocolo ARP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/arp.php3>
- El protocolo ARP.* (s.f.). Obtenido de <http://www.redesyseguridad.es/el-protocolo-arp/>
- El router para LAN.* (s.f.). Obtenido de <http://www.informaticamoderna.com/Router.htm>

REFERENCIAS

- El switch para redes LAN, características y capacidades.* (s.f.). Obtenido de <http://www.informaticamoderna.com/Switch.htm>
- Electronic Industries Alliance.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Electronic_Industries_Alliance
- Entorno social.* (s.f.). Obtenido de <http://definicion.de/entorno-social/>
- Estándar IEEE 802.11 X de WLAN.* (s.f.). Obtenido de http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf
- Estándares 802.* (s.f.). Obtenido de <http://estandaresieee802redes.blogspot.mx/>
- Evolución de los sistemas de detección, prevención y análisis de incidentes.* (s.f.). Obtenido de <http://revista.seguridad.unam.mx/numero-10/evoluci%C3%B3n-de-los-sistemas-de-detecci%C3%B3n-prevenci%C3%B3n-y-an%C3%A1lisis-de-incidentes>
- Explotaciones de día cero.* (s.f.). Obtenido de <http://blog.tresw.com/general/vulnerabilidades-dia-cero-0-day-exploits/>
- Falso positivo.* (s.f.). Obtenido de [http://es.wikipedia.org/wiki/Falso_positivo_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Falso_positivo_(inform%C3%A1tica))
- Falsos positivos para antología de seguridad informática II.* (s.f.). Obtenido de <http://es.scribd.com/doc/48054160/37/FALSOS-POSITIVOS>
- Fibra óptica.* (s.f.). Obtenido de http://html.rincondelvago.com/fibra-optica_18.html
- Fibra óptica.* (s.f.). Obtenido de <http://www.monografias.com/trabajos13/fibropt/fibropt.shtml>
- Firewall.* (s.f.). Obtenido de <http://geeks.ms/blogs/dmatey/archive/2007/01/16/un-firewall-es-un-accesorio-de-cocina-probando-isa-server-2006.aspx>
- Firewall.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Firewall>
- Firma digital.* (s.f.). Obtenido de <http://www.monografias.com/trabajos908/firma-digital/firma-digital.shtml>
- Firma digital.* (s.f.). Obtenido de <http://www.uv.es/sto/cursos/seguridad.java/html/sjava-15.htm>
- Fragmentación de paquetes.* (s.f.). Obtenido de <http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/fragmentacion.html>

REFERENCIAS

- Fragmentación de paquetes IP.* (s.f.). Obtenido de <http://es.scribd.com/doc/27238759/FRAGMENTACION-DE-PAQUETES-IP>
- Fragmentación IP.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Fragmentaci%C3%B3n_IP
- Frecuencia extremadamente baja.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Frecuencia_extremadamente_baja
- Frecuencia ultraalta.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/UHF>
- FTP.* (s.f.). Obtenido de <http://www.ordenadores-y-portatiles.com/ftp.html>
- Full Duplex.* (s.f.). Obtenido de <http://www.mastermagazine.info/termino/5092.php>
- Glosario de términos .* (s.f.). Obtenido de <http://www.pandasecurity.com/spain/homeusers/security-info/glossary/>
- GPRS.* (s.f.). Obtenido de <http://www.gsmspain.com/glosario/?palabra=GPRS>
- Gráfica de Comportamiento.* (s.f.). Obtenido de http://www.ecured.cu/index.php/Gr%C3%A1fica_de_Comportamiento
- GSM.* (s.f.). Obtenido de http://html.rincondelvago.com/gsm_2.html
- Half Duplex.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Half-duplex>
- Herramienta de monitoreo de redes.* (s.f.). Obtenido de http://www.es.paessler.com/network_monitoring_tool
- Herramienta forense: NetworkMiner.* (s.f.). Obtenido de <http://www.soyforense.com/2009/05/26/networkminer-herramienta-forense-de-analisis-de-red/>
- Herramienta forense: Stuxnet Scanner Tool.* (s.f.). Obtenido de <http://blog.trendmicro.es/stuxnet-scanner-una-herramienta-forense/>
- Herramienta forense: Xplico.* (s.f.). Obtenido de <http://www.sahw.com/wp/archivos/2009/09/01/xplico-una-herramienta-de-analisis-forense-de-trafico-de-red/>
- Herramientas para el monitoreo del estado de red.* (s.f.). Obtenido de <http://seguinfo.wordpress.com/2007/09/12/herramientas-para-el-monitoreo-del-estado-de-red/>

REFERENCIAS

- Hilos.* (s.f.). Obtenido de <http://www.xuletas.es/ficha/elementos-por-proceso/>
- Historia de la computación.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Historia_de_la_computaci%C3%B3n
- Historia de la computación.* (s.f.). Obtenido de <http://www.monografias.com/trabajos/histocomp/histocomp.shtml>
- Historia del hardware.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Historia_del_hardware_de_computador
- HTML.* (s.f.). Obtenido de <http://www.monografias.com/trabajos7/html/html.shtml>
- HTTP.* (s.f.). Obtenido de <http://www.masadelante.com/faqs/que-significa-http>
- Hub.* (s.f.). Obtenido de <http://www.informaticamoderna.com/Hub.htm>
- Hypertext Transfer Protocol.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Http>
- IANA.* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/iana.php>
- ICMP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/icmp.php3>
- IDEA.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/International_Data_Encryption_Algorithm
- Identificación y análisis de patrones de tráfico malicioso en redes IP.* (s.f.). Obtenido de <http://www.slideshare.net/dragonjar/identificacin-y-anlisis-de-patrones-de-trafico-malicioso-en-redes-ip>
- Impacto de la tecnología y la informática en los individuos.* (s.f.). Obtenido de <http://html.rincondelvago.com/impacto-de-la-tecnologia-y-la-informatica-en-los-individuos.html>
- Impacto económico.* (s.f.). Obtenido de <http://www.larevistainformatica.com/impacto-economico-tecnologia-informatica.htm>
- Impacto social.* (s.f.). Obtenido de <http://es.scribd.com/doc/7440549/Impacto-Social>
- Impacto social.* (s.f.). Obtenido de <http://www.mailxmail.com/curso-delitos-informaticos/impacto-nivel-social>
- Implementación de una DMZ.* (s.f.). Obtenido de http://www.cudi.edu.mx/primavera_2006/presentaciones/wireless02_mario_farias.pdf

REFERENCIAS

- Información.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Informaci%c3%b3n>
- Informática forense.* (s.f.). Obtenido de <http://html.rincondelvago.com/informatica-forense.html>
- Instituto de Ingenieros Eléctricos y Electrónicos.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/IEEE>
- Instituto Nacional Estadounidense de Estándares.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/ANSI>
- Interconexión de redes.* (s.f.). Obtenido de <http://www.monografias.com/trabajos11/inter/inter.shtml>
- Interfaz de datos distribuidos por fibra.* (s.f.). Obtenido de <http://www.consulintel.es/Html/Tutoriales/Articulos/fddi.html>
- Internet.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Internet>
- Internet Engineering Task Force.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/IETF>
- Introducción a los ataques.* (s.f.). Obtenido de <http://es.kioskea.net/contents/ataques/ataques.php3>
- Introducción a Wi-Fi (802.11 o WiFi).* (s.f.). Obtenido de <http://es.kioskea.net/contents/wifi/wifiintro.php3>
- Introducción al NAT.* (s.f.). Obtenido de <http://www.adslayuda.com/Generico-nat.html>
- Introducción al servicio y requisito del puerto de red para el sistema Windows server.* (s.f.). Obtenido de <http://support.microsoft.com/kb/832017/es>
- IP.* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/ip.php>
- IP estática o dinámica.* (s.f.). Obtenido de <http://es.kioskea.net/faq/569-seguridad-ip-estatica-o-dinamica>
- IPTables en 21 segundos.* (s.f.). Obtenido de http://www.pello.info/filez/IPTABLES_en_21_segundos.html
- ISACA.* (s.f.). Obtenido de <http://www.isaca.org/About-ISACA/History/Espanol/Pages/default.aspx>
- ISDN.* (s.f.). Obtenido de <http://es.kioskea.net/contents/technologies/rnis.php3>

REFERENCIAS

- ISO.* (s.f.). Obtenido de <http://www.gestiopolis.com/recursos/experto/catsexp/pagans/ger/49/iso.htm>
- Java Development Kit.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Java_Development_Kit
- jFlow.* (s.f.). Obtenido de <http://www.plixer.com/blog/general/what-is-jflow/>
- Kernel.* (s.f.). Obtenido de <http://www.linux-es.org/kernel>
- La fibra óptica.* (s.f.). Obtenido de <http://glorsarm.tripod.com/index-4.html>
- La fibra óptica.* (s.f.). Obtenido de <http://neo.lcc.uma.es/evirtual/cdd/tutorial/fisico/fibra.html>
- La importancia del software de auditoría de red.* (s.f.). Obtenido de <http://www.gfihispana.com/lannetscan/network-auditing-software.htm>
- Las redes.* (s.f.). Obtenido de <http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.shtml>
- Las redes. Transmisión de datos.* (s.f.). Obtenido de <http://www.mailxmail.com/curso-redes-transmicion-datos-2/control-acceso-medio-mac-control-enlace-logico-llc>
- Malware.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Malware>
- Manual de AES.* (s.f.). Obtenido de http://www.lawebdelprogramador.com/cursos/Criptografia/4814-Manual_de_AES_-_Advanced_Encryption_Standard.html
- Manual de políticas de seguridad informática.* (s.f.). Obtenido de <http://inf-tek.blogia.com/2009/060207-8.5-manual-de-politicas-de-seguridad-informatica.php>
- Mapa de red.* (s.f.). Obtenido de http://en.wikipedia.org/wiki/Network_mapper
- Mapa de red.* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/mapa%20de%20red.php>
- Metasploit.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Metasploit>
- Metasploit.* (s.f.). Obtenido de <http://www.paginasprodigy.com/jez2904/files/metasploit.pdf>

REFERENCIAS

- Metodología básica de análisis forense*. (s.f.). Obtenido de <http://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-1-de-4.xhtml>
- Metodología básica de análisis forense*. (s.f.). Obtenido de <http://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-2-de-4.xhtml>
- Metodología básica de análisis forense*. (s.f.). Obtenido de <http://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-3-de-4.xhtml>
- Metodología básica de análisis forense*. (s.f.). Obtenido de <http://www.dragonjar.org/metodologia-basica-de-analisis-forense-parte-4-de-4.xhtml>
- MIB*. (s.f.). Obtenido de <http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf>
- Modo de transferencia asíncrona*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode
- Monitoreo de aplicaciones web*. (s.f.). Obtenido de http://www.tecnet.com.mx/index.php?option=com_content&view=article&id=57
- Monitoreo de red*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Monitoreo_de_red
- Monitoreo de tráfico*. (s.f.). Obtenido de <http://ruben.cheng-ca.com/es/knowledge/network/trafficmon.htm>
- NAT*. (s.f.). Obtenido de <http://www.netfilter.org/documentation/HOWTO/es/NAT-HOWTO.txt>
- NetBIOS*. (s.f.). Obtenido de http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/protocol1.htm
- NetSupport Manager 10.5*. (s.f.). Obtenido de <http://ba-k.com/showthread.php?t=295153>
- On-Demand Link Padding in Traffic Anonymizing*. (s.f.). Obtenido de <http://www.eecs.harvard.edu/~htk/publication/2005-jit-cheng-kung-tan.pdf>
- Operación Aurora*. (s.f.). Obtenido de <http://blogs.eset-la.com/laboratorio/2010/01/21/que-es-operacion-aurora/>

REFERENCIAS

- Organización internacional para la estandarización.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/ISO>
- Organizaciones de estandarización.* (s.f.). Obtenido de http://docente.ucol.mx/al940435/public_html/estandares.htm
- Organizaciones de estandarización.* (s.f.). Obtenido de http://docente.ucol.mx/al980347/public_html/organiza.htm
- OSI.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/OSI>
- Paneles de parcheo.* (s.f.). Obtenido de <http://esp.hyperlinesystems.com/catalog/patch-panels/>
- Paquete IP.* (s.f.). Obtenido de <http://www.ordenadores-y-portatiles.com/paquete-ip.html>
- PDU.* (s.f.). Obtenido de http://www.ehow.com/about_6471111_tcp_lp-_amp_-pdu_.html
- Peticiones HTTP: Métodos de petición.* (s.f.). Obtenido de <http://trevinca.ei.uvigo.es/~txapi/espanol/proyecto/superior/memoria/node46.html>
- Política de seguridad.* (s.f.). Obtenido de <http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad>
- Protección de datos.* (s.f.). Obtenido de <http://www.seguinfo.com.ar/proteccion/proteccion.htm>
- Protocolo de Control de Transmisión.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Transmission_Control_Protocol
- Protocolo de control de transporte (TCP).* (s.f.). Obtenido de [http://technet.microsoft.com/es-es/library/cc756754\(W.S.10\).aspx](http://technet.microsoft.com/es-es/library/cc756754(W.S.10).aspx)
- Protocolo de Internet.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Protocolo_de_Internet
- Protocolo de seguridad web.* (s.f.). Obtenido de <http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml>
- Protocolo de transferencia de archivos.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/ftp.php3>

REFERENCIAS

- Protocolo HTTP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/http.php3>
- Protocolo IP.* (s.f.). Obtenido de <http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html>
- Protocolo simple de transferencia de correo.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
- Protocolo SNMP.* (s.f.). Obtenido de <http://www.pablin.com.ar/computer/info/varios/snmp.htm>
- Protocolo SNMP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/snmp.php3>
- Protocolo TCP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/tcp.php3>
- Protocolo Telnet.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/telnet.php3>
- Protocolo UDP.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/UDP>
- Protocolos de Internet.* (s.f.). Obtenido de <http://es.scribd.com/doc/22659415/Protocolos-de-Internet>
- Proxy.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Proxy>
- Prueba de penetración.* (s.f.). Obtenido de <http://comunidad.dragonjar.org/f184/definicion-de-test-de-penetracion-4780/>
- Pruebas de penetración.* (s.f.). Obtenido de https://www.pcisecuritystandards.org/documents/spanish_infosupp_11_3_penetration_testing.pdf
- Puente de red.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Puente_de_red
- Puerta de enlace.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Puerta_de_enlace
- Puerta de enlace predeterminada.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Puerta_de_enlace_predeterminada
- Puertas de enlace gateway.* (s.f.). Obtenido de <http://galeon.com/arquitecturaserver/gateway.htm>
- Puertas de enlace predeterminadas.* (s.f.). Obtenido de [http://technet.microsoft.com/es-es/library/cc779696\(WS.10\).aspx](http://technet.microsoft.com/es-es/library/cc779696(WS.10).aspx)
- Puerto de red.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Puerto_de_red
- Punto de acceso.* (s.f.). Obtenido de <http://tematica.mercadolibre.com.mx/access-point>

REFERENCIAS

- Rack*. (s.f.). Obtenido de <http://esp.hyperlinesystems.com/catalog/cabinets/rk.shtml>
- Rack*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Rack>
- RARP*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/RARP>
- Red de área metropolitana*. (s.f.). Obtenido de http://html.rincondelvago.com/man_3.html
- Red de computadoras*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Redes_de_datos
- Red en anillo*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Red_en_anillo
- Red en árbol*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Red_en_%C3%A1rbol
- Red en bus*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Red_en_bus
- Red en estrella*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Red_en_estrella
- Red en malla*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Topolog%C3%ADa_en_malla
- Red inalámbrica*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica
- Red punto a punto*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Peer-to-peer>
- Redes*. (s.f.). Obtenido de http://www.uhu.es/diego.lopez/Docs_ppal/Transparencias%20Redes%20tema1%2005-06.pdf
- Redes de Computadoras*. (s.f.). Obtenido de <http://www.monografias.com/trabajos24/redes-computadoras/redes-computadoras.shtml>
- Redes: Topología*. (s.f.). Obtenido de <http://vgg.sci.uma.es/redes/topo.html>
- RFC*. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Request_For_Comments
- RMON*. (s.f.). Obtenido de http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html#RMON_Remote_MONitoring
- RMON*. (s.f.). Obtenido de <http://www.normes-internet.com/normes.php?rfc=rfc3577&lang=es>
- Router*. (s.f.). Obtenido de <http://es.kioskea.net/contents/lan/routeurs.php3>
- Router*. (s.f.). Obtenido de <http://es.scribd.com/doc/39774664/Router>

REFERENCIAS

- Seguridad de la capa de transporte.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Transport_Layer_Security
- Seguridad de la información.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- Seguridad de sistemas.* (s.f.). Obtenido de <http://www.duiops.net/hacking/seguridad-sistemas.htm>
- Seguridad en la capa de transporte.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Transport_Layer_Security
- Seguridad en redes inalámbricas.* (s.f.). Obtenido de <http://www.zonagratis.com/servicios/seguridad/wireles.html>
- Seguridad física.* (s.f.). Obtenido de <http://www.seguinfo.com.ar/fisica/seguridadfisica.htm>
- Seguridad física.* (s.f.). Obtenido de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGLI200_archivos/seguridadfisica.htm
- Seguridad física informática.* (s.f.). Obtenido de http://www.cybernautas.es/seguridad_informatica/seguridad-fisica-informatica/
- Seguridad informática.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- Seguridad informática.* (s.f.). Obtenido de <http://www.alegsa.com.ar/Dic/seguridad%20informatica.php>
- Seguridad Informática.* (s.f.). Obtenido de <http://lateoriadelbit.wordpress.com/tag/seguridad-informatica/>
- Seguridad Informática.* (s.f.). Obtenido de <http://reguleon.espacioblog.com/post/2010/03/04/seguridad-informatica-estudio-percepcion-seguridad-la>
- Seguridad informática: Nivel Físico.* (s.f.). Obtenido de <http://www.seguinfo.com.ar/politicas/fisico.htm>
- Seguridad informática: Nivel Humano.* (s.f.). Obtenido de <http://www.seguinfo.com.ar/politicas/humano.htm>

REFERENCIAS

- Seguridad informática: Políticas de seguridad.* (s.f.). Obtenido de <http://www.segu-info.com.ar/politicas/>
- Seguridad informática: Políticas de Seguridad de la Información.* (s.f.). Obtenido de <http://www.segu-info.com.ar/politicas/polseginf.htm>
- Seguridad lógica.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Seguridad_l%C3%B3gica
- Seguridad lógica.* (s.f.). Obtenido de http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/mattos_le/cap2.PDF
- Seguridad lógica.* (s.f.). Obtenido de <http://www.segu-info.com.ar/logica/seguridadlogica.htm>
- Seguridad perimetral.* (s.f.). Obtenido de Seguridad perimetral
- Servicio de mensajes cortos.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Sms>
- Servidor.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Servidor>
- Servidores DNS, Invisibles e imprescindibles para la navegación web.* (s.f.). Obtenido de <http://www.miniguias.com/trucos/servidores-dns-invisibles-e-imprescindibles-para-la-navegacion-web/>
- Servlet.* (s.f.). Obtenido de http://chuwiki.chuidiang.org/index.php?title=Ejemplo_sencillo_de_Servlet
- sFlow.* (s.f.). Obtenido de <http://en.wikipedia.org/wiki/SFlow>
- Sistema de archivos de red.* (s.f.). Obtenido de <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-nfs.html>
- Sistemas de detección de intrusos y Snort.* (s.f.). Obtenido de <http://www.maestrosdelweb.com/editorial/snort/>
- SMTP.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
- SMTP.* (s.f.). Obtenido de <http://support.microsoft.com/kb/87022/es>
- SNMP.* (s.f.). Obtenido de <http://es.kioskea.net/contents/internet/snmp.php3>
- SNMP.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
- Snooping.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/Snooping>

REFERENCIAS

- Socket*. (s.f.). Obtenido de <http://www.masadelante.com/faqs/socket>
- Spam*. (s.f.). Obtenido de <http://www.segu-info.com.ar/malware/spam.htm>
- SSID predeterminada*. (s.f.). Obtenido de <http://www.laneros.com/f110/ssid-predeterminada-101088/>
- SSL*. (s.f.). Obtenido de <http://penta2.ufrgs.br/gereseg/unlp/tut1998/ssl.htm>
- SSL*. (s.f.). Obtenido de http://www.wikilearning.com/curso_gratis/protocolos_seguros_para_el_web-ssl_secure_socket_layer_y_tls_transport_layer_secure/6091-4
- TCP*. (s.f.). Obtenido de http://en.wikipedia.org/wiki/Transmission_Control_Protocol
- TCP Half scan (Stealth scan)*. (s.f.). Obtenido de <http://xforce.iss.net/xforce/xfdb/405>
- TCP/IP: Familia de protocolos de Internet*. (s.f.). Obtenido de <http://redeslorenaymaite.blogspot.com/2010/04/tcpip-familia-de-protocolos-de-internet.html>
- Tecnología de información*. (s.f.). Obtenido de http://www.degerencia.com/tema/tecnologia_de_informacion
- Tendencia en ataques*. (s.f.). Obtenido de <http://www.viruslist.com/sp/analysis?pubid=207271108>
- Tendencia en ataques informáticos*. (s.f.). Obtenido de http://www.iworld.com.mx/iw_Opinions_read.asp?IWID=79
- Tercera y cuarta generación de computadoras*. (s.f.). Obtenido de <http://html.rincondelvago.com/tercera-y-cuarta-generacion-de-computadoras.html>
- TFTP*. (s.f.). Obtenido de <http://es.wikipedia.org/wiki/TFTP>
- Tipos de redes*. (s.f.). Obtenido de <http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/REDES02.htm>
- Tipos de redes por su dispersión*. (s.f.). Obtenido de <http://homejq.tripod.com/redes/tiposredes.htm>

REFERENCIAS

- Topología en red.* (s.f.). Obtenido de
http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red
- Topologías.* (s.f.). Obtenido de <http://www.angelfire.com/mi2/Redes/topologia.html>
- Traducción de dirección de red (NAT).* (s.f.). Obtenido de
<http://www.monografias.com/trabajos20/traductor-nat/traductor-nat.shtml>
- Traffic Confidentiality.* (s.f.). Obtenido de
http://www.streetdirectory.com/travel_guide/137624/computers/traffic_confidentiality.html
- Triple DES.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Triple_DES
- UDP.* (s.f.). Obtenido de <http://www.masadelante.com/faqs/udp>
- Unión Internacional de Telecomunicaciones.* (s.f.). Obtenido de
http://es.wikipedia.org/wiki/Uni%C3%B3n_Internacional_de_Telecomunicaciones
- URL.* (s.f.). Obtenido de http://es.wikipedia.org/wiki/Localizador_uniforme_de_recursos
- Virus Informático.* (s.f.). Obtenido de
http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico
- Virus Informáticos.* (s.f.). Obtenido de
http://es.wikipedia.org/wiki/Virus_inform%C3%A1ticos
- VPN.* (s.f.). Obtenido de <http://www.monografias.com/trabajos11/repri/repri.shtml>
- WiFi.* (s.f.). Obtenido de <http://www.misrespuestas.com/que-es-wifi.html>
- WiMAX.* (s.f.). Obtenido de <http://www.ordenadores-y-portatiles.com/wimax.html>
- WiMAX: ¿Qué es y características?* (s.f.). Obtenido de
<http://www.configurarequijos.com/doc1087.html>
- WLAN.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/WLAN>
- WLAN LAN inalámbrica.* (s.f.). Obtenido de
<http://es.kioskea.net/contents/wireless/wlan.php3>
- WPAN.* (s.f.). Obtenido de <http://es.wikipedia.org/wiki/WPAN>

