



Universidad Nacional Autónoma de México

Facultad de Ingeniería

**“Sitio Web de apoyo para el proceso
enseñanza-aprendizaje de la
asignatura Administración de Redes”**

TESIS PROFESIONAL

Que para obtener el título de:

INGENIERA EN COMPUTACIÓN

Presentan:

Angélica Cervantes Avalos

Dulce Jazmin Cruz Morales

Directora de tesis:

M.C. Cintia Quezada Reyes

México, D.F. Junio 2012





Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



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

"No puedo responder otra cosa que gracias y gracias"

SHAKESPEARE, William

A mi mamá Josefina Avalos Fajardo:

Por siempre brindarme tu apoyo incondicional pero sobre todo por tu amor. Por estar a mi lado en los momentos difíciles y por tus palabras de aliento y ánimo.

Eternamente estaré agradecida contigo por haberme dado lo más hermoso que tengo, la vida y por hacer de mí la mujer que soy.

Con todo mi amor te dedico este trabajo que significa la culminación de mi vida académica y para lo cual has luchado hombro a hombro a mi lado, pero no sólo eso sino el inicio de mi vida profesional.

A mi papá C.P. José Luis Tomás Cervantes Cervantes:

Por tu apoyo incondicional y por la gran confianza que siempre me tuviste, pero sobre todo gracias por el inmenso cariño que día con día me demostraste.

Gracias por ser el mejor papá que pude haber tenido, por ser mi fuerza, por tu gran lucha por darme lo mejor y esta carrera profesional.

Porque Dios decidió que en este momento tan importante estuvieras desde el cielo mirándome, el mejor homenaje que te pude brindar fue la culminación de esta carrera profesional y seguir luchando siempre por mis sueños como me enseñaste.

Vives y vivirás por siempre en mi mente y en mi corazón y siempre recordaré los bellos momentos que pasamos juntos.

Con todo mi amor dedico este trabajo a tu memoria ya que fuiste parte esencial para que lo lograra.

A mis hermanos por todo su cariño y apoyo:

Berenice Paloma: Por la alegría que le das a mi vida, por tu cariño y porque con tu apoyo incondicional me haces sentir segura, nunca dejes de consentirme hermana te quiero mucho.

José Luis Jonathan: no encontré las palabras para expresar lo agradecida que estoy contigo pero sé que la vida y la fortuna siempre estarán de tu lado porque tienes un gran corazón y claro, siempre tendrás en mí apoyo incondicional. Te dedico este trabajo con todo mi cariño y admiración ya que sin ti no hubiera sido posible lograrlo.

A mi hermosa familia, con mucho cariño: A mis abuelitos Thomas y Angelina, Joaquín y María del Refugio; a mis tíos, María Teresa, Joaquín, Concepción, Bárbara, Roberto, Nieves; y bueno creo que saben lo complicado que sería mencionar a todos pero eso no quiere decir que no me acuerde de cada uno. A ti Efrén porque no estás aquí pero sé que tu alma si lo está y porque tuviste los mismos sueños que yo te dedico con todo mi corazón mi tesis.

Les agradezco a todos y cada uno de ustedes el cariño que me han brindado y toda la alegría que he vivido con ustedes.

A mis amigos: Emmanuel, Jazmín, Omar, Daniel, Sandra, Fernanda, Jonathan, por todos los momentos increíbles que pasamos y pasaremos juntos, por el gran equipo que formamos para trabajar día a día en nuestra carrera profesional y porque nuestra amistad sea para toda la vida. Gracias por todas las sonrisas, los quiero mucho y los llevaré por siempre en mi corazón.

Daniel, que te puedo decir, muchas gracias por estos cinco años de conocernos y en los cuales hemos compartido y vivido tantas cosas, por el apoyo que me has brindado y por alentarme a realizar mis sueños y recuerda que eres muy importante para mí.

A la M.C. Cintia Quezada Reyes: Por todo su apoyo y tiempo dedicado para la realización y culminación satisfactoria de esta tesis, por su amistad y por ser una excelente profesora de la cual obtuve muchos conocimientos.

A todos mis profesores de la Facultad de Ingeniería: Por todos sus conocimientos impartidos los cuales serán la herramienta y las bases para desarrollarme en la vida profesional, gracias a todos aquellos que me brindaron su tiempo, atención y amistad.

Gracias a mi Facultad de Ingeniería porque ahí viví una época increíble de mi vida y donde me realice como estudiante y persona.

Es y será un honor y orgullo ser egresada de la Universidad Nacional Autónoma de México. Gracias por mis profesores, mis amigos, por todos y cada uno de los momentos maravillosos e inolvidables que he vivido en sus bellas instalaciones y que han contribuido no sólo en mi formación académica sino humana.

“POR MI RAZA HABLARÁ EL ESPÍRITU”

Angélica Cervantes Avalos

A lo largo de mi vida, desde que llegué a este mundo y hasta este momento, han estado presentes personas que considero muy valiosas para mí, ya que todas ellas han contribuido de diversas formas en mi formación, tanto personal como profesional. Ellas me han brindado su apoyo y confianza incondicionales y desinteresados a cada momento. Definitivamente, no sería lo que soy ni estaría en el lugar que estoy sin ellas. Ahora, que estoy a punto de concluir el primer proyecto, más grande y valioso de mi vida, en el que puse en práctica e hice uso cada una de sus aportaciones, quiero aprovechar para dedicárselos y expresarles mi eterno y profundo agradecimiento.

En primer lugar y más importante a mi madre, la Sra. Margarita Cruz Morales; gracias mami por tomar la decisión de darme la vida, por criarme con todos esos valores que sólo tú podrías haberme dado, pero sobre todo por inculcarme los valores de responsabilidad y agradecimiento. Eres mi principal fuente de inspiración y fuerza. Quiero que sientas que éste, que es un logro para mí, lo es también tuyo, uno más de tantos que has tenido en tu vida. Estoy muy orgullosa de ti, espero lo estés tú de mi.

A mi familia, a mis hermanas Elizabeth Cruz Morales y Miriam Tapia Cruz. Por aguantarme todos los días que duró este proyecto, por disculpar mis ausencias en momentos importantes en sus vidas, por sus palabras de aliento y fuerza. A Víctor Alberto Santana Delgadillo, por su apoyo incondicional cuando más lo he necesitado, por escucharme y transmitirme sus experiencias y conocimientos día a día.

A mis amigos, Emma Acevedo Martínez, Sandra Sánchez Escobar y Angélica Cervantes Avalos, por escucharme, aconsejarme y apoyarme incondicionalmente.

Orgullosamente a la Universidad Nacional Autónoma de México, y con ella mi Facultad de Ingeniería, mi segundo hogar; a mis profesores, mi segunda familia, por transmitirme sus conocimientos, enseñanzas y sus experiencias; y hacer de mí una persona consciente de las necesidades de México; por prepararme para salir allá afuera y ser capaz de utilizar todas las habilidades y conocimientos que adquirí para ir en busca de un bienestar común.

Gracias a todos.

“POR MI RAZA HABLARÁ EL ESPÍRITU”

Dulce Jazmin Cruz Morales

ÍNDICE

INTRODUCCIÓN	1
I. METODOLOGÍA	5
1.1 Problemática.....	7
1.2 Preguntas de investigación	7
1.3 Justificación.....	7
1.4 Objetivos.....	8
1.3.1 General.....	8
1.3.2 Particular.....	8
1.5 Hipótesis.....	8
II. MARCO TEÓRICO	9
CAPÍTULO 1: CONCEPTOS BÁSICOS	11
1.1 Red de computadoras.....	13
1.2 Medios de transmisión.....	13
1.3 Topologías de red.....	22
1.4 Clasificación de las redes por su tamaño.....	30
CAPÍTULO 2: PLANEACIÓN	35
2.1 Objetivos del diseño en las redes.....	37
2.2 Requerimientos de hardware.....	41
2.3 Requerimientos de software.....	45
2.4 Direccionamiento lógico.....	45
a) Subnetting.....	52
b) VLSM.....	57
2.5 Diseño de políticas de cómputo.....	60
2.6 Ética informática.....	68
CAPÍTULO 3: ORGANIZACIÓN	71
3.1 Definición del modelo básico de administración de redes.....	73
3.2 Modelo TMN.....	78
3.3 Modelo TOM.....	86
3.4 Modelo eTOM.....	87
3.5 Definición de protocolos de administración de redes.....	93
a) SNMP.....	93
b) CMIP.....	97
c) CORBA.....	104

CAPÍTULO 4: INTEGRACIÓN.....	111
4.1 Definición de tecnologías de telecomunicaciones.....	107
a) PDH.....	107
b) SDH.....	110
c) DWDM.....	121
4.2 Definición de tecnologías de telefonía.....	126
a) SS7.....	126
b) VoIP.....	129
c) ISDN.....	131
d) xDSL.....	133
4.3 Definición de comunicaciones inalámbricas.....	136
a) Estándar IEEE 802.11.....	136
b) Estándar IEEE 802.16.....	139
c) TDMA.....	143
d) CDMA.....	145
e) GSM.....	146
f) GPRS.....	152
4.4 INTERNET2.....	156
4.5 Videoconferencia.....	159
4.6 Qué es la evaluación de proyectos.....	160
a) Metodología.....	161
CAPÍTULO 5: DIRECCIÓN.....	167
5.1 Dirección general.....	169
5.2 Habilidades directivas del administrador.....	170
5.3 Cómo lograr que un equipo de trabajo sea efectivo.....	172
5.4 Definición de conflicto.....	177
CAPÍTULO 6: CONTROL.....	181
6.1 Definiciones de seguridad en redes.....	183
6.2 Normatividad en seguridad informática.....	192

a) Criterios comunes.....	192
b) Serie ISO 27000.....	195
6.3 Auditoría informática.....	201
6.4 Plan de contingencias informático.....	204
III. DESARROLLO.....	207
CAPÍTULO 7: SITIO WEB EDUCATIVO.....	209
7.1 Conceptos básicos.....	211
7.2 Desarrollo de sitio web.....	214
7.3 Actividades de evaluación.....	260
IV. RESULTADOS.....	265
V. CONCLUSIONES.....	269
VI. GLOSARIO.....	275
VII. REFERENCIAS.....	295
VIII. ANEXOS.....	303
ANEXO A. Manual del usuario.....	305

INTRODUCCIÓN

“Saber no es suficiente, debemos aplicar. Desear no es suficiente, debemos hacer”.

Johann W. Von Goethe

Nos hemos percatado con el correr de los años la evolución que ha manifestado la tecnología y con ella nuestro espacio y tiempo, así, uno de los descubrimientos más grandes y sobre todo atractivo para la humanidad han sido las redes de datos, las cuales juegan un papel primordial hoy en día. Tal avance rebasa las fronteras de la industria, ya que se ha vuelto un elemento que forma parte de la vida cotidiana, por lo que las instituciones deben estar a la vanguardia en dicho tema, así también los profesionales, que deben contar con los conocimientos básicos necesarios para enfrentarse a un mundo en el que las redes de datos están presentes en todos o casi todos los ámbitos de su trabajo.

Es por tal motivo el interés de proporcionar una herramienta que apoye al alumno, futuro profesional, en su aprendizaje de los temas de la asignatura Administración de Redes. Además, y por la misma razón, facilitar a los profesores a que optimicen el proceso de enseñanza.

Dicho lo anterior, se optó por elaborar esta tesis que plantea la construcción de un sitio web. Éste incluye material didáctico que abarca todos los temas abordados actualmente en el temario de la asignatura, los cuales son extensos y se encuentran dispersos tanto en fuentes impresas como digitales. Con esto no nos referimos a que por el simple hecho de consultar el material contenido en el sitio el alumno se vuelva un experto en los temas, pero sí los comprenderá con mayor facilidad.

Vale la pena recalcar que el alcance de esta tesis es lograr el objetivo de apoyo al proceso de enseñanza-aprendizaje de la asignatura de Administración de redes y no el de presentar y/o describir el procedimiento para el desarrollo y construcción de un sitio web.

Así, el presente trabajo está conformado de siete capítulos que se encuentran debidamente interrelacionados y los cuales se describen brevemente a continuación.

El primer capítulo de nombre *conceptos básicos* contiene la explicación y descripción de conceptos fundamentales de redes de datos necesarios para entender temas posteriores; introduciendo y familiarizando al alumno en estos temas para lograr un aprendizaje efectivo en el ámbito de la administración de las redes.

El segundo capítulo, *planeación*, concentra información acerca de los elementos que conforman una red de datos y cómo se lleva a cabo la planeación de una nueva red, lo que implica analizar los objetivos que deberá satisfacer, así como también cuestiones de políticas y ética que rigen el entorno de la computación.

En el tercer capítulo denominado *organización*, se define cómo debe llevarse a cabo la administración de una red, esto con base en modelos de administración de redes. Para ello deben ser tomados en cuenta los objetivos que la red ha de satisfacer y las tareas que deberá desarrollar el administrador para cumplir con mencionados objetivos. Por lo que en el capítulo en cuestión se describe detalladamente la clasificación de los modelos de administración así como los elementos que componen a cada uno de ellos para que de esta manera el lector sea capaz de aplicar los modelos para la administración en las redes de datos.

En el cuarto capítulo llamado *integración*, se dan a conocer algunas de las tecnologías de telecomunicaciones, telefonía y comunicaciones inalámbricas que se implementan en las redes de datos. Se mencionan antecedentes, conceptos, funcionamiento, características, ventajas y desventajas de cada tecnología.

También se define y describe el proceso de la evaluación de proyectos lo cual conlleva a aplicar los conocimientos antes mencionados para la búsqueda de soluciones que aseguren resolver algún problema de manera eficiente, rentable y segura que pudiera estar presente en una red de datos determinada.

El quinto capítulo titulado *dirección*, engloba todos los aspectos para identificar el perfil y las habilidades que deberá poseer un directivo. Cuestiones como: habilidades del administrador, trabajo en equipo y su buen funcionamiento; liderazgo y conflictos laborales, ya que desempeñan un papel fundamental en toda organización para obtener los resultados esperados en un determinado proyecto.

En el sexto capítulo denominado *control* se define una serie de conceptos básicos en el ámbito de seguridad informática para colocar al lector en este contexto. Así mismo se habla de historia, definición y estructura de algunos estándares de seguridad.

Por último, en el séptimo capítulo, *sitio web educativo*, se describe la problemática planteada anteriormente, se especifican los objetivos, hipótesis, análisis, metodología y desarrollo del sitio web, aspectos fundamentales que forman parte de la realización de éste proyecto. En éste capítulo se pretende informar sobre aspectos técnicos y funcionales para utilización de la herramienta y condiciones que se deben cumplir para el óptimo funcionamiento y administración del sistema.

Cabe aclarar que la realización del sitio web es el medio que se eligió para cumplir el objetivo de esta tesis, el cual es brindar una herramienta de apoyo al proceso de enseñanza aprendizaje de la asignatura de Administración de Redes.

METODOLOGÍA

1.1 Problemática

El problema que tenemos es que la información de los temas incluidos en el temario de la asignatura *Administración de Redes* es muy extensa y no se encuentra concentrada en alguna fuente impresa o digital, por lo que el alumno se sitúa en un mundo de información que sólo pretende memorizar, ya que no cuenta con un criterio para distinguir entre información valiosa y complementaria.

Por otra parte, los profesores disponen aproximadamente de 48 horas en el semestre para cubrir el temario, debido a ello, la mayoría de las veces, no le da cabida a evaluar objetivamente el aprendizaje de los alumnos.

1.2 Pregunta de investigación

¿Cómo brindar apoyo tanto a profesores como a alumnos en su proceso de enseñanza-aprendizaje de la asignatura de *Administración de Redes*?

1.3 Justificación

Ante la situación explicada y por las ventajas que nos aporta, se optó por realizar un sitio web, ya que éste representa el medio idóneo de hacer llegar a los alumnos y profesores el apoyo para optimizar su proceso de enseñanza-aprendizaje debido a las siguientes razones:

- Permite la concentración y disponibilidad de la información.
- La información recabada y presentada va encaminada con el firme propósito de lograr que el alumno se interese y comprenda más rápido cada uno de los temas de la asignatura, mediante un diseño web atractivo. Con esto, no nos referimos a que por el simple hecho de leer el sitio el alumno se vuelva un experto en los temas, pero sí servirá como apoyo y sobretodo como fuente de consulta fiable.
- Aporta a los profesores un indicador de evaluación, que podrá tomar en cuenta de acuerdo a su criterio.

La limitación de esta tesis es:

No se presenta a detalle el desarrollo, metodología ni la manera en que se codifico el sitio así como las pruebas exhaustivas de éste, debido a su extensión y a que el objetivo general se refiere al apoyo en el proceso de enseñanza-aprendizaje de la asignatura de *Administración de Redes* y no al de cómo se desarrollan sitios web.

1.3 Objetivos

1.3.1 Objetivo General

Brindar apoyo al proceso enseñanza-aprendizaje de la asignatura Administración de Redes.

1.3.2 Objetivos Específicos

1. Realizar un sitio web que contenga información que cubra el temario de la asignatura Administración de Redes, así como la inclusión de ligas de consulta para ahondar en los temas.
2. Agregar al sitio web una sección de exámenes para evaluar al alumno, así como una sección que contenga dichas evaluaciones que el profesor podrá consultar; tal información le servirá como referencia para reforzar y optimizar su proceso de enseñanza de forma objetiva.

1.4 Hipótesis

Hi: Al desarrollar un sitio web educativo que trate en específico de los temas incluidos en la asignatura de Administración de Redes se obtendrá una herramienta de apoyo tanto para profesores como para alumnos en su proceso de enseñanza – aprendizaje respectivamente.



MARCO TEÓRICO

CAPÍTULO 1

Conceptos básicos



“No se puede desatar un nudo sin saber cómo está hecho”

Aristóteles.

1.1 Red de Computadoras

Un grupo de computadoras y otros dispositivos interconectados a través de uno o varios medios de transmisión cuya finalidad es la de transferir e intercambiar datos entre sí, así como compartir recursos.

El uso de redes de computadoras proporciona los siguientes beneficios:

- Acceso a información remota.
- Comercio electrónico.
- Compartir recursos.
- Correo electrónico.
- Intercambio de datos e información.

1.2 Medios de transmisión en las redes

Un medio de transmisión es el soporte o forma de conexión que permite la transferencia de datos entre dos dispositivos o nodos en una red. Los cuales se clasifican en guiados y no guiados. La diferencia entre éstos radica en que los medios guiados o terrestres requieren de un canal físico, como un cable y en los medios no guiados o aéreos no se requiere de medios físicos, como el aire.

1.2.1 Medios guiados o terrestres

Las ondas circulan a través de un medio sólido, como un cable, como ejemplos se encuentran: cable coaxial, par trenzado y fibra óptica.

El tipo de medio es el que determina la capacidad del canal o también si el enlace es punto a punto (entre 2 sistemas) o multipunto (más de dos sistemas).

La IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos), asignó identificadores a los diferentes medios que puede utilizar Ethernet, cuya forma general es X base Y, donde:

- a) X: es la rapidez de transmisión.
- b) Base: se refiere a la transmisión por banda base. Este método utiliza todo el ancho de banda, por tanto sólo puede transmitir una señal simultáneamente.
- c) Y: proporciona la información sobre el medio físico utilizado en la transmisión.

Un ejemplo se ilustra en la figura 1.1 a continuación:

10: velocidad de transmisión por segundo.

T: utiliza como medio el par trenzado.

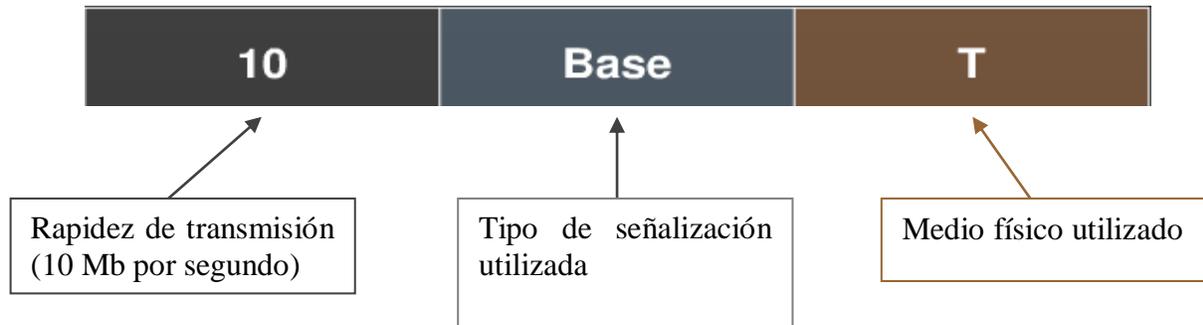


Figura 1.1 Notación de los identificadores de transmisión.

Los tipos de medios de transmisión son los siguientes:

a) *Cable coaxial*

Un cable coaxial consiste en un alambre de cobre rígido como núcleo rodeado por un material aislante. El aislante está forrado por un conductor cilíndrico que con frecuencia es una malla de tejido fuertemente trenzado. El conductor externo se cubre con una envoltura protectora de plástico. La velocidad de transmisión que se puede alcanzar con el cable coaxial llega solo hasta 10Mbps dependiendo de la longitud del cable, si utilizamos un cable delgado se puede transmitir más rápido, en cambio con un cable más grueso la transmisión es más lenta.

El cable coaxial no es habitualmente afectado por interferencias externas y es capaz de lograr altas velocidades de transmisión en largas distancias. Por esa razón se utiliza en televisión y sistemas de telefonía, así como en redes de área local. (Figura 1.2)

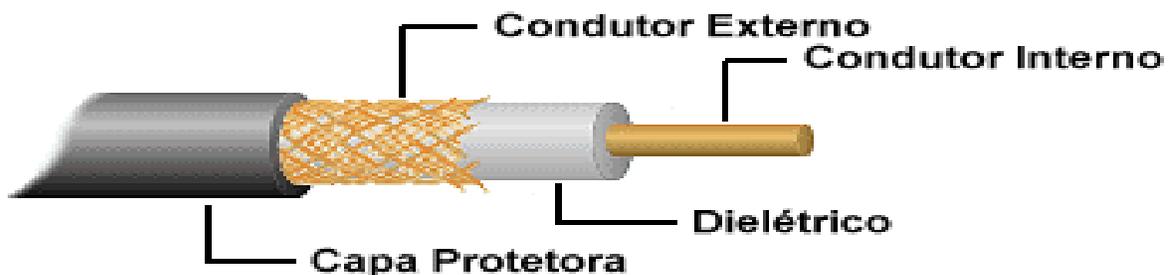


Figura 1.2 Componentes Físicos de un cable coaxial.

Solían usarse ampliamente en sistemas telefónicos, pero ahora se les ha reemplazado en gran medida por fibra óptica en rutas de largo recorrido. (Tenenbaum, 1997, p. 84).

Dentro de la variedad de cables coaxiales existen dos que son los más utilizados para redes Ethernet 802.3, el cable grueso (thicknet) se caracteriza por tener un diámetro de 12 milímetros, en cambio el delgado (thinnet), tiene un diámetro de 6 milímetros. Las características de ambos se muestran en la tabla 1.1.

Tabla 1.1 Características del cable coaxial para Ethernet.

Cable	10 Base 5	10 Base 2
Medio	Coaxial Grueso	Coaxial delgado
Longitud máxima de segmento	500 metros	200 metros
Topología	Bus	Bus

b) Par trenzado

Es el medio de transmisión más común, lo que se debe al costo, flexibilidad y facilidad de instalación, así como las mejoras introducidas en enlaces de mayor velocidad y longitud. Consiste en dos alambres de cobre aislados por un grosor de un milímetro aproximadamente. Los alambres se trenzan con el fin de reducir la interferencia. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados de 2 y 4 pares para redes LAN y utilizan conectores RJ45.

La longitud de trenzado oscila entre 5 y 15 centímetros. Cuanto menor sea la longitud, mayor será la calidad del cable. (Ver figura 1.3)

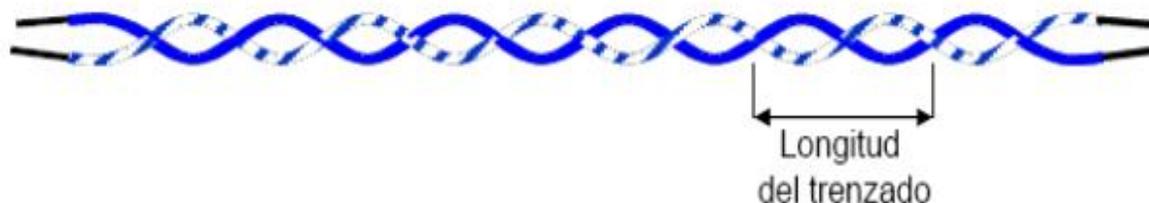


Figura 1.3 Longitud del trenzado.

Existen dos tipos de cables: con blindaje (STP, Shielded Twisted Pair – Par Trenzado Blindado) y sin blindaje (UTP, Unshielded Twisted Pair - Par Trenzado Sin Blindaje) y cada uno posee unas ventajas y algunos inconvenientes, lo que quiere decir que ninguno de estos tipos de cables es mejor que otro.

- **UTP:** Se trata de cables de pares trenzados y no dispone de protección contra las perturbaciones externas por lo que sólo es adecuado para entornos relativamente libres de perturbaciones. Son de bajo costo y de fácil uso, sin embargo, presentan algunos problemas para trabajar a grandes distancias. El cable UTP se divide en categorías de acuerdo con su uso y calidad. (Figura 1.4)
- **STP:** Se trata de cables de cobre aislados dentro de una cubierta protectora metálica. Reduce el ruido eléctrico y brinda una mayor protección ante toda clase de interferencias. Se utiliza en redes de ordenadores como Ethernet o Token Ring. Es más caro que UTP. (Figura 1.5)

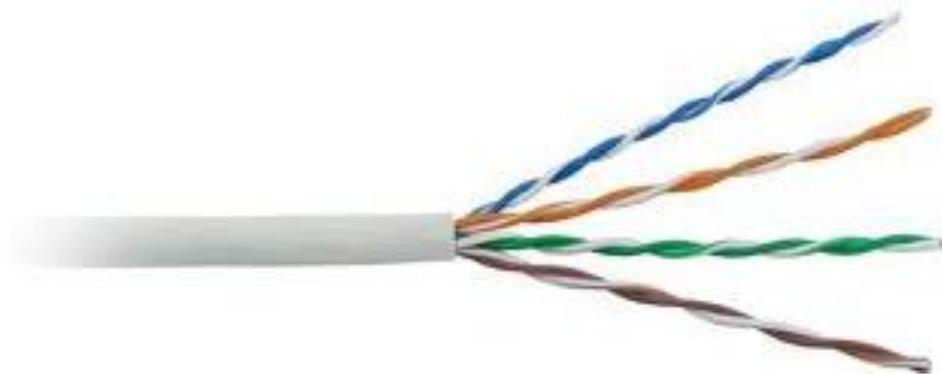


Figura 1.4 Par trenzado UTP.

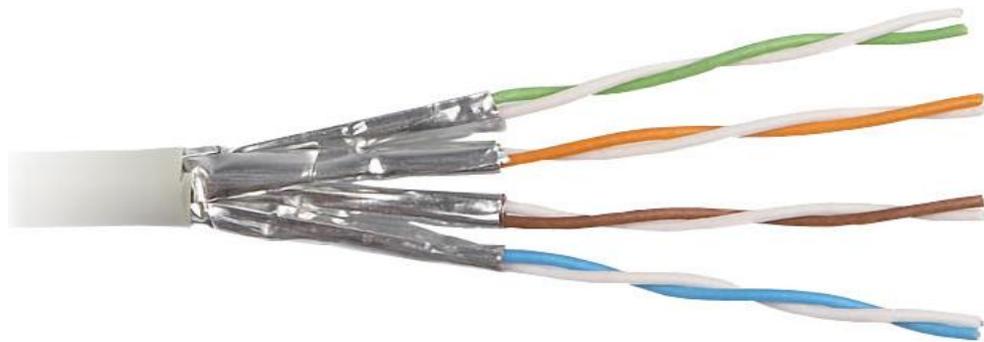


Figura 1.5 Par trenzado STP.

A continuación se muestran en la tabla 1.2 las categorías de cable UTP y sus respectivas características.

Tabla 1.2 Características de las distintas categorías de UTP

TIPO	CARACTERÍSTICAS
Categoría 1	Alcanza como máximo una velocidad de 100 Kbps. Se utiliza en redes telefónicas.
Categoría 2	Este cable consta de 4 pares trenzados de hilo de cobre. Las características de transmisión del medio están especificadas hasta una frecuencia de 4 MHz.
Categoría 3	Velocidad de transmisión de 10 Mbps para Ethernet. Se implementan las redes Ethernet 10BaseT y trabaja a una frecuencia superior de 16 MHz.
Categoría 4	Velocidad de transmisión de 20 Mbps. Usada para redes Token Ring.
Categoría 5	Transmite datos hasta 100Mbps a una frecuencia superior de 100 MHz. Es empleado para redes LAN.
Categoría 5e	Es la categoría 5 mejorada. Minimiza la atenuación y las interferencias. Es la más utilizada actualmente.
Categoría 6	Transmite datos hasta 1Gbps a una frecuencia superior a 250 MHz.

c) Fibra óptica

Una fibra óptica consta de un hilo de vidrio de aproximadamente 0.1 milímetro de grosor el cual es denominado núcleo, tiene un revestimiento exterior de PVC y un conjunto de material que rodean la fibra óptica y su revestimiento. El revestimiento rodea la fibra, ya sea de plástico o de vidrio y está diseñado para prevenir la pérdida de luz de la fibra. (Figura 1.6)

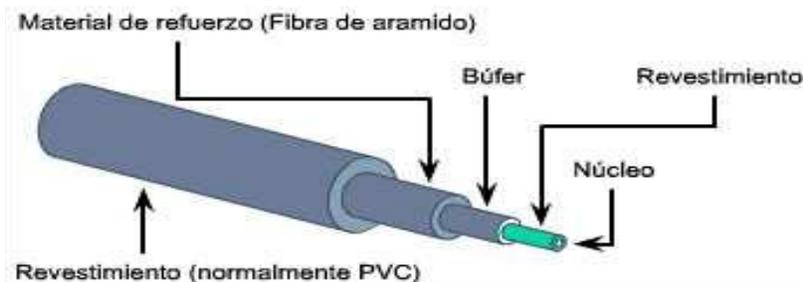


Figura 1.6 Componentes físicos de la fibra óptica¹.

¹ Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 1: Aspectos básicos de networking*, p. 281. México: Pearson Prentice Hall.

La fibra óptica transporta señales en forma de pulsos de luz. Como no transporta impulsos eléctricos, la señal no puede ser intervenida y sus datos no pueden ser robados. Los cables de fibra óptica son adecuados para transmisiones de datos de gran velocidad y capacidad ya que la señal se transmite muy rápidamente y con muy poca interferencia. (Ver tabla 1.3).

Tabla 1.3 Características de los identificadores de la fibra óptica.

IDENTIFICADOR	CARACTERÍSTICAS
10 BASE F	Velocidad de transmisión: 10 Mbps
10 BASE FL	Velocidad de transmisión: 10 Mbps Interconectan nodos con un límite de 2 kilómetros.
100 BASE FX	Velocidad de transmisión: 100 Mbps Interconecta nodos con un límite de 2 kilómetros

Uno de los inconvenientes que presenta la fibra óptica es que se rompe fácilmente si la instalación no se hace adecuadamente ya que es más difícil de cortar que otros cables y requiere equipo especial para cortarlo.

Muchos cables de fibra óptica contienen una fibra de vidrio delgada. Esta característica genera problemas ya que la fibra puede romperse al enroscarla o doblarla fuertemente².

Los cables de fibra óptica pueden clasificarse en dos tipos: monomodo y multimodo.

- **Fibra óptica monomodo**

Transporta un solo rayo de luz, generalmente emitido desde un láser. Puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

- **Fibra óptica multimodo**

Generalmente utiliza emisores LED, su luz ingresa a la fibra multimodo en diferentes ángulos, es decir, emite varios rayos de luz. A diferencia de la fibra monomodo, ésta se usa para transmitir en distancias más cortas. (Figura 1.7)

²Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 1: Aspectos básicos de networking*, p. 348. México: Pearson Prentice Hall.

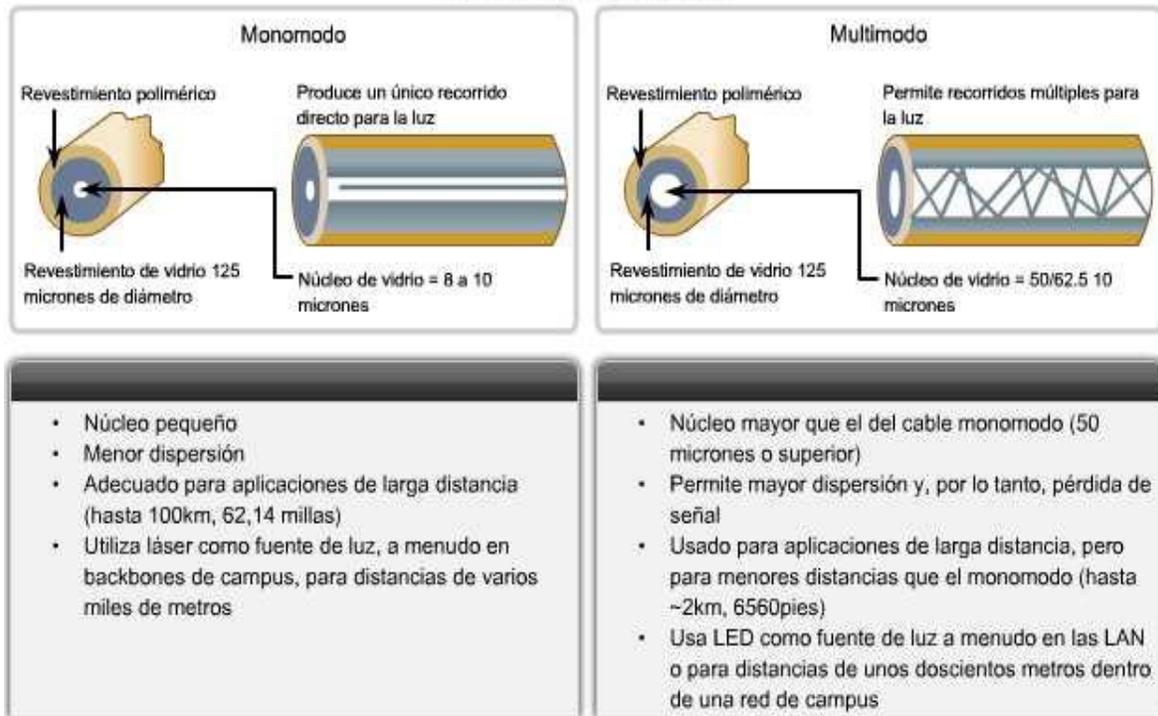


Figura 1.7 Modos de medios de fibra óptica.³

1.2.2 Medios no guiados o aéreos

La señal no circula por ningún medio físico y las transmisiones propias son inalámbricas, la capacidad del canal viene determinada por las antenas.

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

a) Microondas

Las microondas permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 1 y 10 GHz. Transmiten a velocidades del orden de 10 Mbps.

Su principal inconveniente es que requieren de licencia para su uso, además de que no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando se desean realizar comunicaciones a distancias muy largas.

³ Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 1: Aspectos básicos de networking*, p. 282. México: Pearson Prentice Hall.

Por lo tanto se debe poner especial atención en colocar las antenas en un área despejada sin obstáculos de edificios, árboles u otras cosas que pudieran entorpecer una buena recepción en el edificio o la casa del receptor.

b) Infrarrojos

Utiliza un haz de luz infrarroja que transporta los datos entre dispositivos. Debe existir visibilidad directa entre los dispositivos que transmiten y los que reciben ya que de lo contrario se puede ver interrumpida la comunicación, por tal motivo se usan generalmente para la comunicación a corto alcance. (Figura 1.8)

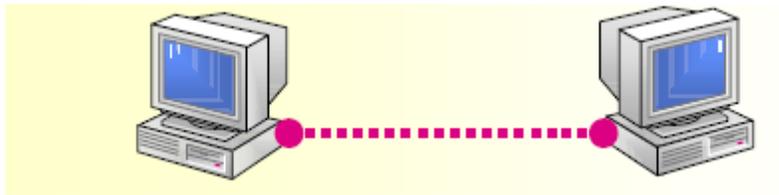


Figura 1.8 Transmisión por medio de infrarrojos.

Existen 3 modos de transmisión:

1. Punto a punto: las estaciones deben verse directamente para poder dirigir el haz de luz directamente de un extremo al otro.
2. Casi-difuso: la emisión es radial; es decir, la emisión se produce en todas direcciones.
3. Difuso: debe ser capaz de abarcar mediante múltiples reflexiones todo el lugar en el cual se encuentran las estaciones.

c) Rayo láser

La palabra láser significa amplificación de la luz por emisión estimulada de radiación. El rayo láser es un rayo de luz de una sola amplitud de onda que ya sea visible o no, tiene un único color.

La tecnología láser se utiliza para conectar redes en áreas metropolitanas densamente pobladas ya que permite conectarlas si se encuentran separadas desde unos pocos metros hasta 4 o 5 kilómetros, alcanzando velocidades de hasta 1500 Mbps.

Es necesario que los equipos cuenten con una línea de visión directa entre ellos, es decir, no puede haber otros edificios, árboles u otras estructuras que bloqueen la línea de visión entre ellos.

d) Ondas de radio

Las ondas de radio son un tipo de radiación electromagnética. Se usan para lograr la comunicación a grandes distancias, son capaces de atravesar paredes de edificios y son omnidireccionales, es decir, viajan en todas las direcciones, por lo que emisor y receptor no necesitan estar alineados como en el caso del infrarrojo. Una de sus desventajas es que están sujetas a interferencias por equipos eléctricos.

Sus propiedades dependen de la frecuencia, a baja frecuencia cruzan perfectamente los obstáculos, en cambio, a altas frecuencias tienden a viajar en línea recta y rebotan en los obstáculos.

Su alcance depende de los siguientes aspectos:

- Potencia de emisión.
- Sensibilidad del receptor.
- Condiciones atmosféricas.
- Relieve del terreno.

e) Enlace satelital

Trasmite microondas por satélite, se utiliza entre dos o más receptores. El satélite funciona básicamente de la siguiente forma:⁴ (ver figura 1.9).

1. Recibe la señal de una banda de frecuencia llamada canal ascendente.
2. La amplifica o repite.
3. La retransmite en otra banda de frecuencia llamada canal descendente.

Entre las ventajas del enlace satelital destacan:

- Transmisiones a grandes velocidades y anchos de banda más grandes.
- Comunicaciones móviles.
- Amplias coberturas.
- Comunicaciones en lugares con terrenos escabrosos.

⁴ Black, U. (1997). *Redes de computadores. Protocolos, normas e interfaces*, p. 138. (2ª ed.) México: Alfaomega.

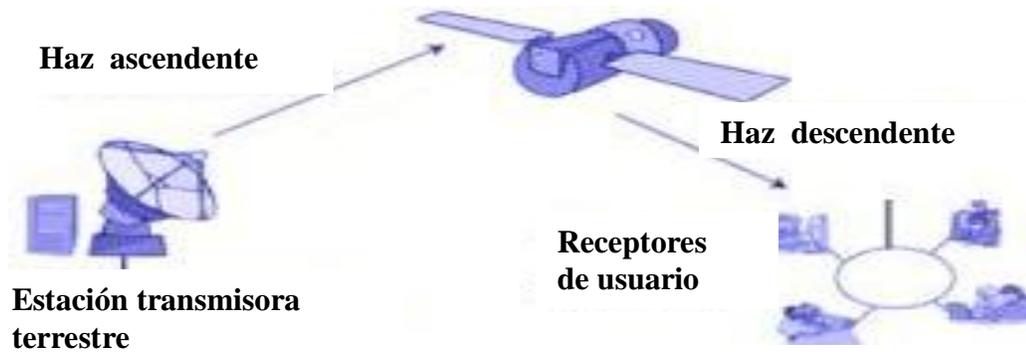


Figura 1.9 Funcionamiento del enlace satelital.

1.3 Topologías de red

Una topología de red es la estructura de equipos, cables y demás componentes en una red. Es un mapa de la red física. El tipo de topología utilizada afecta al tipo y capacidades del hardware de red, su administración y las posibilidades de expansión futura.

La topología es tanto física como lógica:

- La **topología física** describe cómo están conectados los componentes físicos de una red, es la conexión física de circuitos.
- La **topología lógica** describe el modo en que los datos de la red fluyen a través de componentes físicos, la proporciona el software y es una conexión lógica.

Existen cinco topologías básicas:

1. Bus. Los equipos están conectados a un cable común compartido.
2. Estrella. Los equipos están conectados a segmentos de cable que se extienden desde una ubicación central, o concentrador.
3. Anillo. Conecta los equipos con un sólo cable en forma de círculo. La señal pasa a lo largo del anillo, de dispositivo a dispositivo, hasta que alcanza su destino.
4. Malla. Los equipos de la red están conectados entre sí mediante un cable.
5. Híbrida. Dos o más topologías utilizadas juntas.

1.3.1 Topología de bus

En una topología de bus todos los equipos de una red están unidos a un cable contiguo, o segmento que los conecta en línea recta. En esta topología en línea recta el paquete se transmite a todos los adaptadores de red en ese segmento. (Ver figura 1.10)

- Es frecuente en las redes de área local.
- Los dos extremos del cable deben tener terminaciones.
- Todos los adaptadores de red reciben el paquete de datos.

Debido a la forma de transmisión de las señales eléctricas a través de este cable, sus extremos deben estar terminados por dispositivos de hardware denominados terminadores que actúan como límites de la señal y definen el segmento.

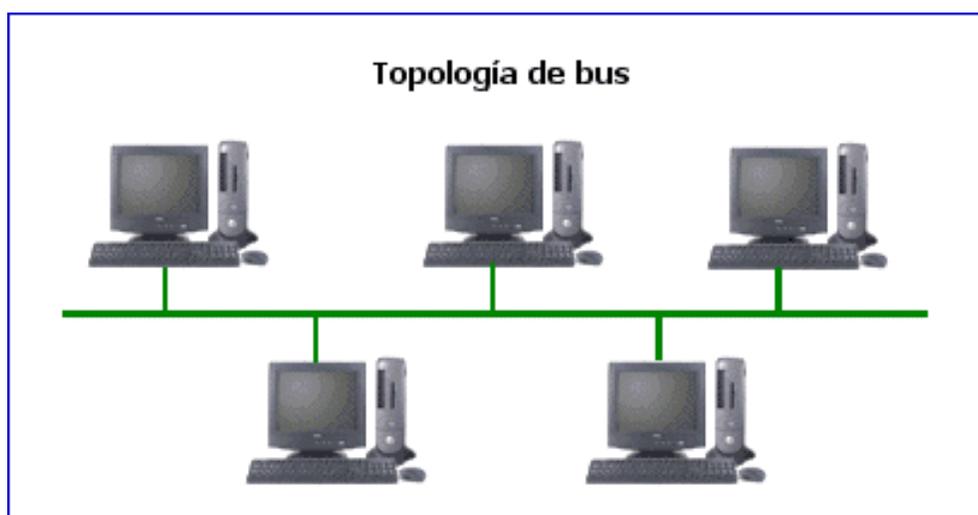


Figura 1.10 Topología de bus.

Ventajas:

1. Esta topología es simple y fácil de instalar.
2. Es relativamente más económica ya que requiere menos cableado a diferencia de las otras topologías⁵.
3. Es especialmente cómoda para una red pequeña y temporal.
4. Es fácil conectar nuevos nodos a la red.

⁵ Una red de topología bus usualmente usa cable coaxial grueso o fino, el Ethernet 10 Base 2 y el 10 Base5.

Desventajas:

1. Suele existir un sólo canal de comunicaciones para todos los dispositivos de la red. En consecuencia si el canal de comunicaciones falla, toda la red deja de funcionar⁶.
2. El número de equipos presentes en un bus también afecta el rendimiento de la red. Cuantos más equipos haya en el bus, mayor será el número de equipos esperando para insertar datos en el bus, y en consecuencia, la red irá más lenta.
3. Debido al modo en que los equipos se comunican en una topología de bus, puede producirse mucho ruido⁷. Un incremento del número de equipos produce un aumento del ruido y la correspondiente reducción de la eficacia de la red.
4. Es conocida como una topología pasiva porque las computadoras no regeneran la señal. Esto hace la red vulnerable a la atenuación ya que pierde señal a través de la distancia del cable. Aunque se pueden utilizar repetidores para arreglar ese problema.

1.3.2 Topología en estrella

En una topología en estrella, los segmentos de cable de cada equipo en la red están conectados a un componente centralizado o concentrador (en inglés hub)⁸. Un concentrador es un dispositivo que conecta varios equipos juntos. En una topología en estrella, las señales se transmiten desde el equipo, a través del concentrador, a todos los equipos de la red. A mayor escala, múltiples LANs (Local Area Networks o Redes de Área local) pueden estar conectadas entre sí en una topología en estrella (ver figura 1.11).

⁶ Algunos fabricantes proporcionan canales completamente redundantes por si falla el canal principal, y otros ofrecen conmutadores que permiten rodear un nodo en caso de que falle.

⁷ Ruido es el tráfico generado en la red cuando los equipos intentan comunicarse entre sí simultáneamente.

⁸ El hub puede ser activo, pasivo o inteligente. Un hub pasivo es sólo un punto de conexión y no requiere energía eléctrica. Un hub activo es actualmente un repetidor con múltiples puertos; impulsa la señal antes de pasarla a la siguiente computadora. Un Hub Inteligente es un hub activo pero con capacidad de diagnóstico, puede detectar errores y corregirlos.



Figura 1.11 Topología en estrella.

- La topología en estrella es la más empleada en los sistemas de comunicación de datos.
- La topología estrella es similar a la de bus, todas las computadoras reciben el mensaje pero sólo la computadora con la dirección igual a la dirección del mensaje puede leerlo.
- El nodo central es el responsable de encaminar el tráfico hacia el resto de los componentes; se encarga además de localizar las averías.

Ventajas:

1. Es más tolerante, esto quiere decir que si una computadora se desconecta o si se le rompe el cable sólo esa computadora es afectada y el resto de la red mantiene su comunicación normalmente.
2. Es fácil de reconfigurar; añadir o remover una computadora es tan simple como conectar o desconectar el cable.

Desventajas:

1. Es costosa ya que requiere más cable que otras topologías.
2. Cada cable se conecta por separado en el hub hacia cada una de las computadoras.
3. Si el hub se cae, la red no tiene comunicación.
4. Si una computadora se cae, no puede enviar ni recibir mensajes.
5. En una topología en estrella el ruido se crea en la red.

1.3.3 Topología en anillo

Los equipos están conectados con un cable de forma circular. A diferencia de la topología de bus, no hay extremos con terminaciones. Las señales viajan alrededor del bucle en una dirección y pasan a través de cada equipo que actúa como repetidor para amplificar la señal y enviarla al siguiente equipo⁹. (Ver figura 1.12).

- La topología en anillo se llama así por el aspecto circular del flujo de datos.
- Todos los componentes del anillo están unidos por un mismo canal.
- En una topología en anillo cada equipo actúa como repetidor, regenerando la señal y enviándola al siguiente equipo. De esta forma, se conserva la fuerza de la señal.



Figura 1.12 Topología en anillo.

Ventajas:

1. La organización en anillo resulta atractiva porque con ella son bastante raros los embotellamientos¹⁰.
2. Mínimo costo de instalación, pues para crearla basta con que los equipos cuenten con tarjetas de red y que exista un cable coaxial que una un punto con otro.
3. Utilizan menos cable que la topología estrella.

⁹ A mayor escala, en una topología en anillo múltiples LANs pueden conectarse entre sí utilizando el cable coaxial ThickNet o el cable de fibra óptica.

¹⁰ En el ámbito de las redes de datos, un embotellamiento se entiende como el fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede cursar.

Desventajas:

1. Si falla el canal entre dos nodos, toda la red se interrumpe¹¹.
2. Una ruptura de cable o fallo de un nodo afecta a toda la red.
3. La topología de anillo utiliza más cable que la de bus.
4. En algunos tipos de topologías de anillo es necesario bajar todo el sistema para agregar nodos.
5. Posee una mayor lentitud en la transmisión de la señal debido a que la información es repartida por todo el anillo.

1.3.4 Topología de malla

Cada equipo está conectado a cada uno del resto de los equipos por un cable distinto. Esta configuración proporciona rutas redundantes a través de la red de forma que si un cable falta, otro transporta el tráfico y la red sigue funcionando¹².

Las redes en malla son aquellas en las cuales todos los nodos están conectados de forma que no existe una preeminencia de un nodo sobre otros, en cuanto a la concentración del tráfico de comunicaciones. (Ver figura 1.13)

Gracias a los múltiples caminos que ofrece a través de los distintos dispositivos, es posible orientar el tráfico por trayectorias alternativas en caso de que algún nodo esté averiado u ocupado, a pesar de que la realización de este método es compleja y cara (para proporcionar estas funciones especiales, la lógica de control de los protocolos de una red en malla puede llegar a ser sumamente complicada), muchos usuarios prefieren la fiabilidad de una red en malla a otras alternativas.

¹¹ Por eso algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se produce la pérdida de algún canal; otros fabricantes construyen conmutadores que dirigen los datos automáticamente, saltándose el nodo averiado, hasta el siguiente nodo del anillo, con el fin de evitar que el fallo afecte a toda la red.

¹² A mayor escala, múltiples LANs (Local Area Network - Red de Área Local) pueden estar en estrella conectadas entre sí en una topología de malla utilizando red telefónica conmutada, un cable coaxial ThickNet o el cable de fibra óptica.

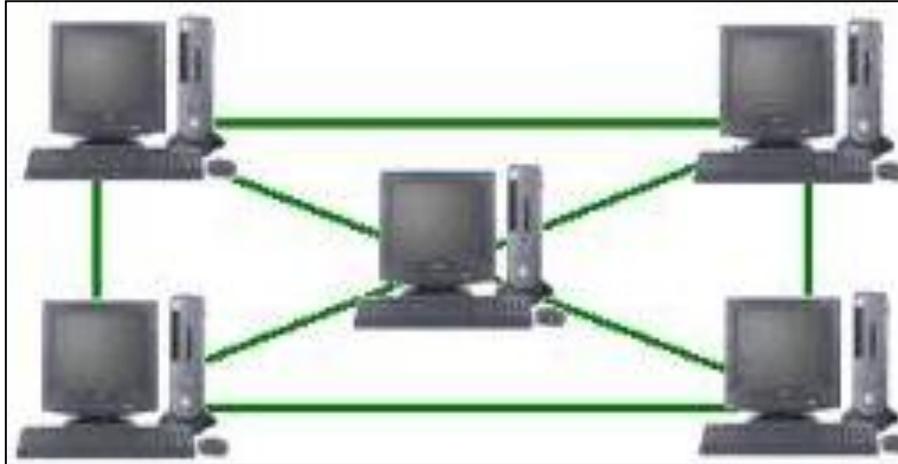


Figura 1.13 Topología en malla.

Ventajas:

1. El uso de los enlaces dedicados¹³ garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos.
2. Una topología en malla es robusta. Si un enlace falla, no inhabilita todo el sistema.
3. Privacidad y seguridad. Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes.
4. Una de las ventajas de las topologías de malla es su capacidad de respaldo al proporcionar múltiples rutas a través de la red.

Desventajas:

1. Debido a que las rutas redundantes requieren más cable del que se necesita en otras topologías.
2. Requiere $n-1$ puertos de comunicación.
3. El mantenimiento resulta costoso a largo plazo.

¹³ El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.

1.3.5 Topología de árbol

Una topología de árbol o topología jerárquica es aquella que combina características de la topología estrella con la de bus, se podría decir que es una combinación de ambas. (Figura 1.14)

Esta topología trabaja de la misma manera que la de bus y estrella por el modo de actuar del nodo ya que el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, sólo que en esta topología las ramificaciones se extienden a partir de un punto raíz como la de estrella, a tantas ramificaciones como sean posibles, según las características del árbol. Una similitud con la de **estrella** es que los **nodos del árbol** están conectados a un concentrador central o hub que controla el tráfico de la red, pero no todos los nodos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al **concentrador central**.

Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.



Figura 1.14 Topología de árbol o jerárquica

Ventajas:

1. Cableado punto a punto para segmentos individuales.
2. Soportado por multitud de vendedores de software y de hardware.
3. Da lugar a la creación de nuevas redes y/o subredes tanto internas como externas, lo que facilita el crecimiento de la red.

Desventajas:

1. La medida de cada segmento viene determinada por el tipo de cable utilizado.
2. Si se viene abajo el segmento principal, todo el segmento se viene abajo con él.
3. Es más difícil su configuración.
4. Las redes de computadoras se montan con una serie de componentes de uso común y que en mayor o menor medida aparece siempre en cualquier instalación.

1.4 Clasificación de las redes por su tamaño.**1.4.1 PAN**

Red de área personal (Personal Area Network). Interconexión de dispositivos en el entorno del usuario, con alcance de escasos metros. (Figura 1.15)

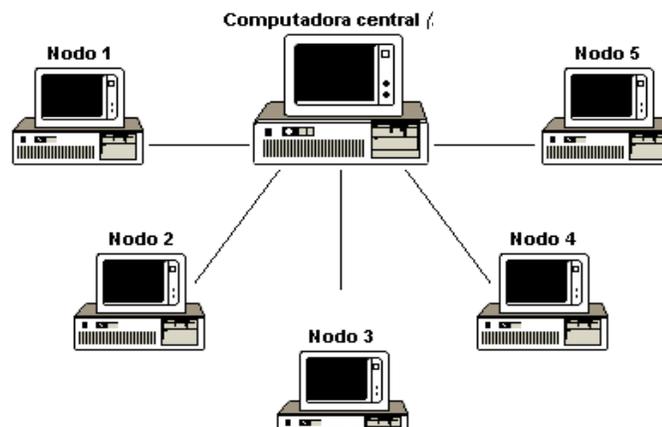


Figura 1.15 Red de área personal.

1.4.2 Redes LAN

Las redes de área local (Local Area Network) son redes de computadoras cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas que generalmente usan la tecnología de broadcast¹⁴. Como su tamaño es restringido, el peor tiempo de transmisión de datos es conocido, siendo velocidades de transmisión típicas de LAN las que van de 10 a 100 Mbps. (Figura 1.16)

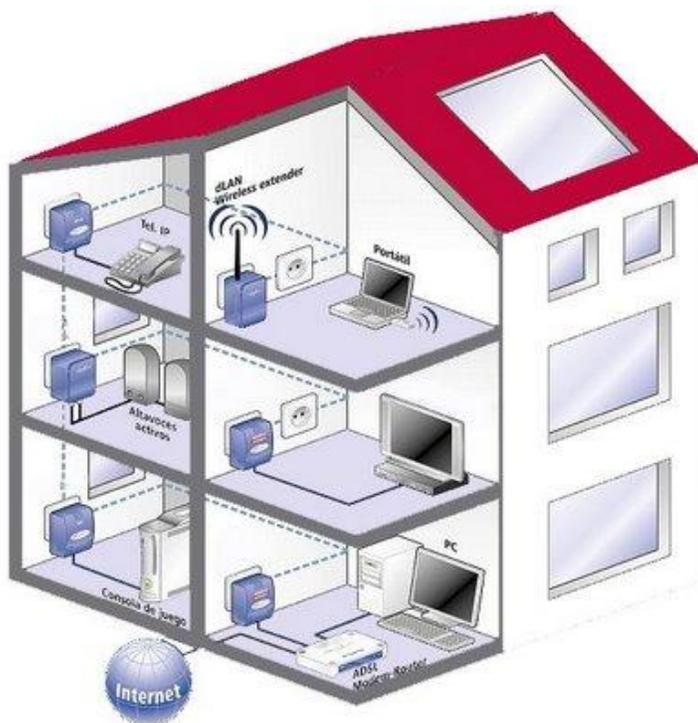


Figura 1.16 Red de área local.

Al extender la definición de una LAN con los servicios que proporciona, se pueden definir dos modos operativos diferentes:

- En una red "de igual a igual", la comunicación se lleva a cabo de un equipo a otro sin un equipo central y cada equipo tiene la misma función.
- En un entorno "cliente/servidor", un equipo central brinda servicios de red para los usuarios.

¹⁴ Tecnología de broadcast: aquella en la que a un solo cable se conectan todas las máquinas.

1.4.3 Redes MAN

Las redes de área metropolitana (Metropolitan Area Network) son redes de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Son típicas de empresas y organizaciones que poseen distintas oficinas repartidas en una misma área metropolitana, por lo que, en su tamaño máximo, comprenden un área de unos 10 kilómetros.

Conecta diversas LAN cercanas geográficamente (en un área de alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. (Ver figura 1.17)

Una MAN está compuesta por conmutadores o routers conectados entre sí mediante conexiones de alta velocidad (generalmente cables de fibra óptica) y presenta las siguientes características:

- Puede ser pública o privada.
- Una MAN puede soportar tanto voz como datos.
- Tiene uno o dos cables y no tiene elementos de intercambio de paquetes o conmutadores, lo cual simplifica bastante el diseño.
- Para las MANs se ha adoptado un estándar llamado DQDB (Distributed Queue Dual Bus- Bus Dual de Cola Distribuida) o IEEE 802.6. Utiliza medios de difusión al igual que las LANs.

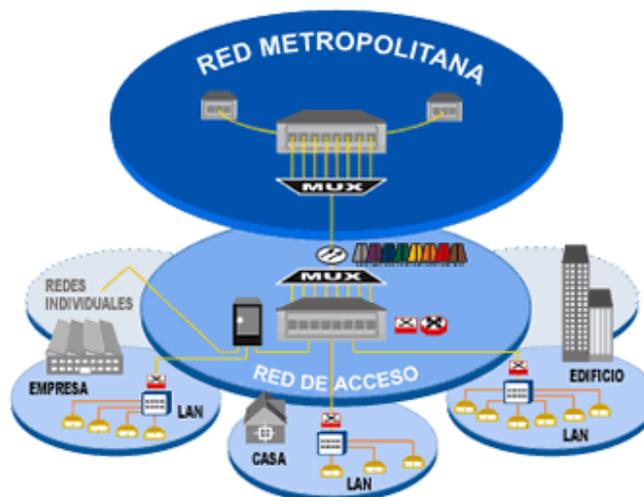


Figura 1.17 Red de área metropolitana.

1.4.4 Redes WAN

Las redes de área amplia (Wide Area Network) tienen un tamaño superior a una MAN, y consisten en una colección de hosts o de redes LAN conectadas por una subred. Esta subred está formada por una serie de líneas de transmisión interconectadas por medio de routers, aparatos de red encargados de encaminar o dirigir los paquetes hacia la LAN o host adecuado, enviándose éstos de un router a otro. Su tamaño puede oscilar entre 100 y 1000 kilómetros. (Figura 1.18)

- Conecta múltiples LAN entre sí a través de grandes distancias geográficas.
- La velocidad disponible en una WAN varía según el costo de las conexiones (que aumenta con la distancia) y puede ser baja.
- Las WAN funcionan con routers, que pueden "elegir" la ruta más apropiada para que los datos lleguen a un nodo de la red.
- La WAN más conocida es Internet.

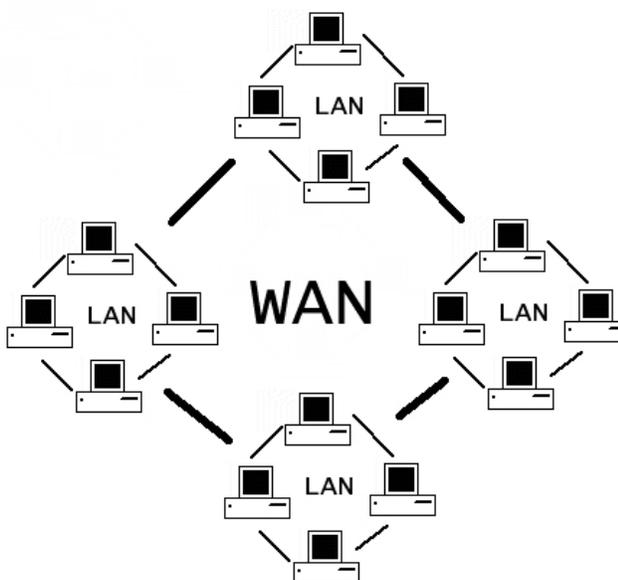


Figura 1.18 Red de área amplia.

1.4.5 Redes internet

Una red internet es una red de redes, vinculadas mediante enrutadores gateways. Un gateway o pasarela es un computador especial que puede traducir información entre sistemas con formato de datos diferentes. Su tamaño puede ser desde 10000 kilómetros en adelante y su ejemplo más claro es Internet, la red de redes mundial. (Figura 1.19)



Figura 1.19 Internet

CAPÍTULO 2

Planeación



“El orden y la simplificación son los primeros pasos hacia el dominio de un tema, el enemigo real es lo desconocido”

Thomas Mann.

2.1 Objetivos del diseño en las redes

El diseño de una red informática es determinar la estructura física y lógica de la red. Un buen diseño de la red informática es fundamental para evitar problemas de pérdidas de datos, caídas continuas de la red, problemas de lentitud en el procesamiento de la información y problemas de seguridad informática.

Si bien la implementación se lleva a cabo del nivel físico hacia arriba (respecto al modelo OSI¹⁵), el diseño se debe hacer del nivel aplicativo hacia abajo. No se diseñan redes para ver qué se puede poner a correr sobre ellas, más bien, su diseño está determinado por los requerimientos de los servicios que se tendrán: correo, voz, emulación de terminal, etcétera.

Cuando se diseña una red o se amplía una configuración existente, es fundamental la realización de un diseño detallado siguiendo una planificación.

Los beneficios del diseño son múltiples. En primer lugar se obtiene una reducción de costos al evitar recursos caros duplicados. Por otro lado, se mejora el rendimiento diario por el fácil acceso a los recursos y datos.

Las redes en general comparten recursos y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una alta fiabilidad al contar con fuentes alternativas de suministro. Por ejemplo, todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias.

Un punto muy relacionado es la capacidad para aumentar el rendimiento del sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores. Con máquinas grandes, cuando el sistema está lleno, deberá reemplazarse con uno más grande, operación que por lo normal genera un gran gasto y una perturbación inclusive mayor al trabajo de los usuarios.

Otro objetivo del establecimiento de una red de ordenadores, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

En el desarrollo de una red deben contemplarse las siguientes características, así como las fases involucradas en dicho desarrollo (ver figura 2.1):

¹⁵ **OSI:** Modelo de interconexión de sistemas abiertos, en inglés Open System Interconnection.

- Multiservicio (convergencia): soporte de datos, audio y video.
- Calidad de servicio: priorización por tipo de aplicación.
- Administración y Monitoreo: soporte de protocolos como SNMP.
- Escalable: la red debe estar preparada para crecer.
- Alta disponibilidad: redundancia en enlaces y componentes como fuentes de poder.
- Buena relación beneficio-costos.

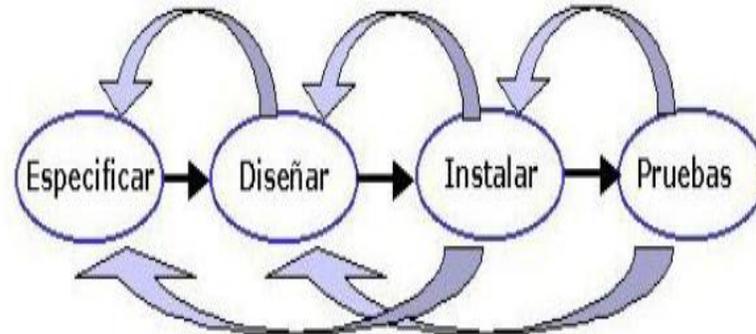


Figura 2.1 Diagrama de 4 pasos en el proceso de construcción e implementación de una red.

A continuación se examinarán las principales metas del diseño de una red, cuáles son las prioridades que se adaptan al desarrollo de la red, entre otras cosas. Un efectivo administrador de la red es también un cuidadoso planeador.

2.1.2 Metas del diseño

El diseñador de la red debe siempre preguntarse algunas cuestiones básicas de la red antes de que empiece la fase del diseño. ¿Quién va a usar la red? ¿Qué tareas van a desempeñar los usuarios en la red? ¿Quién va a administrar la red? Igualmente importante ¿Quién va a pagar por ella? ¿Quién va a pagar para mantenerla? Cuando esas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más productivo. Estas prioridades se convertirán en las metas del diseño. Se examinan a continuación algunas de esas metas clave:

- **Desempeño (performance):** Los tipos de datos procesados pueden determinar el grado de desempeño requerido. Si la función principal de la red son las transacciones en tiempo real, entonces el desempeño asume una muy alta prioridad y desafortunadamente el costo se eleva súbitamente en este trueque desempeño/costo.

- **Volumen proyectado de tráfico:** Algunos equipos de interconexión como los puentes o concentradores pueden ocasionar cuellos de botella en las redes con tráfico pesado. Cuando se está diseñando una red se debe incluir el número proyectado de usuarios, el tipo de trabajo que los usuarios harán, el tipo de aplicaciones que se correrán y el monto de comunicaciones remotas.
- **Expansión futura:** Las redes están siempre en continuo crecimiento. Una meta del diseño deberá ser planear el crecimiento de la red para que las necesidades de la compañía no se saturen en un futuro inmediato. Los nodos deberán ser diseñados para que éstos puedan ser enlazados al mundo exterior. ¿Cuántas estaciones de trabajo puede soportar el sistema operativo de red? ¿La póliza de precios del vendedor de equipos hace factible la expansión futura? ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red? ¿El equipo de comunicaciones tiene puertos disponibles para futuras conexiones?, etcétera.
- **Seguridad:** Muchas preguntas de diseño están relacionadas a la seguridad de la red. ¿Estarán cifrados los datos? ¿Qué nivel de seguridad en las contraseñas es deseable? ¿Qué tipos de sistema de respaldo son requeridos para asegurar que los datos perdidos siempre puedan ser recuperados? Si la red tiene acceso a usuarios remotos, ¿Qué tipo de seguridad será implementada para prevenir que los perpetradores¹⁶ entren a nuestra red?
- **Redundancia:** Las redes robustas requieren redundancia, si algún elemento falla, la red deberá por sí misma seguir operando. Un sistema tolerante a fallas debe estar diseñado en la red de tal manera que, si un servidor falla, un segundo servidor de respaldo entrará a operar inmediatamente. La redundancia también se aplica para los enlaces externos de la red. Los enlaces redundantes aseguran que la red siga funcionando en caso de que un equipo de comunicaciones falle o el medio de transmisión en cuestión.
- **Compatibilidad de hardware y software:** Los sistemas deben ser compatibles para que éstos, dentro de la red, puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar los protocolos, sistemas operativos de red, aplicaciones, etcétera.
- **Compatibilidad en la organización y gente:** Ya una vez que la red está diseñada para ser compatible con el hardware y software existente, sería un gran error si no se

¹⁶**Perpetrador:** Toda aquella persona que lleve a cabo conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

considera la organización y el personal de la compañía. A veces, ocurre que se tienen sistemas de la más alta tecnología y no se tiene el personal adecuado para operarlos. O por el contrario, se tiene personal con amplios conocimientos y experiencia operando sistemas obsoletos. Para tener éxito, la red deberá trabajar dentro del marco de trabajo de las tecnologías y filosofías existentes.

- **Costo:** El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Seguido ocurre que las redes se adaptan al escaso presupuesto y todas las metas anteriores del diseño no se puedan implementar. Los directivos, muchas veces, no tienen idea del alto costo que tiene un equipo de comunicaciones, un sistema operativo para múltiples usuarios y muchas veces no piensan en el mantenimiento. El costo involucrado siempre será un factor importante para el diseño de una red (ver figura 2.2).

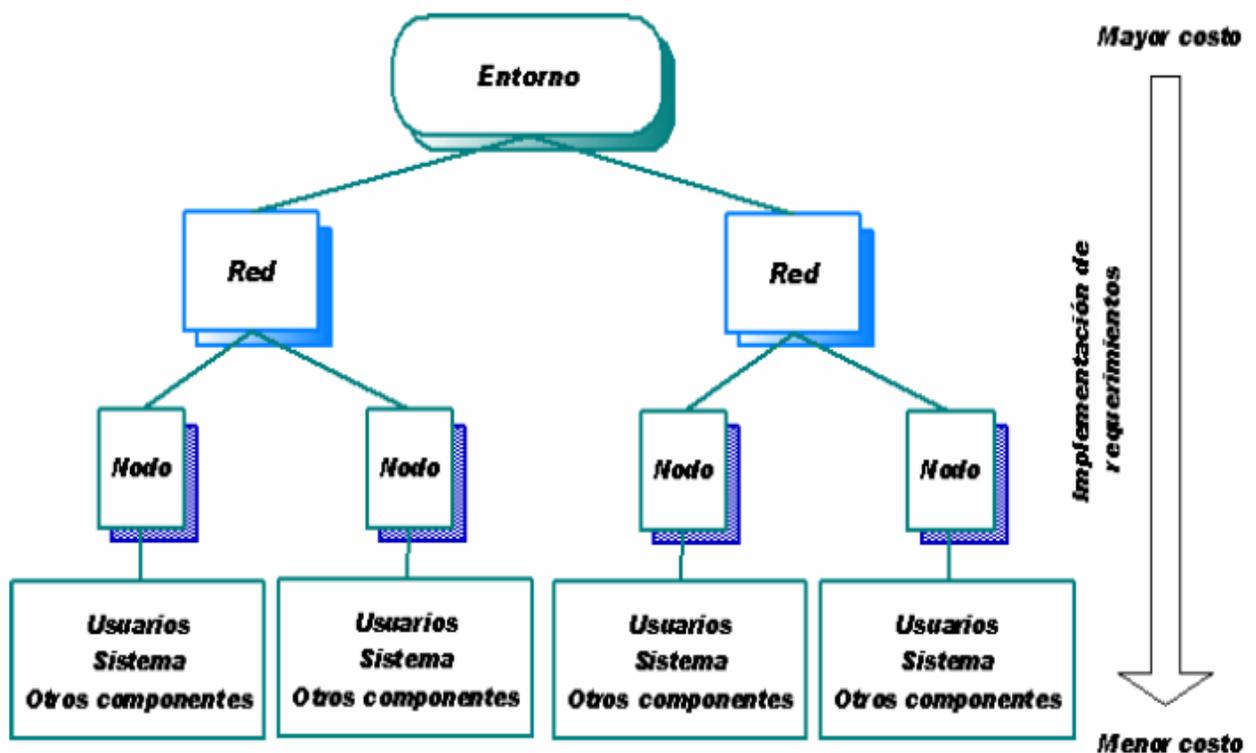


Figura 2.2 Niveles de Jerarquía del sistema¹⁷.

¹⁷ Diagrama realizado por: M.C. Cintia Quezada Reyes, clase Administración de Redes, Facultad de Ingeniería, UNAM.

2.2 Requerimientos de Hardware

Es conveniente analizar la existencia y las necesidades de hardware que se requieren para una red de datos; con ese análisis es posible detectar información sobre los dispositivos, cantidad de memoria RAM, dispositivos sobre-usados¹⁸, y sub-usados¹⁹, qué redes están conectadas a ciertos dispositivos, tipos de enlace de las conexiones, unidad máxima de transparencia, etcétera.

Así también, es preciso percatarse de la estructura actual de la red y darse cuenta si es conveniente o no realizar cambios globales o particulares.

Es conveniente tomar en cuenta los siguientes aspectos para hacer el análisis de requerimientos de hardware para realizar una administración de redes eficiente:

1. Identificación de la red

Identificar la red consiste en conocer y cuantificar cada uno de los elementos que la componen, la topología e identificar posibles puntos de falla.

Existen dos tipos:

- a) **Automática:** se realiza a través de un software lo cual requiere menos tiempo.
- b) **Manual:** se basa en la observación y ésta requiere más tiempo.

2. Análisis del tráfico de la red

Permite identificar los dispositivos dedicados al tráfico, tecnologías empleadas, ubicación de dispositivos en cada segmento y el uso de segmentos con base en el tipo de tráfico.

3. Niveles de confianza

Es el comportamiento que guarda cierto dispositivo o conjunto de dispositivos con relación al estado ideal de éste. Toma en cuenta la funcionalidad y la seguridad.

¹⁸ **Dispositivos sobre-usados:** dispositivos que se siguen usando aún cuando ya finalizó su estimación de vida útil.

¹⁹ **Dispositivos sub-usados:** dispositivos a los que no se les da el funcionamiento adecuado según el rendimiento que éstos tienen.

Existen tres tipos:

- a) **Alto.** Nivel ideal. Se refiere a que el dispositivo funcione sin ningún problema.
- b) **Medio.** El dispositivo funciona medianamente, requiere soporte técnico.
- c) **Bajo.** El dispositivo no funciona como debiera aún con soporte técnico.

4. Capacidades del dispositivo

Se requiere tener conocimiento de las características de los dispositivos que pueden llegar a tener un impacto sobre el rendimiento eficiente de la red, se deben identificar:

- Tecnologías que emplean grandes recursos.
- Servicios que requieren gran ancho de banda.
- Comunicación sofisticada de paquetes.

5. Consideraciones en la elección de dispositivos

Es importante tomar en cuenta los aspectos siguientes para hacer una buena elección de dispositivos:

- Incompatibilidad
- Costos
- Marcas
- Funcionalidad
- Capacidad
- Tiempo de vida
- Protocolos que implementan
- Servicios
- Seguridad
- Mejoramiento
- Adquisición

6. Análisis de requerimientos de usuario

La mayoría de las veces las consideraciones que se hagan para la realización de la construcción de una red va de la mano con los requerimientos del usuario, como son:

- Identificar servicios
- Identificar costos

- Identificar perfil de usuario (sus necesidades)
- Especificar requerimientos en niveles
- Clasificar necesidades en niveles
- Identificar niveles de jerarquía en el sistema

7. Requerimientos

De manera general, los requerimientos (ver figura 2.3) contemplan los siguientes aspectos, que deben contemplarse y llevar a cabo:

- Necesidades del cliente
- Es indispensable la organización
- Comunicación constante
- Identificar las necesidades que satisface el software



Figura 2.3 Clasificación de los requerimientos²⁰.

²⁰ Diagrama realizado por: M.C. Cintia Quezada Reyes, clase Administración de Redes, Facultad de Ingeniería, UNAM.

- **Entrenamiento:** se refiere a la necesidad de capacitar a los usuarios para que puedan operar el equipo de manera adecuada, logrando así el uso eficiente de los recursos de hardware.
- **Disponibilidad:** toda red de datos debe encontrarse disponible y operable en el tiempo que ésta sea requerida por el usuario, cumpliendo siempre con los términos y horarios de uso que la organización establezca.
- **Desempeño:** deben establecerse aspectos tales como la velocidad a la que van a operar los dispositivos y sus diferentes interfaces, esto para darle un uso adecuado al ancho de banda y que no esté desperdiciado. Asimismo las características que cada dispositivos debe tener, como número y tipo de interfaces, mecanismos de seguridad, protocolos soportados, entre otros, ya que esto impacta en el rendimiento y economía de las empresas.
- **Funcionales:** quiere decir, lo que el sistema debe hacer, no lo que pueda hacer, esto de acuerdo con las funciones de las empresas u organizaciones.
- **Interfaz:** ya que será la parte con la que va a interactuar el usuario, ésta debe ser sencilla, intuitiva y amigable para él.
- **Ergonómicos:** se refiere a que los equipos tengan un diseño tal que se consideren las limitaciones físicas de los usuarios, del sistema y del ambiente y al mismo tiempo salvaguardar la seguridad tanto de los equipos como de los usuarios, la salud y el bienestar de estos últimos y así optimizar la eficiencia y el comportamiento de la red.
- **Del entorno:** hay que tener muy en cuenta el entorno donde se encontrarán colocados todos los dispositivos, esto es, ubicarlos en un lugar que cumpla con las especificaciones de humedad y temperatura adecuadas, así como también la ubicación física del lugar y las condiciones climáticas del área geográfica. Por ejemplo, en zonas como Veracruz se incrementa la probabilidad de incidentes debido a los factores ambientales, como el calor y la humedad.
- **Restricción:** para el óptimo funcionamiento de toda red es necesario apearse a un conjunto de leyes y estándares, para que ésta sea operable y eficiente ante cualquier cambio de hardware o bien de software. El uso de estándares también facilita la corrección de errores así como una administración más sencilla de la red.

2.3 Requerimientos de Software

Se deben tomar en cuenta los mismos aspectos que en los requerimientos de hardware, sin embargo, éstos se deben considerar a nivel lógico para llevar a cabo actividades como la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Antes de realizar una instalación, se debe tomar en cuenta lo siguiente:

- Que las cantidades de memoria y almacenamiento sean suficientes para la nueva entidad de software.
- Asegurar que no exista conflicto alguno entre las versiones actuales y las que se pretenden instalar.

Otro requerimiento es satisfacer la necesidad de respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere especial cuidado. Los respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente, lo que se hace es cargar la configuración al dispositivo mediante un servidor.

Así también es importante recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo con el comportamiento encontrado. Para ello se requiere software especializado que realice dichas tareas, además de que algunos de éstos permiten monitorear la red, localizar fallas, prevenir ataques, detectar intrusos, enviar alarmas, corregirlas, hacer reportes de dichos acontecimientos y darles seguimiento.

Toda red, sea cual sea el tamaño de ésta y sus fines particulares, debe cubrir este mínimo de requerimientos para cumplir plenamente con los objetivos de las redes de datos, que se traduce en una transmisión eficiente, segura y confiable.

2.4 Direccionamiento lógico

Se sabe que aplicaciones y servicios de red en un dispositivo pueden comunicarse con aplicaciones y servicios que se ejecutan en otro dispositivo. En la siguiente figura se puede observar cómo se transportan los datos a través de la red: desde el dispositivo origen hasta el destino de manera eficiente. (Figura 2.4)

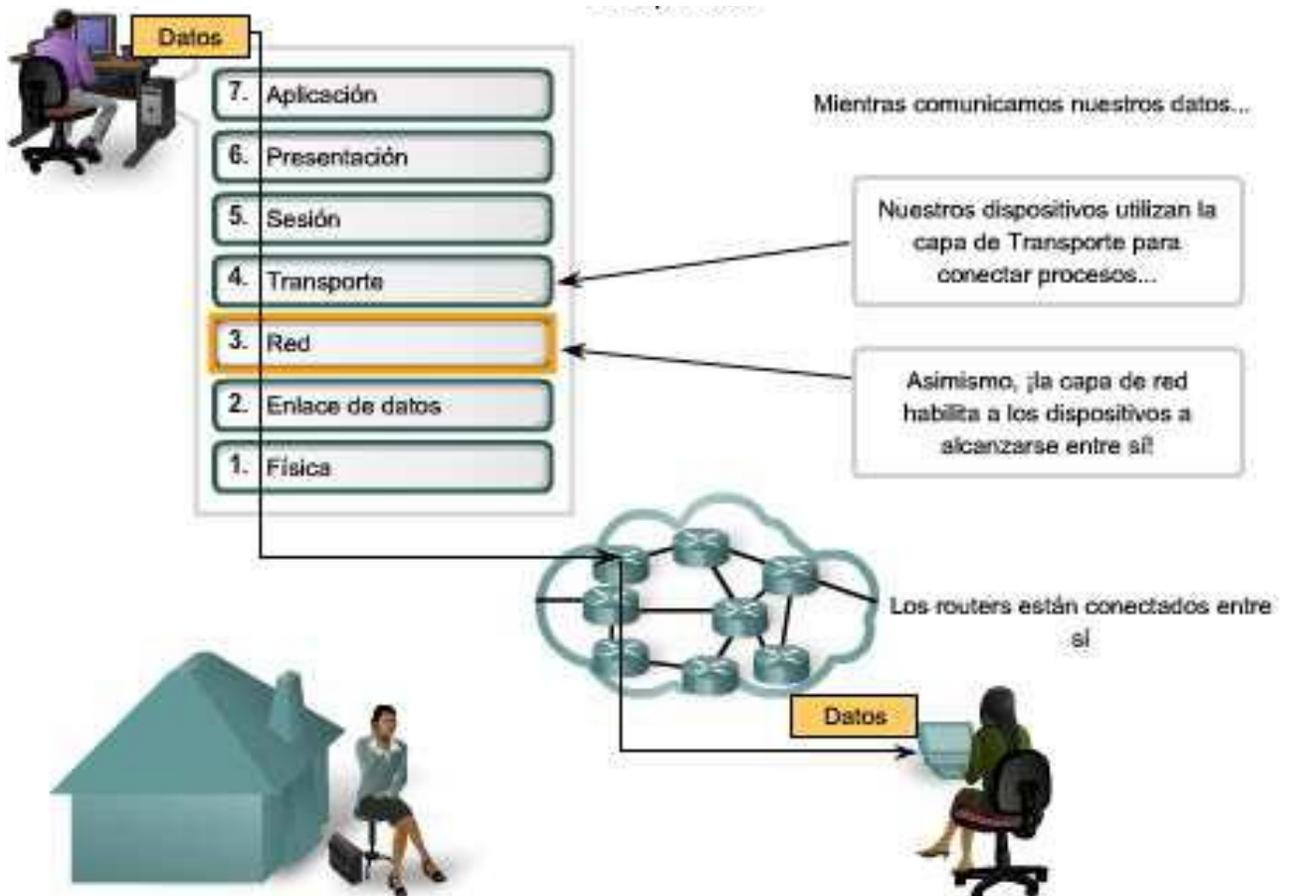


Figura 2.4 Transmisión de datos a través de una red de datos²¹.

Esta comunicación se basa en el modelo de interconexión de sistemas abiertos, también llamado OSI, éste es el modelo de red creado por la Organización Internacional para la Estandarización en 1984. Es un marco de referencia para interconexiones de redes de datos, basándose en siete capas funcionales. (Figura 2.5)

Cada una de ellas desarrolla una función diferente logrando así la comunicación entre distintos dispositivos. La capa de red es quien hace referencia al direccionamiento lógico ya que una de sus funciones principales es proporcionar un mecanismo para direccionar hosts. A medida que crece la cantidad de hosts de la red se requiere más planificación para administrar y direccionar la red.

²¹ Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 1: Aspectos básicos de networking*, p. 125. México: Pearson Prentice Hall.



Figura 2.5 Capas del modelo OSI y función de cada una²².

Por lo regular las redes crecen con el paso del tiempo por lo que pueden volverse demasiado grandes para manejarlas como una única red, por lo que se necesita dividirlos, a esto se le llaman subredes.

Así el direccionamiento lógico permite la comunicación de datos entre hosts de la misma red o en redes diferentes.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 asegura que las redes puedan operar de manera eficaz y eficiente.

Con el protocolo IPv4 cada IP se compone de 32 bits y consta de dos partes; la primera identifica la red y la segunda al host (Figura 2.6). Se encuentra dividida en cuatro octetos, cada uno de ellos se convierte a su valor decimal. A la cantidad de bits de una dirección que se utiliza como porción de red se le denomina prefijo o máscara de subred, también está formada por 32 bits de unos y ceros, los unos indican qué porción de red se está utilizando y los ceros se utilizan para saber cuáles son los bits de host. (Figura 2.7)

²² Bertolini, M. (Diciembre, 2007). *La pila OSI*. Extraído el día 16 de abril desde <http://commons.wikimedia.org/wiki/File:Pila-osi-es.svg?uselang=es>.

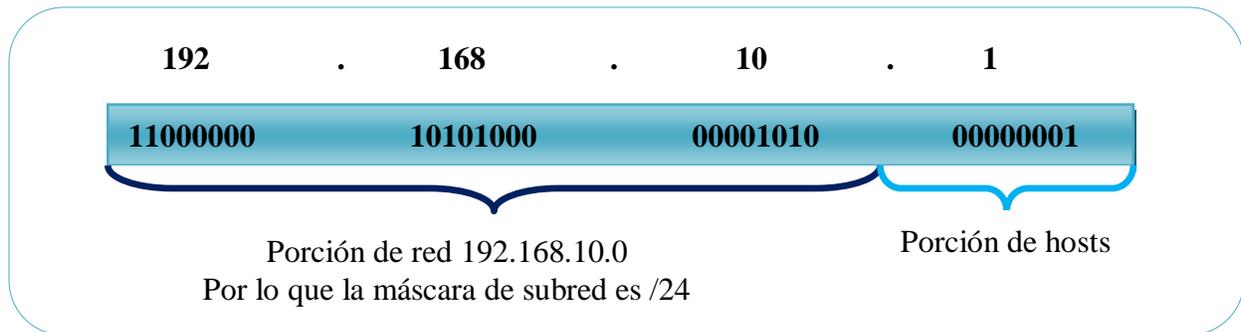


Figura 2.6 Notación de direcciones IP.

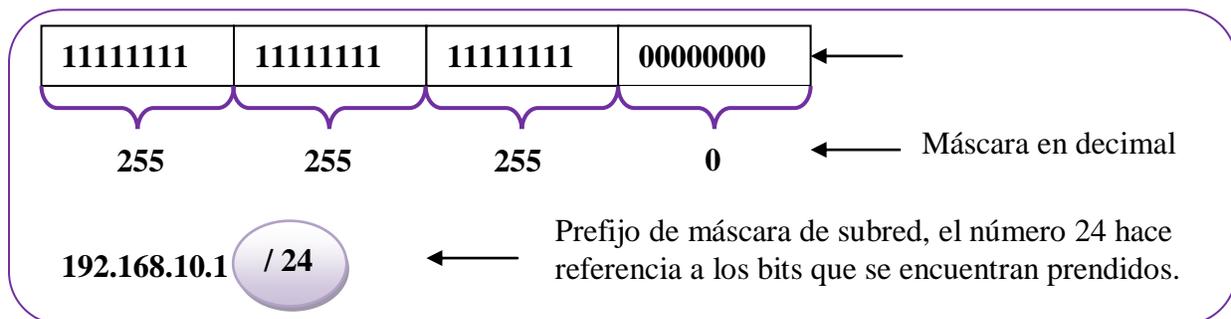


Figura 2.7 Notación de máscaras de subred.

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

1. Dirección de red: hace referencia a la red, esta dirección siempre es reservada y utiliza la primera dirección.
2. Dirección de broadcast: una dirección especial que se utiliza para enviar datos a todos los hosts de la red, esta dirección siempre es reservada y utiliza la dirección más alta.
3. Direcciones de host: las direcciones asignadas a los dispositivos finales de la red, es decir, computadoras, servidores, etcétera. (ver figura 2.8)

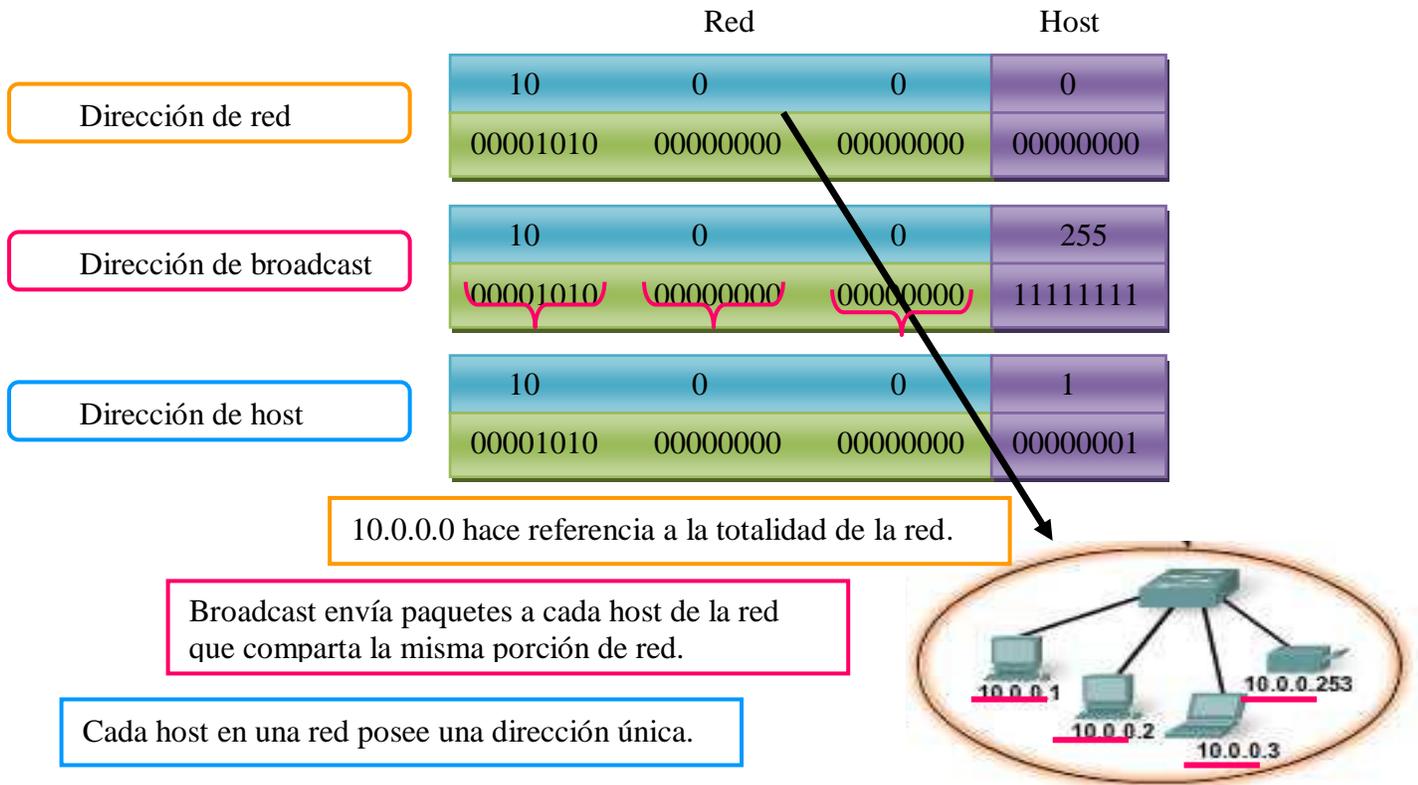


Figura 2.8 Dirección de red, broadcast y de host.

Las direcciones IP se clasifican de varias formas:

1. Públicas y privadas:

- Privadas: requieren o no acceso limitado a Internet y son conocidas como no homologadas o virtuales. El rango de direcciones privadas válidas es el siguiente:
 - a) Clase A: 10.0.0.0 – 10.255.255.255
 - b) Clase B: 172.16.0.0 – 172.31.255.255
 - c) Clase C: 192.168.0.0 – 192.168.255.254
- Públicas: se accede a ellas desde Internet y son conocidas como homologadas o reales.

El rango de direcciones IP públicas está compuesto por todas las direcciones IP que no forman parte del rango de direcciones IP privadas.

2. Por clases:

- Clase A: diseñada para redes extremadamente grandes con más de 16 millones de direcciones host. Utilizan un prefijo de /8, donde el primer octeto es de red y los tres restantes de host. Esto significa que sólo hay 128 redes de clase A, de 0.0.0.0 /8 a 127.255.255.255 /8.
- Clase B: diseñada para redes grandes con más de 65000 hosts. Usa los dos octetos superiores para red y los otros dos para host. De esta manera el bloque de direcciones es 128.0.0.0 /16 a 191.255.255.255 /16.
- Clase C: se diseñó para redes pequeñas con un máximo de 254 hosts. Utilizan un prefijo de /24, es decir, sólo utilizan el último octeto para direcciones de host. Quedando un rango de 192.0.0.0 /24 a 223.255.255.255 /24.
- Clase D: reservada para Multicast en el rango de 224.0.0.0 a 239.255.255.255.
- Clase E: reservada para Investigaciones en el rango de 240.0.0.0 a 255.255.255.255

En la tabla 2.1 se muestran los octetos que pertenecen al segmento de host y de subred de acuerdo con cada clase:

Tabla 2.1 Octetos de las direcciones IP por clase

Clase A	Subred	Host		
Octeto	1	2	3	4

Clase B	Subred		Host	
Octeto	1	2	3	4

Clase C	Subred			Host
Octeto	1	2	3	4

Clase D	Host			
Octeto	1	2	3	4

Para poder realizar cualquier tipo de direccionamiento lógico es necesario saber lo siguiente:

1. La **cantidad de subredes**, las cuales se obtienen de la siguiente forma:

2^n donde n corresponde a la cantidad de bits que se tomaron prestados de la porción de hosts, esto es, los bits que se toman para cubrir los requerimientos de las subredes.

Por ejemplo, se tiene la dirección de red 192.168.10.0 y se requieren 14 subredes y 14 hosts, por lo que (ver figura 2.9):

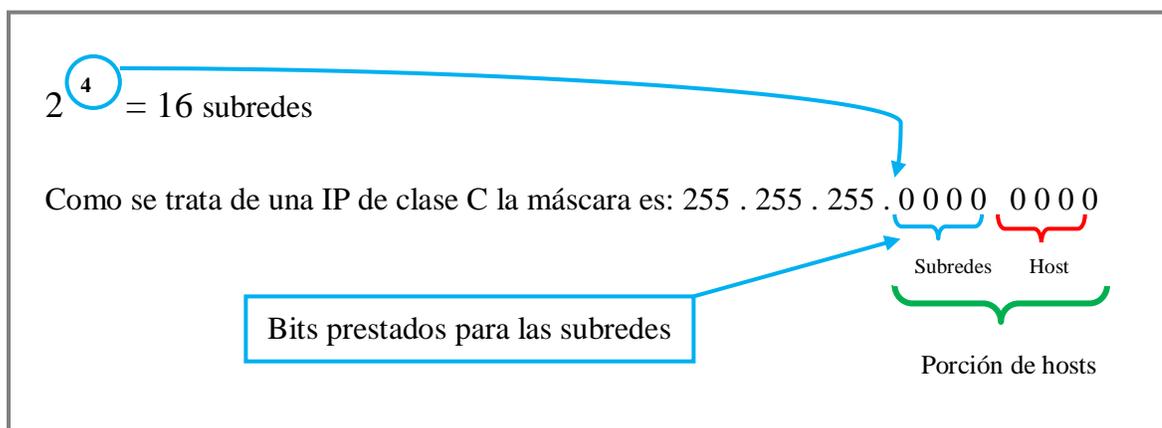


Figura 2.9 Bits prestados para asignación de subredes.

En el cálculo de subredes también es necesario restar dos y así el resultado serán las subredes utilizables, para el caso anterior, $2^4 - 2 = 14$ subredes utilizables.

2. La **cantidad de hosts**, se obtiene de la siguiente forma:

$2^n - 2$ donde n corresponde a la cantidad de bits para hosts.

Se restan dos debido a la dirección de red y a la de broadcast, por ejemplo:

$2^4 - 2 = 16 - 2 = 14$ lo que quiere decir que cada subred puede tener 14 hosts.

A continuación se estudian dos tipos de direccionamiento lógico: subnetting y VLSM.

a) **Subnetting** (subneteo)

Con este método se utiliza la máscara de red de tamaño fijo, es decir, todas las subredes quedan del mismo tamaño por lo que se desperdician muchas direcciones.

Para tener más claro cómo funcionan los métodos de direccionamiento se presenta un ejemplo donde una consultoría desea direccionar su red mediante la dirección de red 172.16.0.0 y cuya topología es la siguiente (Figura 2.10):

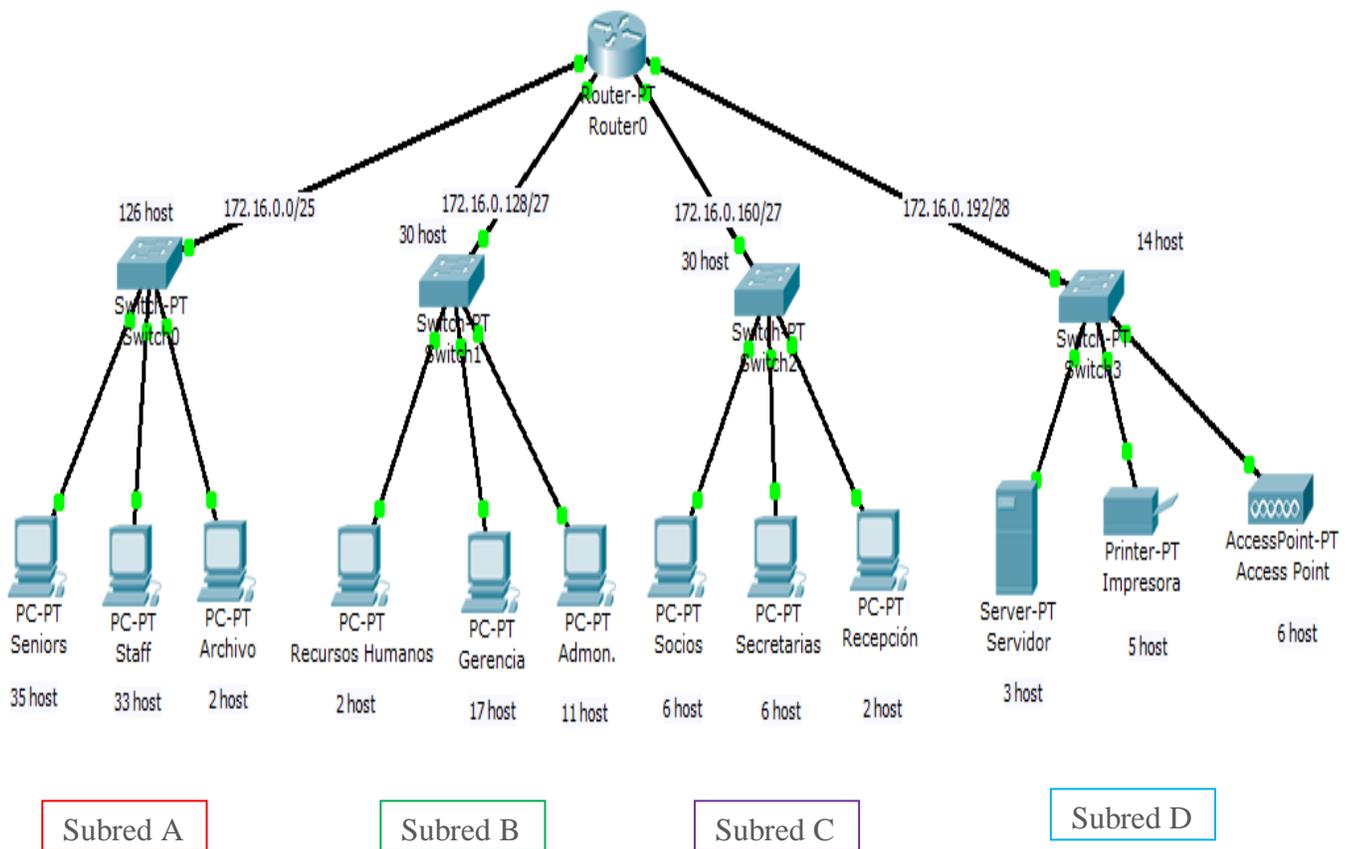


Figura 2.10 Diagrama de topología.

El ejercicio se va a resolver por ambos métodos, subnetting y VLSM para que así sea posible notar las diferencias entre cada tipo de direccionamiento.

Los requerimientos son los siguientes y aplicando la fórmula para obtener el número de hosts queda (ver tabla 2.2):

Tabla 2.2 Requerimientos de la red

Subred	Número de hosts	Bits de host
A	126	$2^7 - 2 = 126$
B	30	$2^7 - 2 = 126$
C	30	$2^7 - 2 = 126$
D	14	$2^7 - 2 = 126$

Solución por subnetting:

Paso 1. La dirección dada es 172.16.0.0, por lo tanto es clase B, cuya máscara por defecto es 255.255.0.0, así los segmentos se encuentran separados como se muestra en la figura 2.11:

Clase B	Subred		Host	
Octeto	172	16	00000000	00000000

Figura 2.11 Octetos de la dirección IP.

Paso 2. Identificar el número de bits a utilizar para cubrir los requerimientos tanto de subredes como de hosts:

- **Cantidad de hosts.** Se Aplica la fórmula $2^7 - 2 = 126$, por lo que siete bits de la sección de hosts serán usados para los hosts. (ver Figura 2.12)

Clase B	Subred		Host	
Octeto	172	16	00000000	00000000

Figura 2.12 Cantidad de bits para hosts.

- **Cantidad de subredes.** Se tiene que, $2^3 - 2 = 6$, lo que quiere decir que hay seis subredes posibles a utilizar, para este caso sólo se usarán cuatro las cuales cumplen con los requerimientos del ejercicio. (Ver figura 2.13)

Clase B	Subred		Host	
Octeto	172	16	00000000	00000000

Figura 2.13 Cantidad de bits para subredes.

Como se observa en la figura se toman tres bits del segmento de hosts para tener las subredes necesarias, por lo que, se tienen las siguientes combinaciones para los segmentos de red. (Ver figura 2.14)

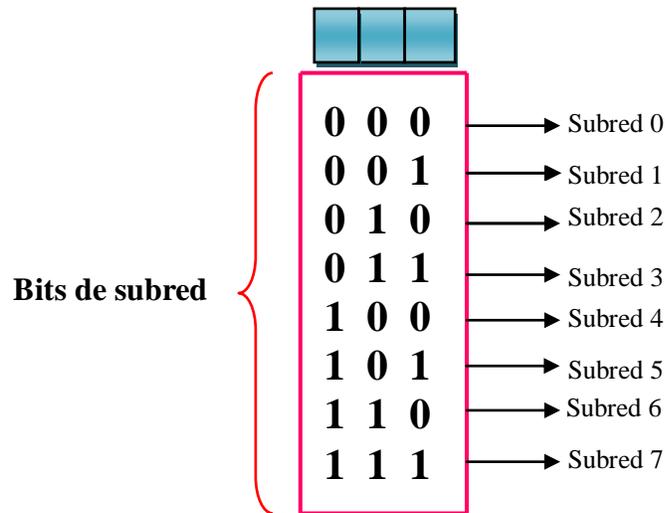


Figura 2.14 Cantidad de Subredes.

Paso 3. A partir de la dirección 172.16.0.0 se obtendrán las direcciones IP del segmento de cada red así como la de broadcast y las direcciones utilizables de cada segmento.

Para obtener las direcciones hay que sumarle un bit a cada dirección hasta obtener la dirección del segmento de red, las direcciones de hosts utilizables y la dirección de broadcast, como se muestra en la figura 2.15:

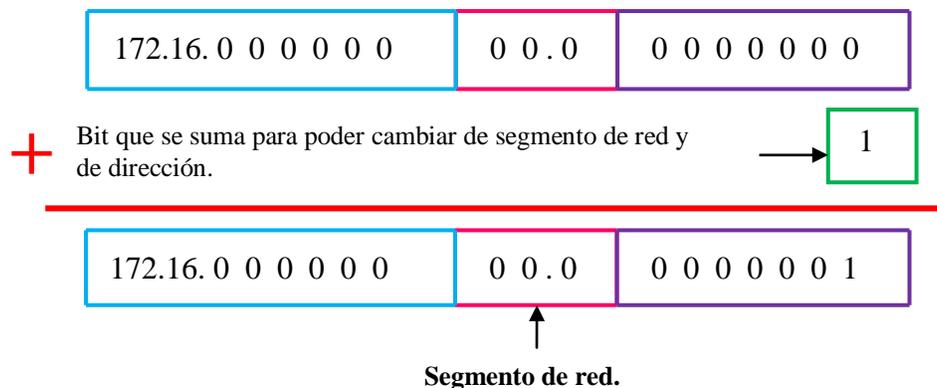
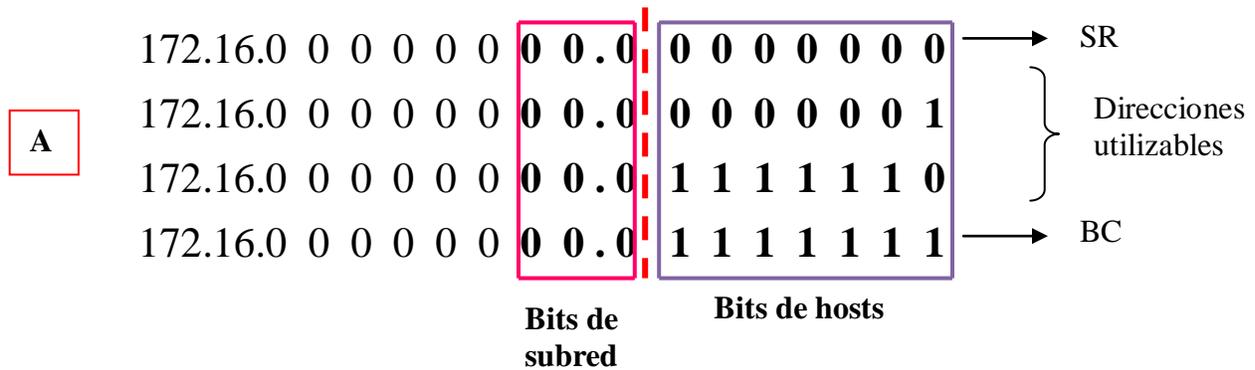
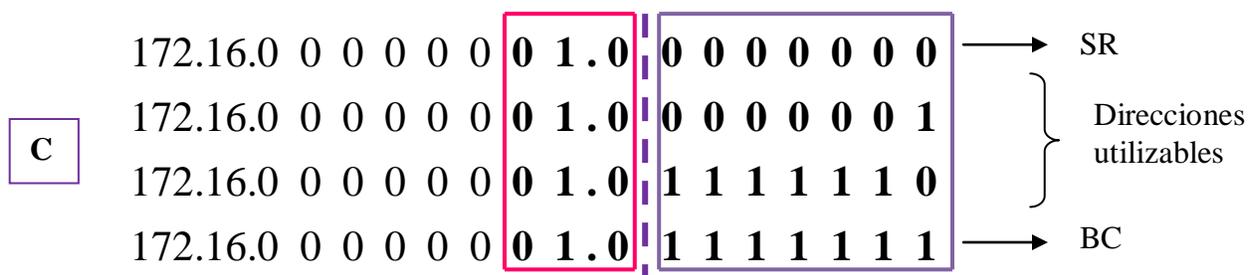
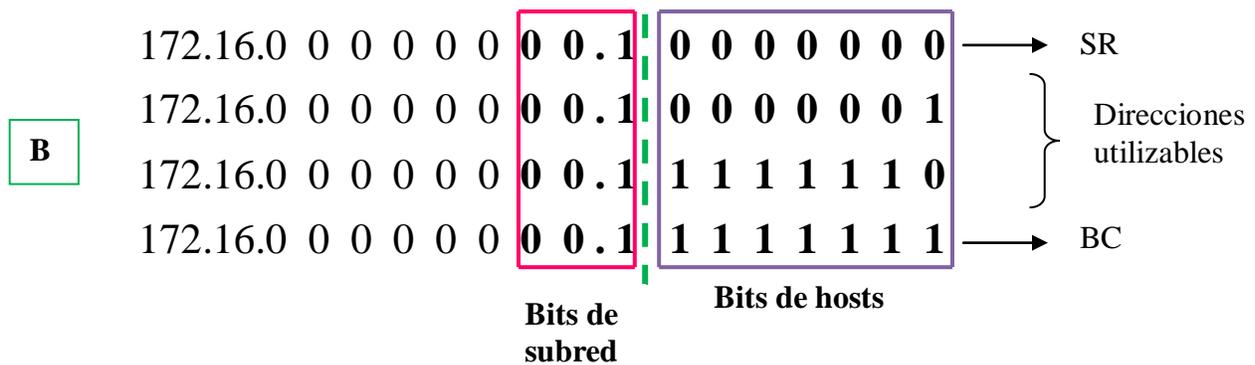


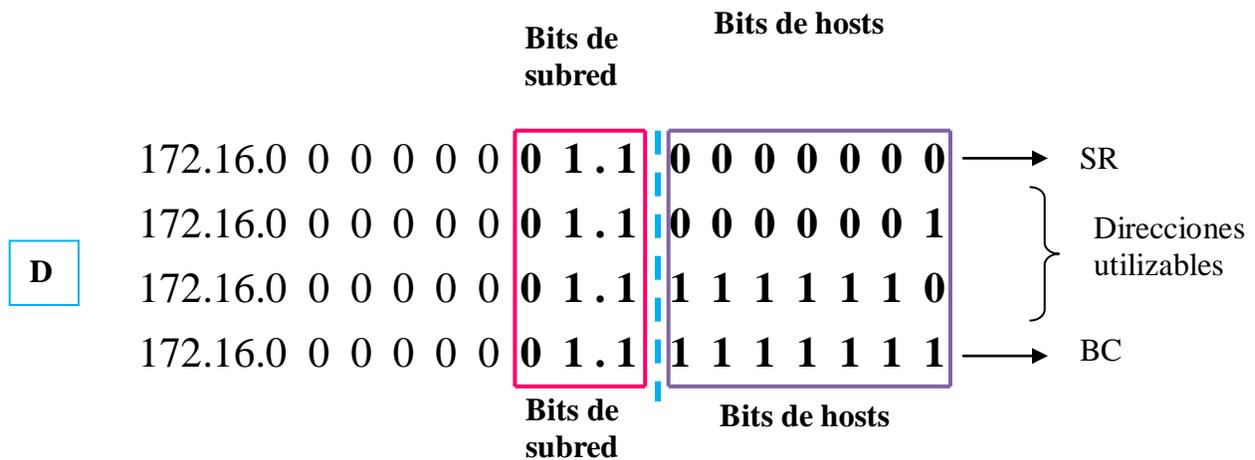
Figura 2.15 Suma de números binarios.

Paso 4. Ya que se tienen los elementos anteriores se desarrolla el subneteo, sumando de a un bit para cambiar de dirección y una vez que se obtiene la dirección de broadcast también se le suma un bit para cambiar al siguiente segmento de red como se mostró en los pasos anteriores.



Paso 5. Para obtener cada dirección se repite el paso cuatro, hasta obtener todos los segmentos de red requeridos, así como sus direcciones de hosts válidas.





Donde:

SR = dirección de segmento de red (primera dirección).

BC = dirección de broadcast (última dirección).

Se puede observar que a partir de la subred C se hace uso de un octeto más para poder cubrir los requerimientos de la red, ya que, con este método, todas las subredes deben quedar con 126 hosts por ser la subred que necesita más hosts. Así, para cada subred se piden “prestados” siete bits aunque no se necesite esa cantidad de hosts para todas las subredes.

Así nos queda una dirección de la siguiente forma (ver figura 2.16):

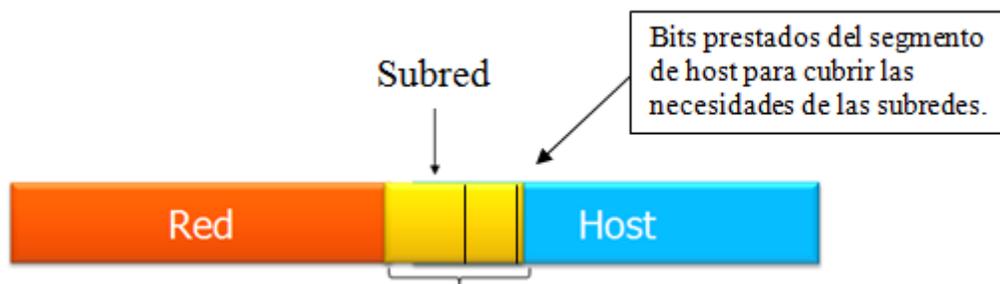


Figura 2.16 Dirección IP con subneteo

Si bien existe un desperdicio de direcciones, también es notable la ventaja que tiene sobre VLSM, ya que al tener un incremento futuro hay espacio disponible para las nuevas necesidades de la red, en cambio, con VLSM, la red queda justa por lo que si se presenta un incremento es necesario cambiar toda la red lo que genera una inversión de tiempo y por lo tanto de dinero para las organizaciones.

En la siguiente tabla se muestran los resultados del ejercicio (Tabla 2.3):

Tabla 2.3 Resultados del direccionamiento por subnetting.

Subred	Dirección de subred	Rango de direcciones utilizables	Dirección de broadcast	Máscara de subred o prefijo	Direcciones desperdiciadas
A	172.16.0.0	1 – 126	172.16.0.127	255.255.255.128 /25	Ninguna
B	172.16.0.128	129 – 254	172.16.0.255	255.255.255.128 /25	96
C	172.16.1.0	1 – 126	172.16.1.127	255.255.255.128 /25	96
D	172.16.1.128	129 – 254	172.16.1.255	255.255.255.128 /25	112

Mediante esta tabla se observa que el desperdicio de direcciones es muy grande, por lo que es conveniente realizar el direccionamiento por el método de VLSM para que el desperdicio de direcciones no sea tan grande.

b) VLSM (Máscaras de subred de tamaño variable)

Se diseñó para maximizar la eficiencia del direccionamiento. Al contrario de subnetting este método utiliza una máscara de longitud variable, por lo que el desperdicio de direcciones no es tan grande como con subnetting.

Se resuelve el ejercicio anterior mediante VLSM. En la tabla 2.4 se muestran los requerimientos y se observa el uso de la fórmula para calcular el número de hosts:

Tabla 2.4 Requerimientos de red por VLSM y cálculo de hosts

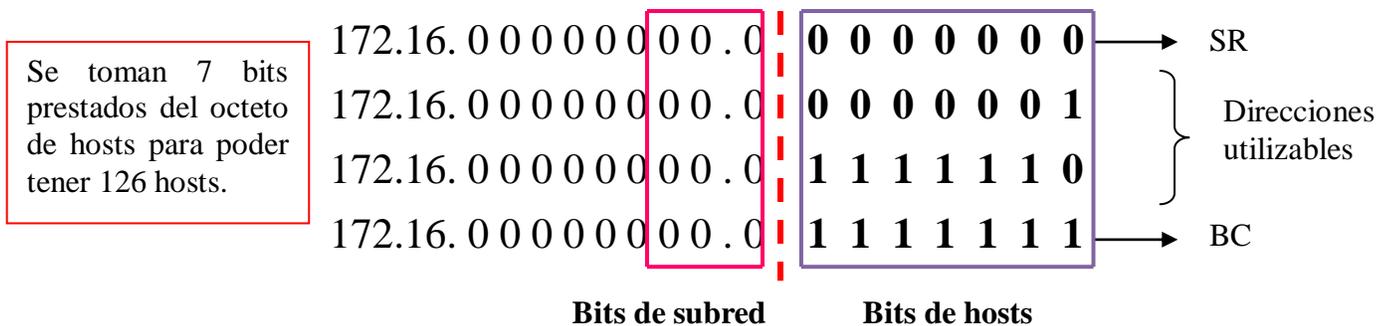
Subred	Número de hosts	Bits de host
A	126	$2^7 - 2 = 126$
B	30	$2^5 - 2 = 30$
C	30	$2^5 - 2 = 30$
D	14	$2^4 - 2 = 14$

Solución por VLSM con la dirección 172.16.0.0:

Paso 1. El proceso para calcular los bits de hosts y de subred es el mismo que se utilizó para subneteo, sin embargo, en este caso el número de hosts será variable, de acuerdo con las necesidades de la red, como se muestra en la tabla 2.4.

Para el número de subredes se tiene que también se necesitan tres bits prestados del segmento de hosts, pero al utilizar el método de máscara de longitud variable, estos bits van a variar en cada segmento de red a diferencia del subneteo que eran fijos. Tomando en cuenta esta variación, la máscara de subred va a cambiar para cada subred.

Paso 2. Una vez calculados los bits a utilizar se comienza a obtener las direcciones. La dirección dada es 172.16.0.0 la cual pertenece al primer segmento de red, de ahí se parte para obtener el rango de direcciones IP utilizables sumando de bit en bit para cambiar de dirección, hasta obtener la dirección de broadcast, como se muestra a continuación:



Ya que son necesarios siete bits para poder tener 126 hosts se obtienen direcciones de la siguiente forma cuya máscara corresponde a 255.255.255.128 o bien prefijo /25 (ver figura 2.17). Así para cada segmento de red cambiará la máscara de acuerdo con el número de hosts requeridos.

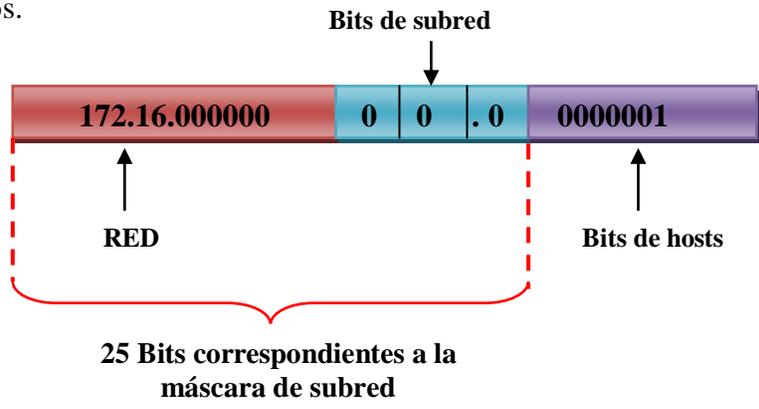
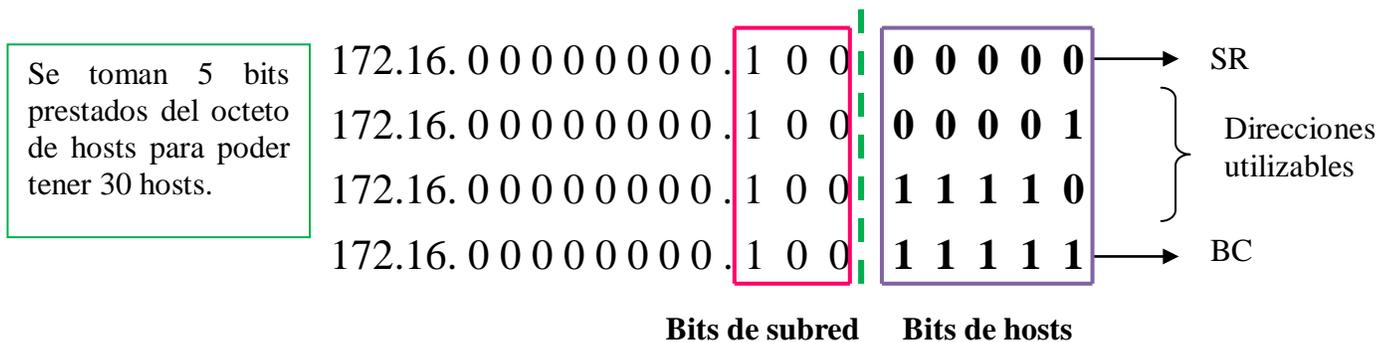
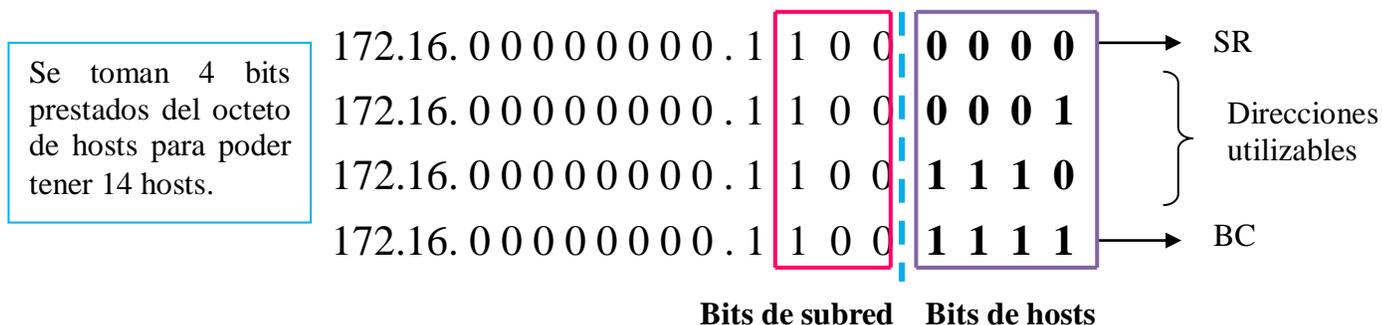
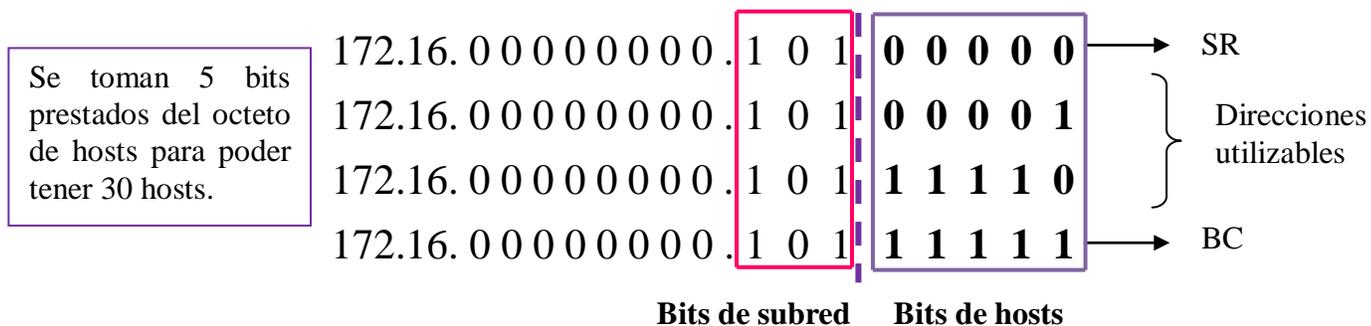


Figura 2.17 Dirección IP con VLSM.

Paso 3. Continuando con el siguiente segmento de red se suma un bit a la última dirección obtenida del segmento anterior, es decir, a la dirección de broadcast, en este caso a la dirección 172.16.00000000.01111111, para así, obtener la nueva dirección del segmento de red.



Paso 4: se repite el paso anterior hasta obtener todos los segmentos de red requeridos.



De esta manera los resultados quedan como se muestran en la tabla 2.5:

Tabla 2.5 Resultados del direccionamiento por VLSM

Subred	Dirección de subred	Rango de direcciones utilizables	Dirección de broadcast	Máscara de subred o prefijo	Direcciones desperdiciadas
A	172.16.0.0	1 – 126	172.16.0.127	255.255.255.128 /25	Ninguna
B	172.16.0.128	129 – 158	172.16.0.159	255.255.255.224 /27	Ninguna
C	172.16.0.160	161 – 190	172.16.0.191	255.255.255.224 /27	Ninguna
D	172.16.0.192	193 – 206	172.16.0.207	255.255.255.240 /28	Ninguna

Mediante esta tabla se nota que no se desperdicia ninguna dirección, lo cual no siempre sucede, sin embargo, son mucho menores los sobrantes de direcciones con VLSM que con subnetting.

2.5 Diseño de políticas de cómputo

Actualmente la seguridad informática juega un papel de suma importancia en las organizaciones por lo que éstas se han preocupado por diseñar un conjunto de políticas de seguridad para proteger sus activos tanto físicos como lógicos.

La mayoría de los incidentes de seguridad se producen porque los administradores de sistemas no implementan las medidas correctivas disponibles y los agresores o los empleados descontentos explotan el descuido. De aquí que las políticas de seguridad en cómputo sean de gran importancia.

Una política es un conjunto de reglas que guían una identidad, cada regla define una acción.

Una política de seguridad en cómputo es un documento que define reglas y principios para lograr la seguridad, tener un orden y hacer buen uso de variables de red de una determinada organización, en ella se especifican las condiciones, los derechos y las obligaciones de cada persona que colabore en dicha organización.

En resumen, una política de seguridad en cómputo se puede interpretar como se muestra en la figura 2.18:

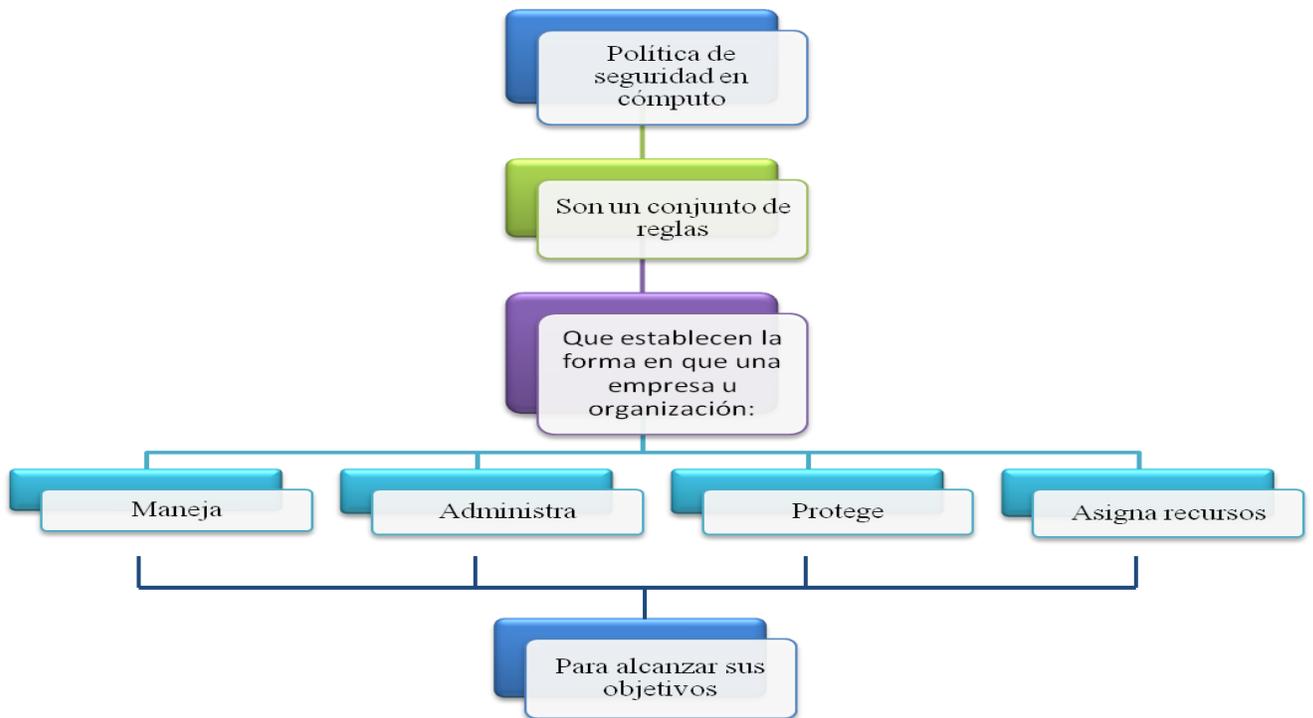


Figura 2.18 Definición de política de seguridad en cómputo.

El RFC-2196 establece que “una política de seguridad es una declaración formal de las normas por las que se deben regir las personas que obtienen acceso a los bienes de tecnología e información de una organización”.

Una política de seguridad en cómputo debe cumplir los siguientes objetivos:

- Informar a los usuarios y al personal acerca de los requisitos obligatorios para proteger los bienes de tecnología e información.
- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos.
- Prevenir la pérdida de información.
- Tener un uso adecuado y eficiente de los sistemas de cómputo y telecomunicaciones.
- Estandarizar la seguridad tanto en el ámbito humano como en el tecnológico.

El hecho de realizar un manual de políticas de seguridad en cómputo presenta varias ventajas que permiten el mejor desempeño de las organizaciones, tales como:

- Ayudan a la adquisición del Hardware y Software.
- Permite que las autoridades actúen en caso de una violación a la seguridad.
- Facilita la auditoría.
- Evita la excusa llamada ignorancia.

Para poder realizar una política de seguridad se debe dar respuesta a las siguientes interrogantes (figura 2.19):



Figura 2.19 Cuestionamientos necesarios para la realización de una política de seguridad en cómputo.

Una vez respondidas estas preguntas, hay que tomar en cuenta los siguientes aspectos:

Consideraciones

- ¿Quién debe poder usar los recursos?

De acuerdo con la estructura de la empresa y los puestos asignados, a cada empleado se le asignan los recursos, ya que no todos necesitan los mismos para realizar su trabajo. Por tanto se pueden dividir en áreas de acuerdo con su función, por ejemplo, contabilidad, recursos humanos, etcétera.

- ¿Qué constituye un uso adecuado de los recursos?

Una vez determinados los usuarios autorizados para tener acceso a los recursos de la red, se deberán establecer los lineamientos del uso aceptable de dichos recursos. Esto depende de la clase de usuarios, como desarrolladores de software, estudiantes, profesores, proveedores, etcétera. Por lo que la política debe establecer qué tipo de uso es aceptable y cual inaceptable de manera clara.

Para que esto sea posible es necesario crear políticas por secciones, como se muestra en la tabla 2.6:

Tabla 2.6 Políticas de seguridad en cómputo por secciones.

Políticas por sección	Descripción
1. Usuarios	En cada organización existen distintos tipos de usuarios, como estudiantes, investigadores, administrativos, docentes, programadores, etcétera. Por lo que es necesario establecer los derechos y obligaciones que cada uno tendrá.
2. Cuentas	Se refiere a la creación, seguimiento y características de las cuentas, por ejemplo: dar de alta sólo las cuentas que se ocuparán, dar de baja las cuentas de los ex-empleados, establecer una contraseña robusta, así como una fecha de caducidad de ésta, cambiar las contraseñas con privilegios de administrador cuando uno de ellos ya no labore en la organización, entre otras.
3. Administradores	También deben existir políticas para los administradores de la red ya que en muchas ocasiones necesitan recabar información de directorios y archivos privados de los usuarios para diagnosticar problemas del sistema e investigar violaciones de la seguridad. Por lo que se debe especificar el grado al que el administrador pueda examinar.
4. Seguridad Física	Se refiere al acceso físico, estructura del edificio, ubicación y acceso del centro de datos. Establece qué controles se van a implementar en la organización para controlar el acceso a las instalaciones.
5. Red	Se trata de la configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, gestión de cambios y desarrollo de aplicaciones.

- ¿Quién debe proporcionar acceso al sistema?

Los directivos junto con los expertos en tecnologías de la información se encargan de definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de una actividad determinada, con lo que los procesos más

importantes recibirán mayor protección, proporcionando acceso al sistema al personal calificado de acuerdo con cada actividad y al rol dentro de la organización de cada empleado.

- ¿Quién debe tener privilegios de administrador?

Se debe de poner a cargo a un especialista en gestión de recursos tecnológicos y de información. Quién es responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas y procedimientos de seguridad en la organización. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, así como proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad informática.

- ¿Cuáles son los derechos y responsabilidades de los usuarios?

Las políticas de seguridad deben definir tanto las responsabilidades como los derechos de los usuarios que utilizan los recursos y servicios de la red, a continuación se listan los más importantes:

1. Los usuarios son responsables de hacer respaldos de sus datos o es esta responsabilidad del administrador del sistema.
2. Acciones legales u otros castigos pueden implantarse a los usuarios que divulguen información que pueda estar patentada.
3. Cumplir con los lineamientos acerca del uso de recursos de la red con el fin de no afectar el desempeño del sistema.

Metodología

1. **Objetivos:** esta etapa se encarga de identificar por qué se necesita la política. Se deben establecer las normas que soporten y orienten el proceso de seguridad de la información en la organización.
2. **Preparación:** es necesario realizar un análisis de lo que se quiere proteger y cómo se va a proteger, de lo contrario, las políticas implementadas no tendrán éxito. Por tal motivo, hay que hacer una serie de investigaciones e inventarios, de acuerdo con la importancia que cada bien tenga para la empresa, para así poder desarrollar políticas de acuerdo con las necesidades específicas de la organización.

3. **Redacción:** se escriben las políticas de seguridad de acuerdo con las siguientes reglas:

- Elegir una filosofía básica, esto es, permisiva o prohibitiva, es decir (ver figura 2.20):



Figura 2.20: Filosofías a elegir para crear una política de seguridad.

- Deben estar escritas en tiempo presente, de estar en futuro, deberá tomarse en cuenta la fecha en la cual entrarán en vigor, la cual debe estar claramente especificada e impresa en el documento.
 - Debe cubrir todos los aspectos relacionados con el sistema, esto es, tomar en cuenta los distintos componentes del sistema, hardware, software, entorno físico y usuarios, así como la interacción entre los mismos.
 - Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.
 - Debe tomar en cuenta el entorno del sistema, es decir, si se trata de una organización comercial, bancaria, educativa, etcétera.
4. **Edición:** una vez redactadas las políticas de seguridad éstas podrán ser impresas para su revisión y aprobación por los directivos y especialistas en tecnologías de la información y así poder ser aplicadas.
5. **Aprobación:** una vez terminada la documentación de la política, ésta debe ser remitida a los directivos de la organización para que puedan realizar todos los ajustes y revisiones necesarias para obtener una versión final de la política y que finalmente sea aprobada para su publicación.
6. **Difusión:** esta etapa implica determinar el alcance y el método de distribución de la política. La política debe ser inicialmente difundida a los miembros que sean

afectados directamente por éstas. Se deben tomar en cuenta factores como la ubicación geográfica, el idioma y la cultura.

7. **Revisión:** con el objetivo de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del mismo. Esta simulación y los casos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.
8. **Aplicación:** para un buen funcionamiento debe realizarse un control periódico de las políticas, asegurando así el fiel cumplimiento de todos los procedimientos plasmados en éstas.
9. **Actualización:** la seguridad es un proceso por lo que las políticas de seguridad tienen un ciclo de vida. Se trata de un proceso dinámico y continuo sobre el que hay que adecuarse continuamente a fin de subsanar inmediatamente cualquier debilidad descubierta, con el fin de que el sistema se encuentre lo más seguro posible.

Contenido

- **Ámbito de aplicación:** es necesario tomar en cuenta el entorno del sistema, es decir, el tipo de organización o entidad, ya sea, comercial, bancaria o educativa, adecuándose así a sus necesidades y recursos, el valor que se le da a los recursos y a la información y el uso que cada departamento hace del sistema.
- **Análisis de riesgo:** procedimiento para estimar o calcular el riesgo²³ de los activos y la pérdida debido a la manifestación de las amenazas, es decir, de los ataques.
- **Enunciados de políticas:** se trata de las reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.
- **Sanciones:** éstas son aplicadas en caso de que se detecte la violación de una política de seguridad, para lo cual es necesario determinar si ésta ocurrió debido a negligencia, accidente o error, ignorancia de la política vigente o si deliberadamente la política fue pasada por alto. Así para cada caso habrá una sanción distinta, es por ello que debe existir un apartado de sanciones que sean explicadas detalladamente

²³ Riesgo: posibilidad o probabilidad de que exista una pérdida o daño.

debido a que éstas pueden ir desde una advertencia verbal, una carta formal o la presentación de cargos judiciales.

Debe llevarse un registro de las violaciones a las políticas de seguridad, el cual será revisado periódicamente para observar tendencias y tal vez ajustar la política tomando ya en cuenta cualquier nuevo tipo de amenaza.

- **Sección de procedimientos para el manejo de incidentes:** se implementa esta sección de procedimientos alternativos a la operativa normal de la empresa, con la finalidad de permitir el funcionamiento de ésta, aún cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.

Participantes

- **Administradores de sistemas:** son los responsables de monitorear y vigilar que las políticas de seguridad se cumplan al pie de la letra, así como de mantener actualizados los datos de las cuentas, software del equipo y que el sistema trabaje eficientemente, entre otras tareas. Además, como se mencionó, ellos también se encuentran sujetos a ciertas políticas.
- **Personas con autoridad:** autoridad de nivel superior que integra la organización. Bajo su administración se encuentra la aprobación de las políticas de seguridad.
- **Representante jurídico:** es necesario contar con su presencia ya que algunas sanciones implican aspectos legales.
- **Editor / Redactor:** se refiere a la persona encargada de redactar y editar las políticas de seguridad de la empresa u organización para poderlas dar a conocer a todos los colaboradores de ésta.
- **Usuarios:** son quienes llevaran a la práctica las políticas de seguridad establecidas, pueden ser: estudiantes, administrativos, docentes, investigadores, sistemas, etcétera.

La política de seguridad es para todos, empleados, contratistas, proveedores y usuarios que tienen acceso a la red. Sin embargo, debe tratar a cada uno de estos grupos de manera diferente. A cada grupo sólo se le debe mostrar la parte de la política correspondiente a su trabajo y a su nivel de acceso a la red.

2.6 Ética informática

La ética es una rama de la filosofía y es considerada la ciencia que se ocupa de las normas de la conducta humana, lo que la hace distinguirse de las ciencias exactas.

La palabra ética proviene del latín *ethos*²⁴, cuyo significado es costumbre; actualmente se define como el conjunto de principios, valores, costumbres y normas de conducta, adquiridos, asimilados y practicados de un modo estrictamente racional o consciente. Corresponde al ejercicio libre y consciente de la razón para justificar nuestros actos desde el punto de vista del bien y del mal. Tiene como objeto de estudio la acción humana y la moral.

A diferencia de la ética, la moral, no depende de una actitud plenamente consciente o racional, sino principalmente, de un sentimiento de respeto a la autoridad moral de la que provienen, ya que se refiere a un conjunto de normas que se transmiten de generación en generación, que evolucionan a lo largo del tiempo y poseen fuertes diferencias con respecto a las normas de otra sociedad y de otra época histórica.

La moral tiene una base social, es un conjunto de normas establecidas en el seno de una sociedad y como tal, ejerce una influencia muy poderosa en la conducta de cada uno de sus integrantes. En cambio la ética surge como tal en el interior de una persona, como resultado de su propia reflexión y su propia elección.

La ética informática se trata de una rama de la ética, la cual analiza los problemas éticos que son creados por la tecnología, las computadoras o también de los que son transformados o agravados por las mismas, es decir, por las personas que utilizan los avances de las tecnologías de la información con fines maliciosos o para perjudicar a otras personas.

Fue creada recientemente debido al crecimiento de las tecnologías de la información.

Su existencia tiene como punto de partida el hecho de que los ordenadores suponen unos problemas éticos particulares y por tanto distintos a otras tecnologías.

Los objetivos de la ética informática son:

1. Contribuir al bienestar humano y de la sociedad.
2. Evitar daños.
3. Ser honesto y confiable.

²⁴ López, M.J. y Quezada, C (2006). *Fundamentos de seguridad informática*, p. 179. Facultad de Ingeniería: UNAM.

4. Honrar los derechos de propiedad, incluyendo derechos de autor y patentes.
5. Dar los créditos apropiados por la propiedad intelectual.
6. Respetar la privacidad de los demás.
7. Alcanzar la más alta calidad y efectividad en el proceso y en los productos del trabajo profesional.
8. Acceder a los recursos de computación y comunicación sólo con la debida autorización.

La ética informática se encuentra sustentada en una serie de principios, los cuales, se listan a continuación:

1. **Intimidad:** se refiere a que se debe tratar a la información privada con respeto no compartiéndola con otras personas que no tienen derecho a ello. Cumpliendo con el secreto profesional y la confidencialidad.
2. **Exactitud:** se define como la puntualidad y la fidelidad en la transmisión de los datos. Requiere que los profesionales de las tecnologías de la información salvaguarden la información que está a su cuidado.
3. **Propiedad intelectual:** instruye a los informáticos para respetar la propiedad intelectual personal de los otros y para dar referencias apropiadas de tal manera que la propiedad intelectual de los otros sea reconocida cuando es usada en investigación o redacción. Los derechos de autor y otras protecciones legales de la propiedad intelectual deben ser apropiadamente obedecidas.

El informático debe evitar copiar programas, bases de datos, archivos, información y demás, que es propiedad intelectual que no le pertenece, para no cometer delitos informáticos que pudieran ser perseguidos por la ley.

4. **Acceso:** se refiere a que el acceso a la información esté disponible a cualquier persona siempre y cuando cuente con autorización.

En la ética informática se incluyen también **diez mandamientos**²⁵, éstos son:

1. No usarás una computadora para dañar a otros.
2. No interferirás con el trabajo ajeno.
3. No indagarás en los archivos ajenos.
4. No utilizarás una computadora para robar.
5. No utilizarás la informática para realizar fraudes.
6. No copiarás o utilizarás software que no hayas comprado.

²⁵ Los diez mandamientos de la ética informática fueron extraídos de la siguiente página de Internet: <http://www.cpsr.org/issues/ethics/cei>

7. No utilizarás los recursos informáticos ajenos sin la debida autorización.
8. No te apropiarás de los derechos intelectuales de otros.
9. Deberás evaluar las consecuencias sociales de cualquier código que desarrolles.
10. Siempre utilizarás las computadoras para respetar los derechos de los demás.

Códigos de ética

Otra herramienta útil dentro de las organizaciones son los códigos deontológicos o de ética profesional, los cuales se encargan de fijar normas que regulan el comportamiento profesional de las personas dentro de una empresa u organización.

Tienen como objetivo guiar el comportamiento de los integrantes de la organización y de aquellos con los cuales ésta actúa habitualmente: clientes, proveedores y contratistas. De aquí que sea sumamente importante contar con un código de ética en las empresas u organizaciones.

Las funciones de los códigos deontológicos son las siguientes:

- Hace responsable a un profesional de las consecuencias económicas, sociológicas y culturales del producto.
- Sirve como suplemento a las medidas legales y políticas.
- Dan identidad a los informáticos como un grupo que piensa de una determinada manera.
- Fuente de evaluación pública.
- Función sociológica ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera.

Debido a que actúa como un mecanismo de autorregulación en el ámbito de la comunicación social, la psicología, la medicina, la informática, y muchas otras áreas, ha cobrado una enorme popularidad por lo que en la mayoría o en todas las instituciones se adopta este método como una forma de controlar lo que los empleados puedan hacer con la información, dispositivos e instalaciones dentro y fuera de las organizaciones.

Así es como surge una gran variedad de códigos de ética, desde códigos de escuelas, como es el caso del código de la Universidad Nacional Autónoma de México²⁶ o hasta el código de ética de una profesión en específico, como lo es el código del Ingeniero mexicano²⁷.

²⁶ El código de ética de la UNAM se puede consultar en la siguiente página de Internet: <http://redyseguridad.fi-p.unam.mx/politicas/Codigo%20de%20etica%20universitario.pdf>

²⁷ El código de ética del Ingeniero mexicano se puede consultar en la siguiente página de Internet: <http://www.ingenieria.unam.mx/~guiaindustrial/valores/info/3/1.htm>

CAPÍTULO 3

Organización



“¿Cómo se verá la corporación del futuro? Desde afuera, parecerá sin fronteras, con interfaces permeables y en cambio constante entre la empresa, proveedores y clientes. Desde adentro, no será menos amorfa, con oficinas, departamentos y divisiones reformándose constantemente según sea necesario”

Bill Davidow y Mike Malone

3.1 Modelo básico de administración de redes.

La administración de redes requiere de la habilidad para supervisar, comprobar, sondear, configurar y controlar los componentes de hardware y software de una red. Así mismo, el administrador de redes debe dominar los aspectos que permiten definir una red, de tal manera que ésta sea:

- Escalable: habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, así como de estar preparada para hacerse más grande sin perder calidad en los servicios ofrecidos.
- Transparente: habilidad de un protocolo de transmitir datos a través de la red de manera que sea transparente para aquellos que están usando el protocolo.
- Eficiente: uso racional de los dispositivos con los que se cuenta para alcanzar los objetivos y metas programadas, con el mínimo de recursos disponibles y tiempo, logrando de esta forma su optimización.
- Confiable: asegurar que cada sección de datos que envía el origen llegue al destino, tal y como fueron enviados.

Principales tareas de un administrador

1. Monitoreo de la disponibilidad de red: ésta es una tarea imprescindible para la administración de una red, ya que gracias a esto es posible detectar fallas en la red y así trabajar enseguida en su solución permitiendo una mayor eficiencia en la red.
2. Mejorar la automatización: optimizar los procesos haciendo que éstos se realicen de manera automática mediante programaciones, incrementando la calidad de los resultados.
3. Vigilar el tiempo de respuesta: monitorear el tiempo en que se realizan los procesos con lo cual se podrá percatar el administrador qué procesos son los que llevan más tiempo, pudiendo así hacer correcciones necesarias en éstos para que sean más eficientes.
4. Seguridad: indica que determinado sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

La seguridad en muchas ocasiones no se ha tomado en cuenta, sin embargo, es un proceso imprescindible dentro de la implementación y administración de una red, que si no se considera desde un inicio, después resulta mucho más costoso.

5. Redireccionar el tráfico: configurar protocolos de acuerdo con las necesidades de la red, de manera que los paquetes viajen por el mejor camino, evitando así pérdidas de datos y un menor tiempo de transmisión.
6. Contar con la capacidad de restablecimiento: en caso de que la red falle, el administrador debe configurarla de manera que se recupere de los fallos y de resolver los errores en el menor tiempo posible.
7. Registrar usuarios: el administrador es la única persona que puede dar de alta, de baja o proporcionarle más accesos o menos a los usuarios de la red, esto de acuerdo con las tareas desempeñadas por cada colaborador de la empresa.

La administración de redes considera

- a) Controlar los medios corporativos, para que éstos ofrezcan un correcto rendimiento.
- b) Control de la complejidad, controlar tanto los componentes, como el número de usuarios, interfaces, protocolos, proveedores, para no perder la pista de la red.
- c) Mejorar el servicio, los usuarios esperan mejores servicios aunque la red crezca.
- d) Balanceo de distintas necesidades, los usuarios deben contar con diversas aplicaciones para un nivel de soporte en específico, con especial interés en las áreas de rendimiento, disponibilidad y seguridad.
- e) Reducción de tiempos muertos, es importante considerar una alta disponibilidad de los recursos, gracias al propio diseño redundante.
- f) Control de costos, vigilar y controlar la utilización de los recursos para que los usuarios estén sin la necesidad de incrementar costos.

La interacción entre el administrador y el dispositivo administrado, añade tráfico a la red, por lo que es necesario que cuando estos elementos se incorporen, se cuente con estrategias de monitoreo que aumenten el rendimiento de la red, considerando que los dispositivos administrados deben contar con la capacidad de responder a las peticiones del administrador, sin tener que descuidar sus funciones.

La administración de redes se subdivide en administración de redes informáticas y administración de redes de telecomunicaciones (ver figura 3.1).

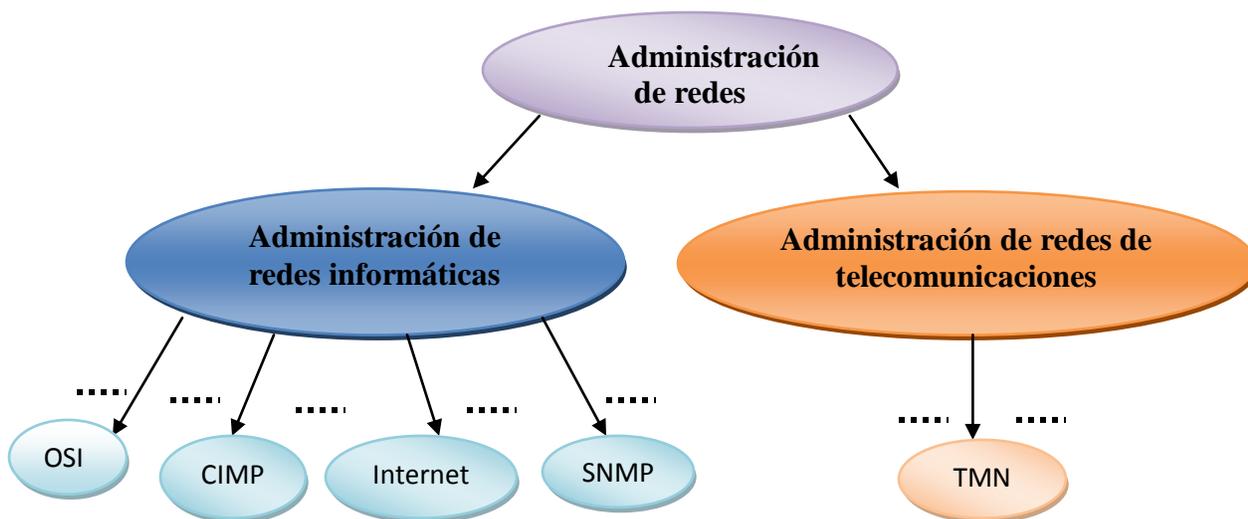


Figura 3.1 División de la administración de redes.

La Administración de Redes Informáticas es un conjunto de acciones cuyo objetivo primordial es mantener la red operativa, eficiente, y segura. La administración de la red debe por tanto conseguir, mejorar la continuidad de la red con mecanismos de control interno y externo, así como la resolución de problemas en el menor tiempo posible. Para ello la administración de la red debe hacer uso de protocolos que permiten conseguir dicho objetivo.

Por otro lado, la administración de redes de telecomunicaciones proporciona funciones de gestión y comunicaciones para la operación de la administración y mantenimiento de las redes de telecomunicaciones y sus servicios en un entorno de múltiples fabricantes. Razón por la cual se desarrolla la arquitectura TMN, así como por la heterogeneidad en la tecnología para la construcción de redes de telecomunicación.

Arquitectura de administración de redes

La administración de redes requiere de la habilidad para supervisar, comprobar, sondear, configurar y controlar los componentes de hardware y software de una red. Para ello se requiere de una arquitectura de sistemas de administración de redes que se compone de los siguientes elementos.

²⁸ (ver tabla 3.1):

²⁸ Ford. M., Lew. K., Spanier. S. y Stevenson. T. (1998). Fundamentos de la administración de las redes. *Tecnologías de interconectividad de redes*, (p. 77-82) México: Prentice Hall.

Tabla 3.1 Elementos y descripción de la arquitectura de sistemas de administración de redes.

Elemento	Descripción
Entidad administradora	Aplicación con control humano que se ejecuta en una estación centralizada de administración de red (NOC: Centro de operaciones de red).
Base de información de administración (MIB)	Lugar donde se almacenan los datos referentes a los objetos administrados.
Agente de administración de red	Proceso residente que se ejecuta en cada dispositivo administrado.
Protocolo de administración de red	Éste se ejecuta dentro de la entidad administradora y el dispositivo administrado.

Los agentes pueden utilizar el protocolo de administración de red para informar a la entidad administradora de eventos excepcionales, por ejemplo: el fallo de componentes o la trasgresión de los umbrales de rendimiento. Esta infraestructura es la base de la implementación de diferentes modelos de administración de red. (Ver figura 3.2)

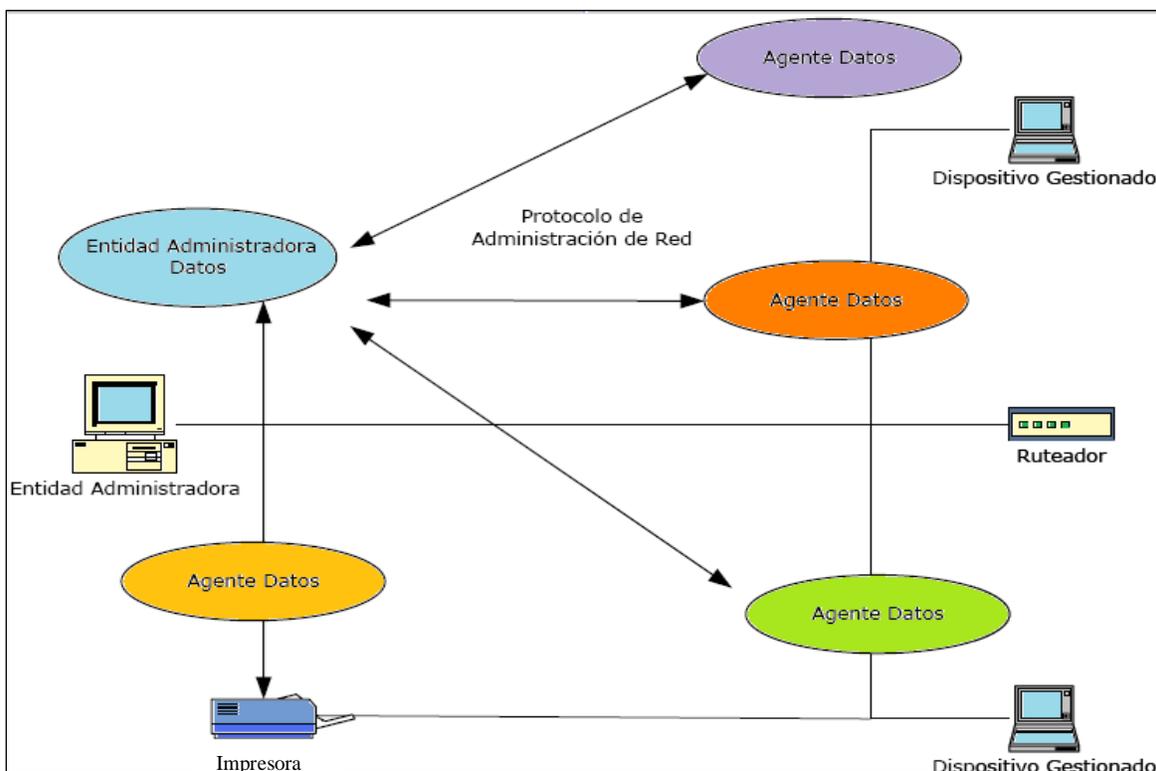


Figura 3.2 Infraestructura de administración de redes.

La OSI (Organization International for Standardization – Organización Internacional para la Normalización) creó un comité para generar un modelo para la administración de una red, éste se compone de cuatro submódulos, con el propósito de tener un entorno de trabajo estructurado, como se plantea en la figura 3.3.

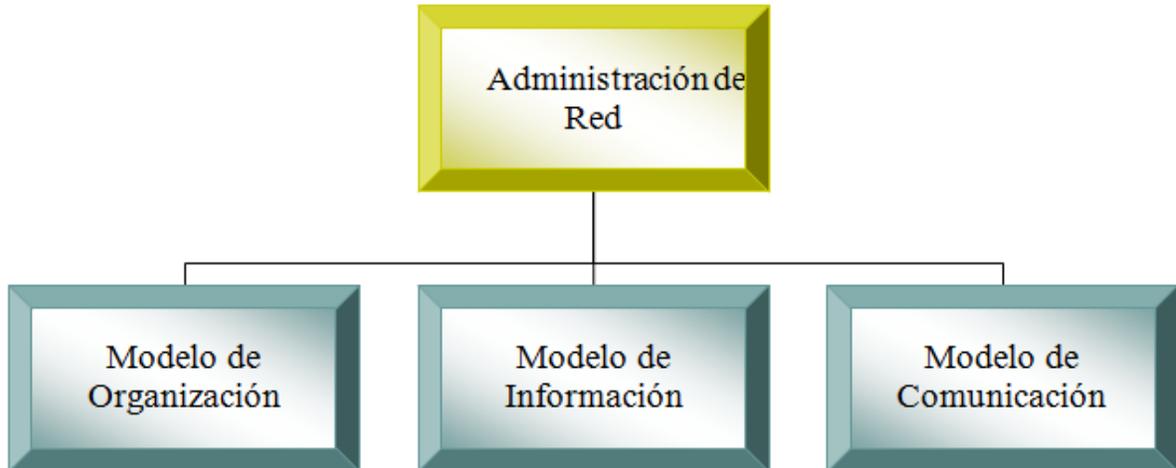


Figura 3.3 Modelo de Administración de Redes, propuesto por la OSI.

- a) **Modelo de organización:** está encargado de la descripción de los componentes de la administración de la red, esto es: el administrador, el agente, etcétera, junto con sus relaciones. La forma en cómo estos componentes interactúan da lugar a diferentes arquitecturas.
- b) **Modelo de información:** es el encargado de la estructura y el almacenamiento de la información de administración de los objetos de la red, la cual se almacena en una base de datos llamada MIB (Management Information Base - Base de Información de Administración).
- c) **Modelo de comunicación:** se encarga de verificar la forma en que se comunican los datos de administración entre el agente y el proceso administrador. Abarca los protocolos de transporte y aplicación junto con los comandos y respuestas.
- d) **Modelo de funcionalidad:** es quien direcciona las aplicaciones de administración de red, que se encuentra en el NMS (Network Management System - Sistema de Administración de la Red).

Se encarga de permitir la interoperabilidad entre las distintas plataformas de redes y los estándares de administración de redes, esto ha obligado a los fabricantes de los dispositivos de red a adaptarse a ellos.

3.2 Modelo TMN

“Una TMN (Telecommunications Management Network – Administración de Redes de Telecomunicaciones) es conceptualmente una red separada que hace interfaz con una red de telecomunicaciones en varios puntos diferentes”

29

Existieron dos motivaciones básicas para el desarrollo de la arquitectura TMN:

- Una es la creciente heterogeneidad en la tecnología para la construcción de redes de telecomunicaciones y la coexistencia de redes analógico-digitales.
- Otra deriva de las mayores demandas:
 - ✓ Posibilidad de introducir nuevos servicios.
 - ✓ Alta calidad de servicios.
 - ✓ Posibilidad de reorganizar las redes.
 - ✓ Métodos eficientes de trabajo para operar.
 - ✓ Las redes y competencia entre empresas privadas.

Antecedentes

El estudio del concepto de TMN comenzó en 1985 por la ITU (International Telecommunications Union - Unión Internacional de Telecomunicaciones), mediante el estudio para desarrollar una manera más comprensiva y estandarizada para mejorar los elementos de una red mediante un sistema de gestión de red. Como resultado formal de este proceso se obtuvo la recomendación M.30, la cual se publicó en 1988.

M.30 resume los principios fundamentales de TMN. Más tarde, se introdujeron varias versiones y la recomendación M.30 fue sustituida por la recomendación M.3010 en 1991. La primera recomendación definiendo los principios fundamentales fue seguida por varias otras tratando cada aspecto importante de TMN, tal como modelos de gestión de red, funciones de gestión de red, protocolos e interfaces estándares, la manera de gestionar arquitecturas estándar de red (por ejemplo, SDH), interconexión de redes, sistemas de gestión de redes, etcétera.

Objetivos

TMN persigue fundamentalmente dos objetivos principales:

²⁹ http://www.eie.fceia.unr.edu.ar/ftp/Tecnologias%20de%20banda%20angosta/Notas_sobre_TMN.pdf

- Proporcionar funciones de gestión y comunicaciones para la operación, administración y mantenimiento de una red de telecomunicaciones y aprovisionamiento de sus servicios en un entorno de múltiples fabricantes.
- Proporcionar una estructura de red organizada para conseguir interconexión usando una arquitectura estándar e interfaces normalizadas.

3.2.1 Funciones y Arquitectura de una TMN

Las funciones y la arquitectura de una TMN pueden ser consideradas en varias dimensiones. Cada dimensión está definida por estándares existentes o en desarrollo. Las recomendaciones M.3010 de la ITU-T tratan:

- Funciones asociadas con TMN.
- Aspecto de arquitecturas TMN.
- Arquitectura lógica estratificada de TMN.

Las funciones asociadas con una TMN están clasificadas en términos de la gestión OSI; concordantemente, se definen cinco áreas funcionales, las cuales son: bloque de función de sistemas de operaciones (Operations System Function: OSF), bloque de función de elemento de red (Network Element Function: NEF), bloque de función de estación de trabajo (Workstation Function: WSF), bloque de función de mediación (Mediation Function: MF) y bloque de función de adaptador Q (Q Adaptor Function: QAF). Dichos bloques se definen más adelante (ver figura 3.5). Éstos representan las funciones apropiadas requeridas por TMN para cumplir su función general de gestión de red. Dichas funciones son realmente ejecutadas por elementos de la arquitectura física de TMN. De acuerdo con la recomendación M. 3919, algunos de los bloques de función están parcialmente dentro y parcialmente fuera de TMN, esos bloques de función son el bloque de función workstation (estación de trabajo), el bloque de función Q adaptador (adaptador Q), y el bloque de función network element (elemento de red). Esto significa que los bloques de función (además de aquellas funciones definidas por la recomendación M. 3010) pueden incluir un rango de funcionalidad (y preverlas por parte de TMN) no cubierto por las recomendaciones TMN.

En lo que respecta a la arquitectura general de TMN, se consideran tres aspectos básicos en ITU-T M.3010:

1. **Arquitectura funcional de TMN:** bloques funcionales y puntos de referencia entre ellos. Cada uno de los cuales recoge un subconjunto de las funcionalidades

necesarias (orientado a los requisitos de operadores de red) para que TMN pueda cumplir los objetivos de gestión para los que fue concebida.

- 2. Arquitectura de información de TMN:** definición de la información que se transmite entre los bloques funcionales.
- 3. Arquitectura física de TMN:** estructura y entidades (elementos e interfaces) de la TMN. Muestra cómo los bloques funcionales de la Arquitectura Funcional se pueden implementar en diversos equipos físicos (building blocks en terminología TMN) interconectados entre sí a través de interfaces (implementación de los correspondientes puntos de referencia de la Arquitectura Funcional).

La TMN define la relación entre los bloques funcionales básicos constituyentes de la red a través de interfaces estándares. Introduce el concepto de control de subred y es tratada como una sola entidad por la aplicación de gestión. (Ver figura 3.4)

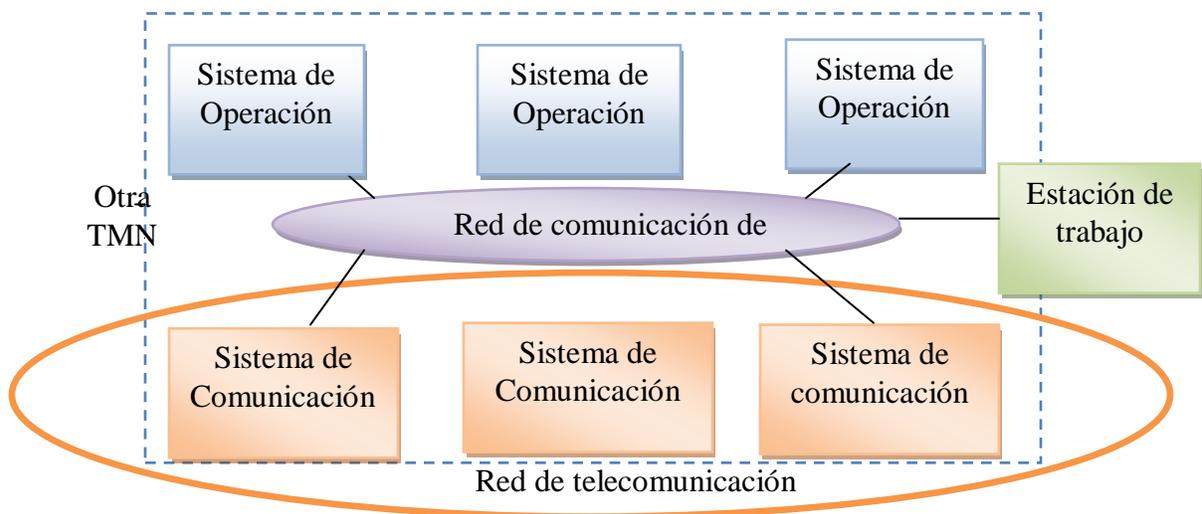


Figura 3.4 Relación entre bloques funcionales.

El modelo está compuesto por:

- Arquitectura funcional que describe un número de funciones de gestión.
- Arquitectura física que define cómo las funciones de gestión pueden implementarse en equipos físicos.
- Arquitectura de información que describe conceptos que han sido adoptados de la gestión del modelo OSI.

- Arquitectura lógica por niveles, que incluye una de las mejores ideas de TMN: un modelo que presenta cómo puede estructurarse la gestión de acuerdo con diferentes responsabilidades.

a) Arquitectura funcional

La arquitectura funcional de TMN está basada en un número de bloques de función TMN. Éstos representan las funciones apropiadas requeridas por TMN para cumplir su función general de gestión de red. Éstas son realmente ejecutadas por elementos de la arquitectura física de TMN.

De acuerdo con la recomendación M.3010 algunos de los bloques de función están parcialmente dentro y parcialmente fuera de TMN. Esos bloques de función son el bloque de función workstation (estación de trabajo), el bloque de función Q adaptador (adaptador Q), y el bloque de función network element (elemento de red). Lo cual quiere decir que estos bloques de función (además de aquellas funciones definidas por la recomendación M.3010) pueden incluir un rango de funcionalidad no cubierto por las recomendaciones TMN y proveerlo por parte de TMN.

La recomendación M.3010 define cinco bloques de función (ver figura 3.5):

1. Bloque de función de sistemas de operaciones (Operations System Function: OSF).
2. Bloque de función de elemento de red (Network Element Function: NEF).
3. Bloque de función de estación de trabajo (Workstation Function: WSF).
4. Bloque de función de mediación (Mediation Function: MF).
5. Bloque de función de adaptador Q (Q Adaptor Function: QAF).

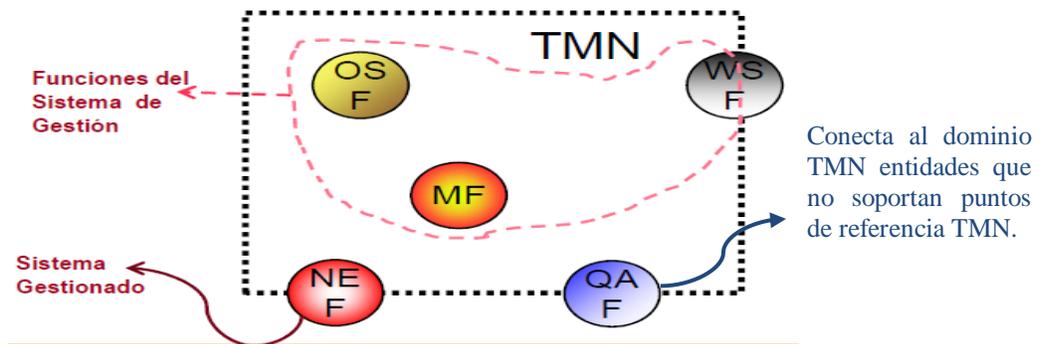


Figura 3.5 Elementos de TMN³⁰.

³⁰ Marcano. H. (s.f.). Modelo TMN. Extraído el 16 de abril de 2012 desde <http://www.slideshare.net/ronaldlopez/modelo-tmn>

Los requerimientos de comunicación de datos de estos bloques de función son satisfechos por la función de comunicación de datos (Data Communication Function: DCF) (ver tabla 3.2)

Tabla 3.2 Función de los bloques de la arquitectura funcional TMN.

Bloque	Función
OSF	Procesa información relacionada a la gestión de telecomunicaciones con el propósito de monitorear/coordinar y/o controlar funciones de telecomunicaciones incluyendo funciones de gestión.
NEF	Se comunica con la TMN con el propósito de ser monitoreado y/o controlado. También incluye funciones de telecomunicaciones que son materia de gestión, pero no son parte de la TMN. Estas funciones están representadas por la TMN por el NEF.
WSF	Provee los medios para interpretar la información de TMN por parte del usuario y viceversa. Partes de WSF pueden también estar ubicadas fuera del campo de TMN.
MF	Actúa sobre la información transferida entre un OSF y un NEF QAF para asegurar que la información entre un bloque de función TMN-compatible y un bloque de función no-TMN-compatible será traducida por la QAF. Una parte dada de las funciones del QAF está definitivamente fuera de la MTN.
QAF	Definen funciones que permiten incorporar a la red de administración TMN, entidades.

Cada uno de los bloques de función antes mencionados está formado de componentes funcionales básicos, los cuales han sido identificados como bloques elementales de construcción de la TMN.

DCF se aplica a transferir información entre los bloques de función TMN. Cada par de bloques funcionales de TMN que intercambian información de gestión están separados por puntos de referencia, esto es, los puntos de referencia son fronteras entre dos bloques de función de gestión.

b) Arquitectura física

La arquitectura física de TMN describe los bloques de construcción física (elementos físicos) de un sistema de gestión de red TMN y contiene reglas exactas para sus relaciones. El estándar relacionado es la recomendación CCITT/ITU-T M.3010.

La M.3010 define los elementos físicos de TMN como sigue:

- Sistema de operaciones (Operations System: OS).
- Estación de trabajo (Workstation: WS).
- Elemento de red (Network Element: NE).
- Red de comunicación de datos (Data Communication Network: DCN).
- Dispositivo de mediación (Mediation Device: MD).
- Adaptador Q (Q Adaptador: QA).

El OS ejecuta funciones del sistema de operaciones (OSFs). Éste prácticamente es el corazón en sí mismo, es responsable por la gestión de la red controlando la operación de sus elementos. En lo que a su realización respecta, el OS está básicamente constituido por uno o más centros de procesamiento, ejecutando la tarea de juntar información desde los elementos de red y procesándola de acuerdo con las funciones del sistema de gestión de red. Basado en el principio de división de tareas, ellos pueden ejecutar un set predefinido de tareas y estar interactuando a través de la red de comunicación de datos. La WS ejecuta funciones de workstation (WSFs). Ellas son la representación física de las interfaces hombre-máquina necesarias por medio de las cuales los operadores pueden comunicarse con la TMN.

Las workstations son preferiblemente computadoras en sí mismas, equipadas con capacidades gráficas eficientes a efectos de ser capaces de satisfacer los requerimientos de los operadores. Los NEs ejecutan funciones de elemento de red (NEFs). Los NEs son básicamente dispositivos de telecomunicaciones gestionables ubicados en los nodos de la red a ser gestionada. Ellos proveen las funciones adecuadas en la operación de red, y usualmente pueden ser identificados con una dirección simple por el sistema de operaciones de la TMN. Las partes de equipamiento que constituyen los elementos de red son dispositivos inteligentes controlados por sus propias microcomputadoras y equipados con interfaces estándares.

La DCN es una red que ejecuta la función de comunicación de datos (DCF). Ésta transmite mensajes requeridos para ejecutar funciones de gestión entre el OS y los NEs. La información es intercambiada a través de la DCN, usando protocolos estándares según lo establecido por las interfaces estándares.

Los dispositivos de mediación (MD) ejecutan funciones de mediación (MFs). Ellos pueden adaptar la información transferida entre el OS o el DCN y aquellos elementos TMN-compatibles ubicados en la red, la cual aún requiere operaciones apropiadas (almacenamiento, adaptación, filtrado, etcétera) a ser ejecutadas sobre los datos intercambiados.

Los QAs ejecutan funciones de adaptador Q (QAFs). Ellos logran el intercambio de información entre el OS o la DCN, aplicando protocolos estándares, y los eventuales NEs no-estándares ubicados en la red.

c) Arquitectura de información

Las características generales del modelo de información de TMN son discutidas por las recomendaciones M.3010 y M.3100 de CCITT/ITU-T. Esencialmente, la gestión de red involucra el intercambio de información entre procesos de gestión. El modelo de información de gestión de red TMN se soporta, en gran medida, sobre el modelo de gestión de red OSI/CMIP, la arquitectura de información orientado a transacción, y utiliza el principio así llamado de agent/manager (agente/gestor).

Los conceptos básicos usados en la definición de la arquitectura de información de TMN son similares a aquellos aplicados en SNMP y OSI/CMIP, ellos son:

- Objeto gestionado (Management Object: MO).
- Agente (Agent).
- Gestor (Manager).
- Base de Información de Gestión (Management Information Base: MIB).

Los MOs son abstracciones de los recursos físicos o lógicos a ser gestionados en orden a monitorear la operación de la red y a prevenir desórdenes en la operación de la red. Un objeto gestionado generalmente no se corresponde a un simple elemento de red según se definió como parte de la arquitectura física. En la mayoría de los casos, un objeto gestionado representa uno de los componentes de un elemento de red físico.

Un gestor es un elemento de sistema cuya tarea es enviar requerimientos de gestión hacia los agentes para propósitos de control, coordinación y monitoreo, ejecutando operaciones sobre los agentes con la ayuda de esos requerimientos y la recepción de mensajes emitidos por los objetos gestionados y retransmitidos por los agentes del gestor.

Un agente es un elemento de sistema hacia el cual se dirigen los comandos de gestión para propósitos de control, coordinación, y monitoreo. Los agentes ejecutan operaciones sobre los objetos gestionados de acuerdo con los requerimientos del gestor y retransmiten mensajes emitidos por los objetos gestionados hacia el gestor.

La base de información de gestión es una base de datos que contiene datos pertenecientes a los objetos gestionados del sistema. Similar al concepto aplicado en el caso de SNMP y

OSI/CMIP, cada uno de los agentes tiene su propia MIB, el gestor está en comando de un súper set de MIBs de agentes.

d) Arquitectura Lógica por Niveles de TMN

De acuerdo con la terminología TMN, las OSFs de la gestión de red están separadas en cuatro capas jerárquicas. Cada capa de la jerarquía dada define un grupo apropiado de operaciones de gestión. Estas capas son construidas una sobre otra, ellas y sus operaciones apropiadas están muy interrelacionadas. (Ver figura 3.6)

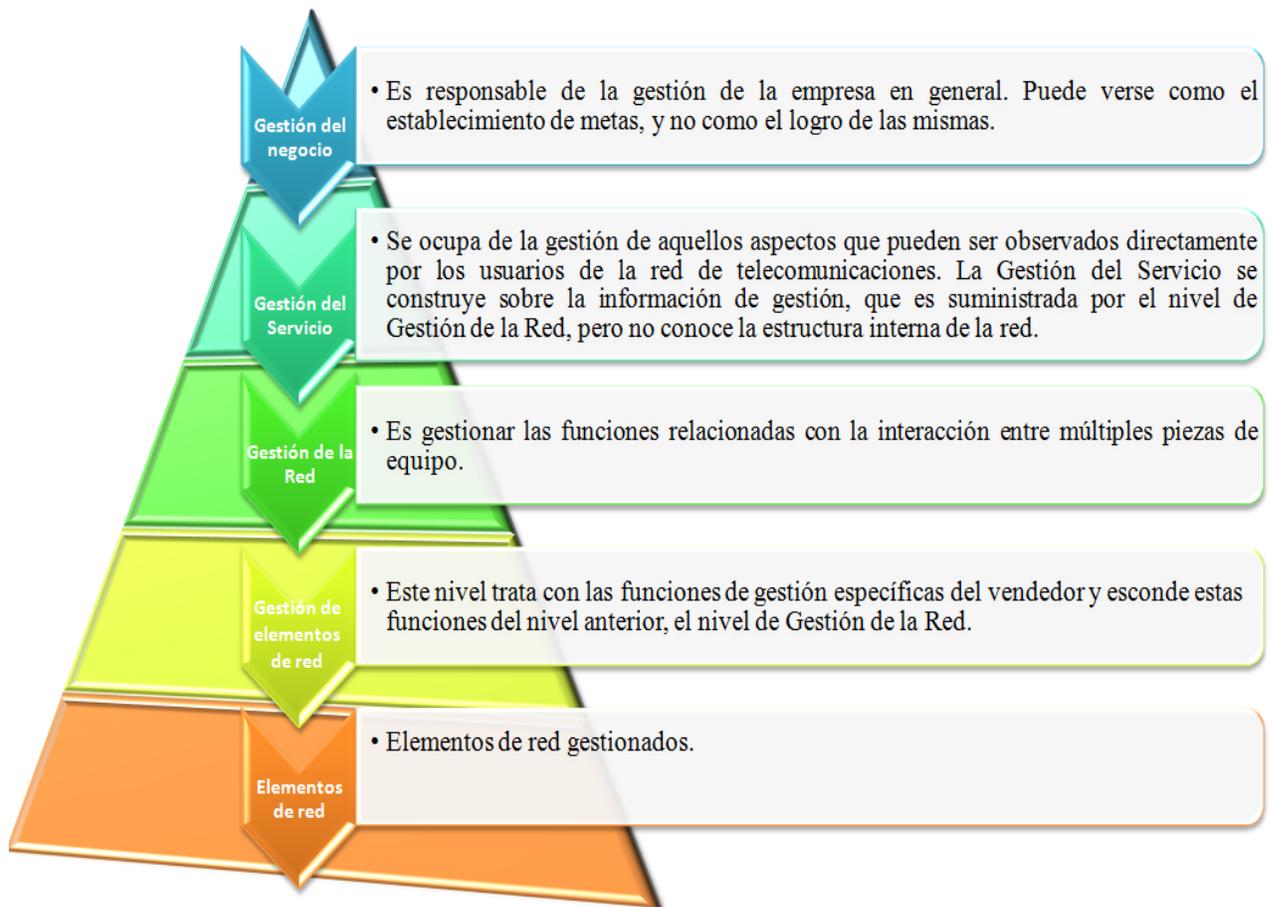


Figura 3.6 Arquitectura Lógica de TMN.

3.3 Modelo TOM

El Mapa de operaciones de Telecomunicaciones, por sus siglas en inglés, Telecommunication Operations Map, fue desarrollado entre 1995 y 1998 por la organización TMF (Telemanagement Forum), la cual es una organización fundada en 1988 por un grupo pequeño de empresas proveedoras de servicios de telecomunicaciones y por empresas

desarrolladoras de aplicaciones para automatizar los procesos de esta industria. Con el fin de ayudar a los prestadores de servicios de telecomunicaciones a automatizar sus procesos de negocio en una forma eficiente, por ello, se creó un consorcio de empresas internacionales de comunicaciones, entre cuyos objetivos se incluyen:

- Establecer una guía operacional de los procesos del negocio.
- Determinar el tipo de información que debe fluir entre procesos.
- Identificar un ambiente realista que soporte la interconexión de sistemas de soporte.
- Propender por el desarrollo de un mercado y productos para integrar y automatizar procesos de telecomunicaciones.

Así el modelo TOM Se desarrolló con el propósito de sustituir al modelo Telecommunications Management Network (TMN) para cumplir con los objetivos antes mencionados.

Estructura

En el modelo TOM se agrupan las funciones de gestión de un operador de telecomunicaciones en cajas, las que representan agrupamientos de actividades afines. Sobre este escenario de capas lógicas y cajas funcionales se mapean los diferentes procesos que conforman la operación de gestión. (Figura 3.7)

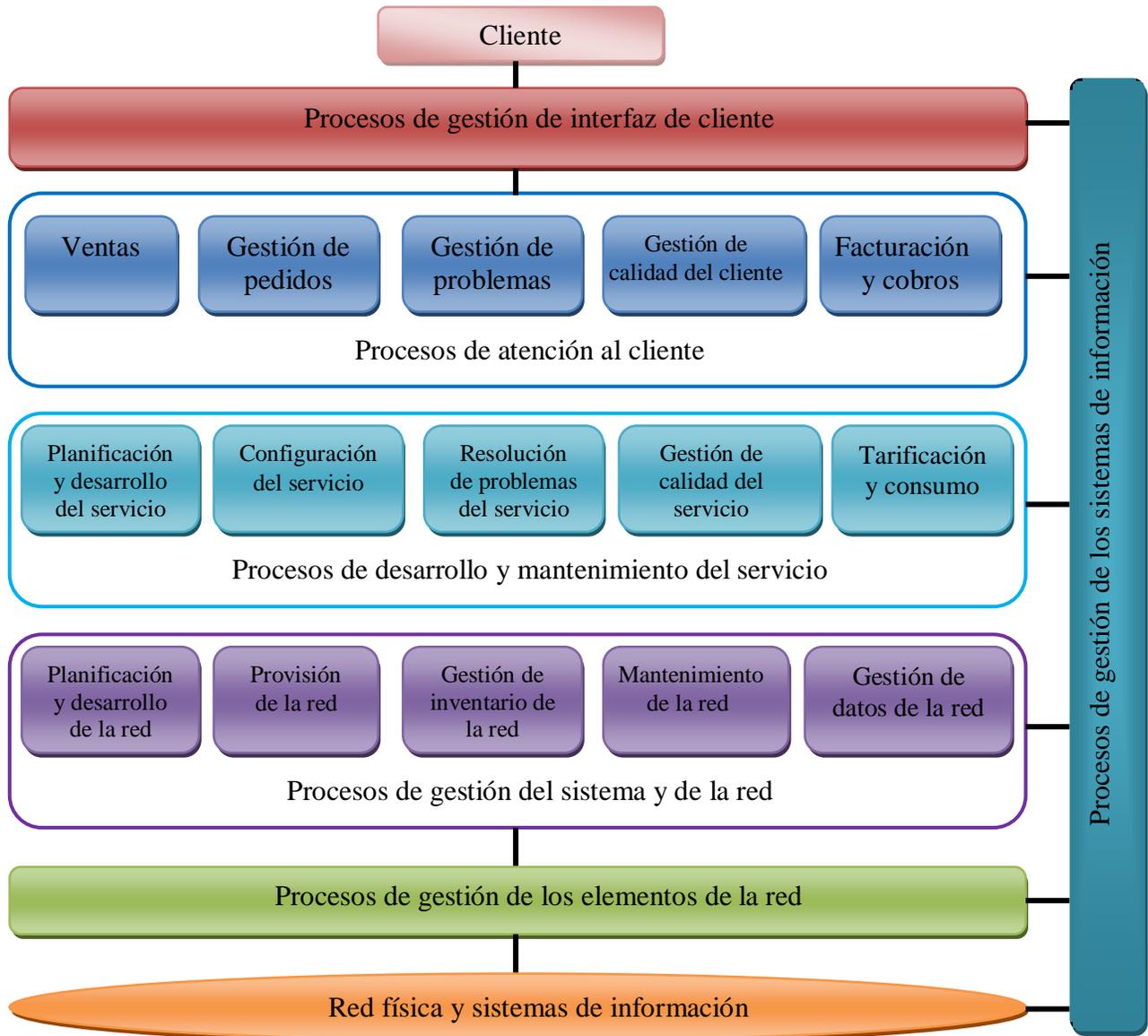


Figura 3.7 Diagrama del modelo TOM.

3.4 Modelo eTOM

El Mapa de Operaciones de Telecomunicaciones Mejorado, eTOM, por sus siglas en inglés, Enhanced Telecommunication Operations Map, es un modelo que sirve como marco de referencia de procesos de negocio orientado al sector de las telecomunicaciones. Describe y analiza todos los procesos empresariales necesarios para el funcionamiento de una empresa.

Tiene como objetivo analizar los procesos existentes en una organización y también desarrollar nuevos procesos.

Se plantea la necesidad de identificar, controlar y mantener todos los componentes de las tecnologías de la información.

Surge gracias a las mejoras que se le hacen al modelo TOM, es por ello que la letra “e”, que significa enhanced, se le asigna para diferenciarlo del marco original TOM. Estas mejoras son desarrolladas también por la TMF, en el año 2001.

Estructura

El modelo comienza a nivel empresarial, definiendo procesos de negocio y presentándolos en áreas. A nivel conceptual presenta tres áreas principales de procesos: (ver figura 3.8)

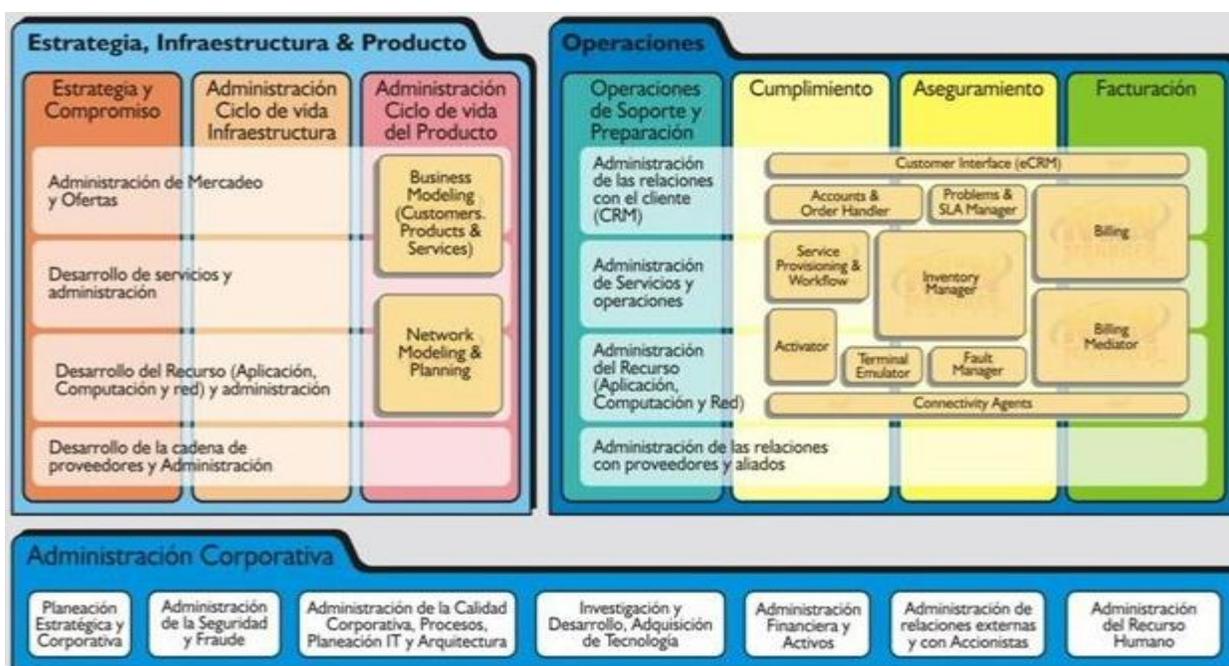


Figura 3.8 Diagrama del modelo eTOM³¹.

1. Estrategia, Infraestructura y producto: cubre la gestión de planificación y de los ciclos de vida. El objetivo son los procesos relacionados con la planificación.
2. Operaciones: se ocupa del núcleo de la gestión de operaciones.
3. Administración corporativa: se ocupa del soporte al negocio. Aquí se concentran los procesos que toda empresa debe tener para su normal funcionamiento.

³¹ IP Total software. *Modelo eTOM*. (s.f.). Extraído el 16 de abril de 2012 desde http://www.iptotal.com/s_etom.html.

Como se puede observar en el diagrama, en las áreas de Operaciones y Estrategia, Infraestructura y Productos, existen divisiones verticales y horizontales: las verticales representan flujos de procesos de extremo a extremo pasando por las capas horizontales de Interfaz con el cliente, servicios, recursos e interfaz con los socios y proveedores.

A continuación se describen detalladamente cada una de las áreas del modelo eTOM:

Las secciones verticales del área de Estrategia, Infraestructura y Producto, en general se encargan de dirigir y soportar la provisión de productos a los clientes. Su misión es el cumplimiento de las expectativas del cliente.

Cada una de sus secciones verticales se describe en la tabla 3.3:

Tabla 3.3 Descripción de las secciones verticales del área Estrategia, Infraestructura y Producto del modelo eTOM.

Nombre	Descripción
1. Estrategia y compromiso	Estos procesos proveen el enfoque dentro de la empresa para la generación de estrategias de negocio específicas así como el compromiso que éstas requieran. Haciendo partícipes desde el mercado, clientes y productos hasta la vinculación de proveedores.
2. Administración del ciclo de vida de infraestructura	Se encarga de planear e implementar las infraestructuras necesarias para el negocio. Dentro de sus tareas también se encuentran: identificar nuevos requerimientos y nuevas capacidades y a su vez diseñar y desarrollar infraestructura nueva o mejorada para soportar dichos requerimientos.
3. Administración del ciclo de vida del producto	Es responsable por la definición, planeación e implementación de todos los productos del portafolio de la empresa. Basándose en el ambiente del negocio, los requerimientos de los clientes y las ofertas competitivas.

Las cuatro secciones de procesos funcionales de soporte se representan en niveles horizontales dentro del área de Estrategia, Infraestructura y Producto, las cuales se describen en la tabla 3.4:

Tabla 3.4 Descripción de las secciones horizontales del área Estrategia, Infraestructura y Producto del modelo eTOM.

Nombre	Descripción
1. Administración de mercado y ofertas	Incluyen los procesos que involucran las ventas, administración de mercadeo, productos y ofertas. Así como la administración de las relaciones con los clientes.
2. Desarrollo de servicios y administración.	Incluyen los procesos que involucran el desarrollo de servicios y su configuración, la administración de problemas de servicios y el análisis de calidad de los mismos así como de su tarificación.
3. Desarrollo del recurso (aplicación, computación y administración)	Incluyen todo lo que tiene que ver con el desarrollo y la administración de la infraestructura de la empresa, ya sea relacionada con los productos y servicios, o bien, con el soporte de la empresa.
4. Desarrollo de la cadena de proveedores y administración	Incluyen lo relacionado con la interacción de la empresa con sus proveedores.

El área de Operaciones contiene las secciones verticales de los procesos directos de operaciones de Cumplimiento, Aseguramiento y Facturación, junto con la sección de los procesos de Soporte y Preparación. (Tabla 3.5)

Tabla 3.5 Descripción de las secciones verticales del área de Operaciones del modelo eTOM.

Nombre	Descripción
1. Operaciones de soporte y preparación	Es responsable de soportar los procesos de Cumplimiento, Aseguramiento y Facturación.
2. Cumplimiento	Provee a los clientes los productos que requiere de manera oportuna y correcta.

<p>3. Aseguramiento</p>	<p>Se encarga de la ejecución de las actividades proactivas y reactivas de mantenimiento, para asegurar que los servicios provistos al cliente estén disponibles continuamente. Cuando se presenta un problema, informa al cliente sobre su estado y asegura la restauración y reparación de dicho problema.</p>
<p>4. Facturación</p>	<p>Produce oportuna y correctamente las facturas de los clientes, así como, seguir el procesamiento de sus pagos y el recaudo de los mismos. Maneja también las consultas de los clientes sobre facturación, provee el estado de dichas consultas y es responsable de resolver cualquier problema referente a facturación.</p>

El área de Operaciones abarca cuatro secciones horizontales: administración de las relaciones con el cliente, administración de servicios y operaciones, administración del recurso y administración de las relaciones con proveedores y aliados. (Tabla 3.6)

Tabla 3.6 Descripción de las secciones horizontales del área de Operaciones del modelo eTOM.

Nombre	Descripción
<p>1. Administración de las relaciones con el cliente (CRM)</p>	<p>Posee el conocimiento fundamental de las necesidades de los clientes e incluye todas las funcionalidades necesarias para la adquisición, ampliación y retención de una relación con un cliente. Además trata del servicio y soporte al cliente.</p>
<p>2. Administración de servicios y operaciones</p>	<p>Incluye todas las funcionalidades necesarias para la administración y las operaciones de comunicaciones y los servicios de información requeridos por el cliente.</p>
<p>3. Administración del recurso (aplicación, computación y red)</p>	<p>Tiene la responsabilidad de asegurar que la infraestructura de la red y las tecnologías de la información soporten la entrega diaria de los servicios requeridos. Asegurando así, que la infraestructura funcione sin contratiempos, sea accesible, mantenida y responda a las necesidades, de los servicios, clientes y empleados.</p>
<p>4. Administración de las relaciones con proveedores y aliados</p>	<p>Soporta los procesos de Cumplimiento, Aseguramiento y Facturación del cliente, así como la administración de calidad de los proveedores y aliados.</p>

La sección de Administración Corporativa involucra el conocimiento de las acciones y las necesidades a nivel de la empresa, al contrario que con las secciones de Estrategia, Infraestructura, Producto y Operaciones, que se enfocan más en las necesidades de los clientes.

Los procesos que la conforman se tornan necesarios para cualquier empresa, ya que se requieren para dirigir el negocio y son críticos para soportar los procesos del cliente. También establece estrategias y direcciones corporativas, y provee guías y metas para el resto del negocio.

Está compuesta por siete secciones, las cuales, se describen en la tabla 3.7:

Tabla 3.7 Descripción de las secciones del área de Administración corporativa del modelo eTOM.

Nombre	Descripción
1. Planeación estratégica y corporativa	Se enfoca en el desarrollo de estrategias y planes para la empresa con el fin de que mejore su posición financiera.
2. Administración de la seguridad y fraude	Asegura que la empresa pueda soportar sus operaciones, procesos, aplicaciones y comunicaciones de misión crítica, ante desastres, amenazas de seguridad e intentos de fraude, a través del establecimiento de las políticas de seguridad y de guías de buenas prácticas.
3. Administración de la calidad corporativa, procesos, planeación de las tecnologías de la información (TI) y arquitectura.	Se encarga de desarrollar y mejorar las arquitecturas claves de la empresa, así como, en la definición de nuevos procesos y políticas de administración de calidad de la empresa.
4. Investigación y desarrollo, adquisición de tecnología.	Desarrollan investigaciones de nuevos mercados para ampliar su cartera de clientes. Así como también adquirir diferentes productos y servicios para la empresa.
5. Administración financiera y activos	Es el responsable de la administración de las finanzas y los activos de la empresa (bienes raíces, servicios necesarios para su buen funcionamiento, etcétera).

<p>6. Administración de relaciones externas y con accionistas</p>	<p>Se dedica a la administración de las relaciones de la empresa con los grupos de interés (accionistas, organizaciones de los empleados, etcétera) sobre ella y las entidades externas (sindicatos).</p>
<p>7. Administración de recursos humanos</p>	<p>Provee la infraestructura de recursos humanos para las personas que laboran en la empresa, tales como: definición de perfiles de cargos y fortalezas de los empleados, planeación de reemplazos, capacitación, reclutamiento, contratos laborales, etcétera.</p>

Ventajas de implementar el modelo en la Administración de Redes

- Permite establecer un marco común del negocio para empresas de telecomunicaciones.
- Proporciona definiciones comunes para describir los procesos de un proveedor de servicios u operador de telecomunicaciones.
- Acuerdos en la información básica requerida para realizar cada proceso.
- Proporciona un marco de procesos que permite identificar cuales procesos e interfaces son más factibles de integrar, automatizar y estandarizar.

Desventaja de implementar el modelo en la Administración de Redes

- Es un método para el cual se necesita de mucha preparación para poder implementarlo, ya que va por varios niveles.

3.5 Definición de protocolos de administración de redes

Un protocolo de red es un conjunto de convenciones y normas para enviar y recibir información mediante una red. Tales convenciones regulan el contenido, el formato de los datos, la velocidad de envío y recepción y la gestión de errores a través de la red.

A continuación se definen tres de los protocolos más usados e importantes en la administración de redes.

a) SNMP (Simple Network Management Protocol - Protocolo Simple de Administración de Red).

El primer protocolo que se usó fue el SNMP [RFC 1157]. Fue desarrollado en los inicios del Internet por el Internet Activities Board para la administración de redes TCP/IP y

originalmente como una solución a corto plazo para la problemática del monitoreo de las redes.

En los años 80 aparece el nuevo protocolo SNMP, que incorporaba muchas de las funciones del original (que sigue en uso) e incluía nuevas características que mejoraban sus deficiencias. Es un protocolo de la capa de aplicación que forma parte del conjunto de protocolos TCP/IP de Internet y por su amplia utilización en redes empresariales es considerado el estándar de facto en detrimento del protocolo CMIP de la familia de protocolos OSI, más utilizado en las grandes redes de las operadoras de telecomunicación.

SNMP siguió evolucionando, dando lugar en 1993 a SNMPv2, que define un mayor número de operaciones de protocolos, un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció SNMPv2c, que añade como mejoras una configuración más sencilla y una mayor modularidad. La última versión, SNMPv3, surgió en 1997 para reforzar las prestaciones de seguridad (incluyendo autenticación, privacidad y control de acceso) y de administración de protocolo (con una mayor modularidad y la posibilidad de configuración remota). Cabe destacar que SNMPv3 no reemplaza a SNMPv1 o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con ambas versiones.

Características

- Es un protocolo de gran flexibilidad y que permite una gran extensibilidad a todo tipo de redes.
- El gestor pregunta periódicamente a la información del agente sobre los recursos gestionamos, es el gestor el responsable de monitorear los recursos.
- Al ser un protocolo basado en UDP/IP no garantiza la llegada de los mensajes.
- El programa cliente (llamado el gestor de red) realiza conexiones virtuales a un programa servidor (llamado el agente SNMP).
- Ejecutado en un dispositivo de red remoto. La base de datos controlada por el agente SNMP se denomina Management Information Base (MIB), y es un conjunto estándar de valores estadísticos y de control de status.
- Los mensajes enviados por el cliente (gestor de red) a los agentes SNMP están formados de identificadores de objetos MIB, junto con instrucciones a fin de cambiar u obtener un valor.

- Es independiente del protocolo, aunque la mayor parte de las instalaciones SNMP, se utilicen en redes TCP/IP.
- Se emplea el puerto 161 para enviar y recibir mensajes, los mensajes trap enviados por los agentes son recibidos en el puerto 162.

Arquitectura de SNMP

Implícita en el modelo de arquitectura del SNMP existe una colección de estaciones de gestión de red y de elementos de red. Las estaciones ejecutan aplicaciones de administración que monitorizan y controlan los elementos de red. Los elementos de red son dispositivos como hosts, gateways, servidores de terminal, y parecidos, que poseen agentes de gestión para realizar las funciones de administración de red solicitadas por las estaciones de gestión de red.

El SNMP es usado para transmitir información de administración entre las estaciones de gestión y los agentes en los elementos de red.

Peticiones SNMP (ver figura 3.9)

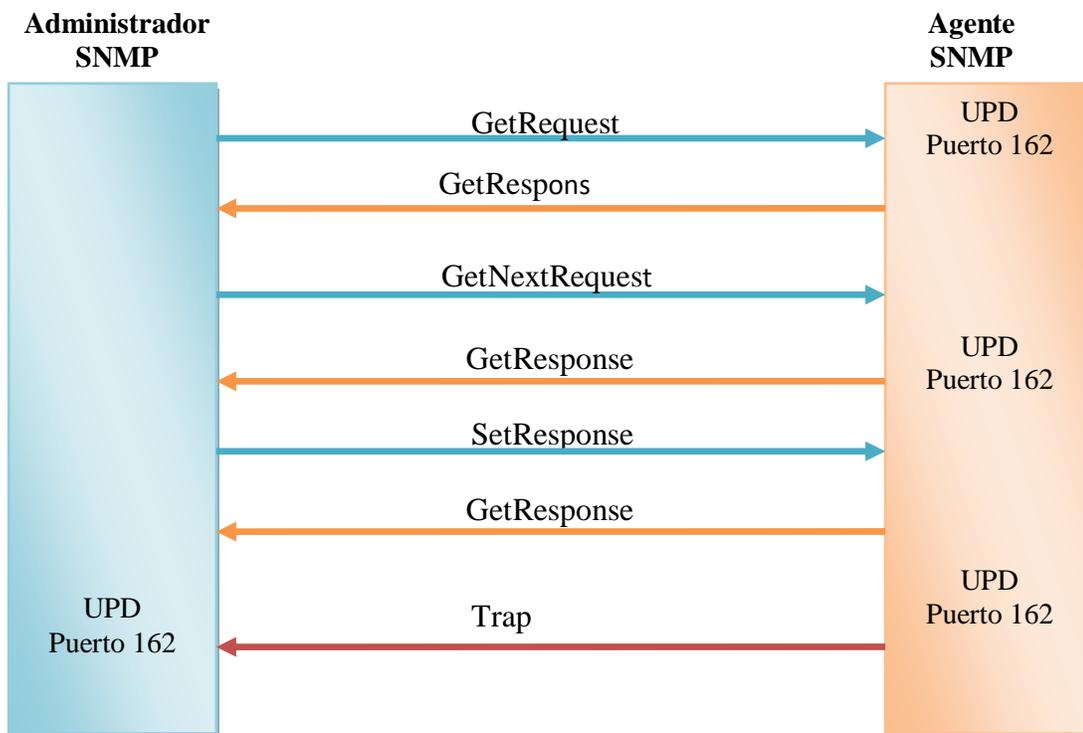


Figura 3.9 Peticiones SNMP

Ventajas

- Para los programadores de herramientas de gestión de red, la principal ventaja es su sencillez, lo cual reduce mucho los costos y tiempo de desarrollo de las aplicaciones, así como de su posterior actualización.
- SNMP opera sobre varios protocolos de transporte, como: UDP, OSI CLNS, AppleTalk DDP y Novell IPX.
- SNMP cuenta con el soporte de varias plataformas comerciales de gestión de red multifabricantes, como OpenView de HP, SunNet de Sun Microsystems o NetView de IBM.
- Es un estándar de mercado.
- Modelo útil para el acceso a datos de gestión de la red.
- Acceso y organización eficientes de los datos gestionados.
- Independencia del entorno de comunicaciones.

Desventajas

- Consume más ancho de banda que CMIP en entornos de red extendidos, ya que trabaja mediante sondeo secuencial en vez de en modo conectado, lo cual impide optimizar el tráfico.
- En su versión original, tampoco permite transferir eficientemente grandes cantidades de datos.
- Tiene una altísima vulnerabilidad a varias cuestiones de seguridad, por ejemplo, modificación de información, alteración de la secuencia de mensajes o enmascaramiento de la entidad emisora, entre otras.
- En su versión original, cada gestor y agente es configurado con un nombre de comunidad que es una cadena de texto plano.
- Limitaciones en el mecanismo de obtención de información.
- Limitaciones de las capacidades del modelado de datos: MIB estática, correlación de datos difícil, Modelados de sistemas complejos.

b) CMIP (Common Management Information Protocol - Protocolo de administración de información común)

Alternativamente también se desarrolló el CMIP como parte de los trabajos de la Organización Internacional de Estándares (OSI) y el Comité Consultivo Internacional de Telefonía y Telecomunicaciones (CCITT). Este protocolo se desarrolló como una solución a largo plazo, sin embargo, debido a la facilidad y a la velocidad en la que el SNMP fue primero implementado, además de algunas otras diferencias, el desarrollo del CMIP se considera separado del desarrollo del SNMP.

CMIP [RFC 1189] fue diseñado teniendo en cuenta a SNMP, solucionando los errores y fallos que tenía SNMP y volviéndose un gestor de red mayor y más detallado. Su diseño es similar a SNMP por lo que se usan PDUs (Protocol Data Unit) como variables para monitorear la red.

La serie CMIP está compuesta por seis protocolos que se esquematizan en la tabla 3.8:

Tabla 3.8 Protocolos de la serie CMIP.

Procesos de Gestión de Aplicaciones	
CMISE	
ISO 9595/9596	
ACSE ISO 8649/8650	ROSE ISO DIS 9072-1/2
ISO Presentación	
ISO Sesión	
ISO Transporte	

Características de CMIP

- Es un protocolo de gestión de red que se implementa sobre el modelo de Interconexión de Redes Abiertas OSI que ha sido normalizado por la ISO. Trabajando sobre la capa siete (Aplicación).
- Tiene una arquitectura de gestión de red que provee un modo de que la información de control y de mantenimiento pueda ser intercambiada entre un gestor (manager) y un elemento remoto de red.

- Define una relación igual a igual entre el gestor y el agente incluyendo lo que se refiere al establecimiento y cierre de conexión, y a la dirección de la información de gestión.
- Requiere gran cantidad de memoria y capacidad de CPU.
- Genera largas cabeceras en los mensajes.
- Especificaciones difíciles de realizar y tediosas de implementar en aplicaciones.
- Comunicación con los agentes orientada a conexión.
- Estructura de funcionamiento distribuida.
- Permite jerarquía de sistemas de operación.
- Asegura que los mensajes lleguen a su destino.
- Orientado a gestión por eventos.
- El agente notifica al gestor de sucesos la información concerniente a los recursos gestionados.
- El agente es responsable de monitorear los recursos.
- Presenta la ventaja de que existe menor gestión de tráfico.
- Presenta la desventaja de tener agentes más complejos.

Arquitectura CMIP

En concreto, CMIP ofrece un mecanismo de transporte en la forma de servicio pregunta-respuesta (ver figura 3.10) para las siete capas del modelo OSI.

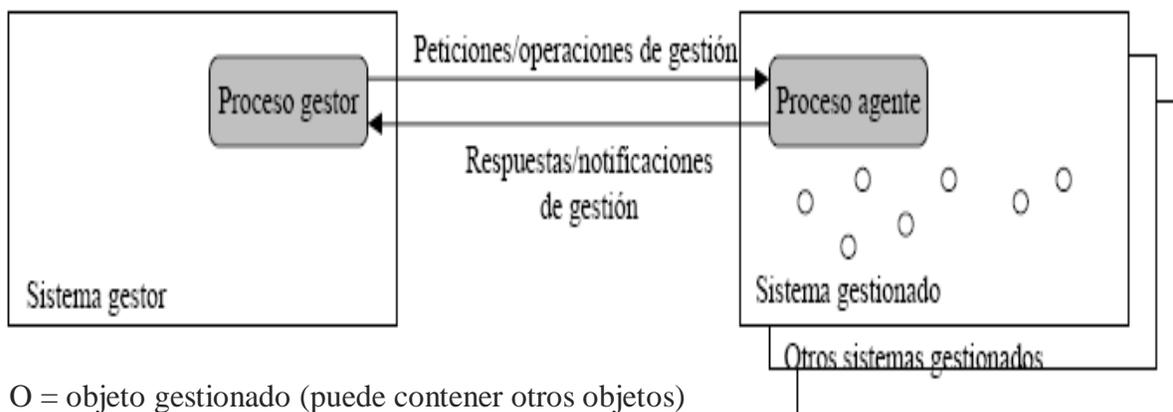


Figura 3.10 Funcionamiento de CMIP.

CMIP se encuentra formado esencialmente por los siguientes dos componentes:

1. Entidad de aplicación de gestión de sistemas (SMAE – Systems Management Application Entity):

- Entidad de nivel de aplicación responsable del intercambio de información de gestión con SMAEs de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red.
- Para esta función se utiliza un protocolo normalizado (CMIP):
 - Entidad de gestión de nivel (LME – Layer Management Entity): proporciona funciones de gestión específicas de cada capa de la torre OSI.
 - Base de información de gestión (MIB).

A su vez, la entidad de aplicación de gestión de sistemas, SMAE presenta la siguiente división:

- **De propósito general** (diseñadas para ser útiles en muchas aplicaciones):
 - **ACSE (Association Control Service Element – Elemento de Servicio de Control de Asociación):** es responsable de ejecutar la negociación inicial a efectos de decidir si se puede establecer una conexión de datos y ponerla a disposición de la comunicación. ACSE provee facilidades básicas para el control de una asociación de aplicación entre dos entidades de aplicación. ACSE incluye dos unidades funcionales opcionales. Una unidad funcional soporta el intercambio de información soportando autenticación durante el establecimiento de la asociación. La segunda unidad funcional soporta la negociación del contexto de aplicación durante el establecimiento de la asociación.
 - **ROSE (Remote Operations Service Element – Elemento de Servicio de Operación Remota):** controla y supervisa las interacciones entre entidades remotas de una aplicación, donde esas interacciones pueden ser modeladas y soportadas como operaciones remotas. Una operación remota es requerida por una entidad; la otra entidad intenta ejecutar la operación remota y luego reportar el resultado del intento.

- **Específicas para gestión de sistemas:**
 - **SMASE (System Management Application Service Element - Elemento de Servicio de Aplicación de Gestión de Sistemas):** implementa funciones básicas de gestión en las áreas de gestión de fallos, costos, configuración, prestaciones y seguridad. Proporciona servicios al gestor de red y a las aplicaciones de gestión.
 - **CMISE (Common Management Information Service Element - Elemento Común de Servicio de Información de Gestión):** es responsable por la generación de requerimientos (requests) estándares básicos y el procesamiento de mensajes de respuesta según lo definido por el CMIS.

El CMIS puede ser utilizado por un proceso de aplicación en un ambiente de gestión centralizado o descentralizado para intercambiar información y comandos para el propósito de sistemas de gestión.

A través de CMISE (Common Management Information Service Element – Información Común de Gestión de Elementos de Servicio), CMIP proporciona tres tipos de servicio:

- Manejo de datos: usado por el gestor para solicitar y alterar información de los recursos del agente.
 - Informe de sucesos: usado por el agente para informar al gestor sobre diversos sucesos de interés.
 - Control directo: usado por el gestor para solicitar la ejecución de diversas acciones en el agente.
- **FTAM (File Transfer Access and Management o Gestión y Acceso de Transferencia de Ficheros):** se encarga de organizar y gestionar el acceso a archivos para procesos de aplicaciones. Ofrece servicios de transferencia de archivos entre el cliente y el servidor.

2. CMIS (Common Management Information Services – Servicios Comunes de Información de Administración): se refiere al conjunto de servicios proporcionados por la arquitectura de administración OSI los cuales definen su implementación en el protocolo

CMIP y son invocados mediante un conjunto de instrucciones relacionadas con uno o varios objetos de la MIB como se muestra en la tabla 3.9:

Tabla 3.9 Instrucciones CMIS.

Instrucción	Descripción
M – GET	Obtiene información sobre los valores de los atributos de un objeto administrable.
M – SET	Modifica la información contenida en un objeto administrable.
M – ACTION	Invoca una operación sobre un objeto administrado.
M – CREATE	Crea la presentación de una instancia de un objeto administrado de una clase determinada.
M – DELETE	Elimina la representación de una instancia de un objeto administrado.
M – CANCEL – GET	Cancela una petición M – GET previa. La cancelación se puede deber a un excesivo consumo de tiempo por parte de un servicio GET.
M – EVENT – REPORT	Notifica un evento, como una notificación de alarma entre elementos de una red y este servicio puede ser o no confirmado.

Una vez explicados cada uno de los elementos de CMIP, se puede obtener el siguiente diagrama que muestra los distintos elementos que integran al protocolo CMIP (figura 3.11):

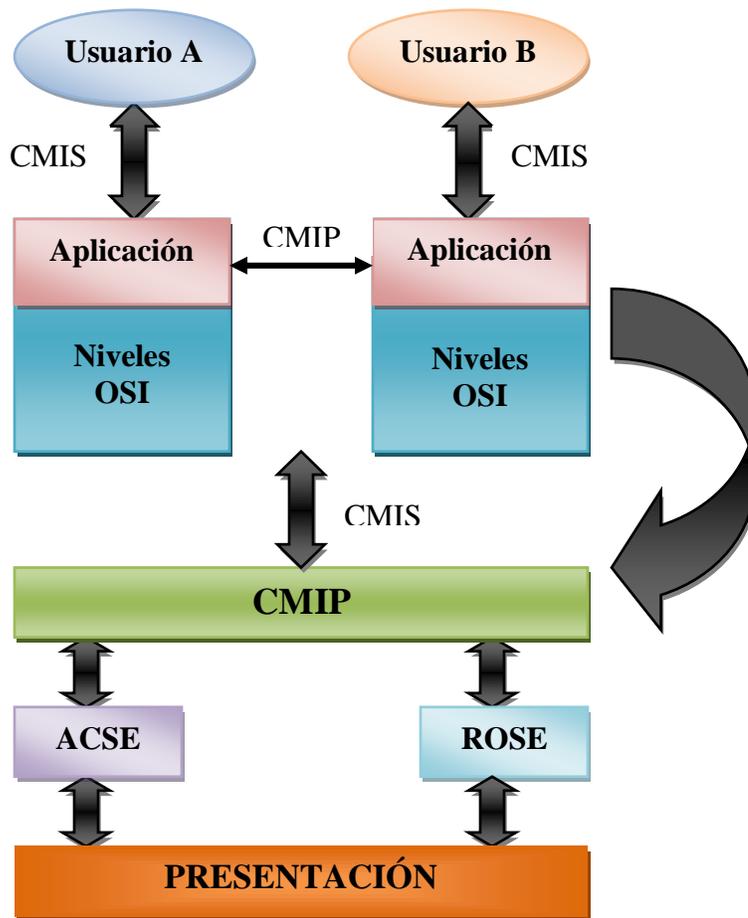


Figura 3.11 Protocolos que integran a CMIP.

El protocolo de séptima capa (aplicación) utilizado por la gestión OSI es el protocolo común de información de gestión (Common Management Information Protocol: CMIP). En un ambiente de gestión basado en el modelo OSI/CMIP, el proceso de aplicación de usuario (cuya operación está basada en el principio de manager/agent) es provisto con el servicio común de información de gestión (Common Management Information Service: CMIS) en función de una interface de programa de aplicación (API) por la denominada entidad de aplicación de gestión de sistemas (Systems Management Application Entity: SMAE), la cual está implementada en la séptima capa (aplicación) del modelo de siete capas OSI.

El modelo de administración OSI define los sistemas administrados y los sistemas de administración, éstos tienen las siguientes características:

- Cada nodo de comunicaciones debe tener una base de información de administración (MIB).
- Un Proceso de Aplicación del Sistema de Administración (SMAP – Systems Management Application Process) proporciona la interfaz con la información compartida por la MIB. Los SMAPs dialogan con otros SMAPs a través de la red.
- Una Entidad de Aplicación del Sistema de Administración (SMAE) soporta la comunicación de los SMAP y las SMAEs usan CMIP para intercambiar datos entre nodos.
- CMIP define la metodología para diseñar el sistema de administración de red y las especificaciones de la interfaz están indicadas en CMIS (Servicio de Información de Administración Común).

Ventajas

- No sólo se puede enviar información de gestión de o hacia una terminal, sino que es posible desarrollar tareas que serían imposibles bajo SNMP.
- CMIP soluciona varios de los fallos de SNMP. Por ejemplo, tiene incluidos dispositivos de gestión de la seguridad que soportan autorizaciones, control de acceso, contraseñas, como resultado de la seguridad que de por sí proporciona CMIP no necesita de posteriores actualizaciones.
- CMIP, por trabajar en modo conectado, ofrece una mayor seguridad que SNMP.

Desventajas

- Existe tal cantidad de variables en CMIP que sólo los programadores más hábiles son capaces de sacarles todo su potencial. Sus variables son demasiado complejas.
- Para el usuario de las herramientas de gestión, CMIP tiene como principal desventaja requerir unas diez veces más recursos de red (capacidad de memoria y de procesador de los routers y de los servidores del centro de gestión) que SNMP.
- La implementación de los protocolos OSI sobre routers y plataformas de gestión es muy cara. En otras palabras, muy pocas redes empresariales son capaces de soportar una implementación completa de CMIP.

c) CORBA (Common Object Request Broker Architecture - Arquitectura Común de Intermediarios en Peticiones a Objetos)

CORBA fue introducido en 1991 y estandarizado por el OMG (Object Management Group – Grupo de Gestión de Objetos), el mayor consorcio de la industria del software y define el IDL (Interface Definition Lenguaje – Lenguaje de Descripción de Interfaz) y las API (Application Programming Interfaces – Interfaz de Programación de Aplicaciones) que hacen posible la interacción entre objetos siguiendo un modelo cliente/servidor.

CORBA es, básicamente, una arquitectura de programación distribuida diseñada para soportar objetos independientemente de su ubicación dentro de una red o máquina. En este caso será la empresa que adquiera dichos gestores la encargada de realizar la integración de los productos de varios proveedores sobre una única plataforma, una tarea sumamente compleja.

Características

- La comunicación con los agentes está orientada a conexión.
- La estructura de funcionamiento es distribuida.
- El protocolo asegura que los mensajes llegan a su destino.
- El hecho de que se trate de una gestión conducida por eventos se traduce en que:
 - El agente notifica al gestor de sucesos la información concerniente a los recursos gestionados.
- El agente es responsable de monitorear los recursos.
- Existe menor gestión de tráfico.
- Presenta agentes más complejos.

- Define:
 - La interfaz de los objetos (IDL).
 - Cómo se comunican entre sí (IIOP, Internet Inter ORB Protocol – Interoperabilidad entre ORB).
 - Servicios de objeto.

- CORBA trata con Interfaces, no con la implementación de los objetos. Los programadores usan referencias a objetos remotos como si fuesen locales.
- CORBA pone el objeto a disposición de cualquier aplicación conectada al bus de objetos de forma transparente.
- Interoperatividad entre objetos heterogéneos distribuidos. (Aplicaciones distribuidas).

- Los objetos se clasifican según su naturaleza, agrupándose dentro de un ORB (Object Request Broker – Intermediario de Petición de Objetos).

Arquitectura

CORBA se encuentra formado por varios elementos principales, los cuales se explican a continuación:

- **ORB (Object Request Brokers - Intermediario de Petición de Objetos):** se trata del núcleo de cualquier implementación CORBA, transmiten los mensajes que se intercambian cliente y servidor (figura 3.12), por lo que se ocupan de:
 - Canalizar las comunicaciones entre los objetos locales y los remotos.
 - Empaquetar los parámetros que el cliente pasa al método remoto y el resultado que el método devuelve al cliente.
 - Localizar al objeto remoto a partir de una referencia.

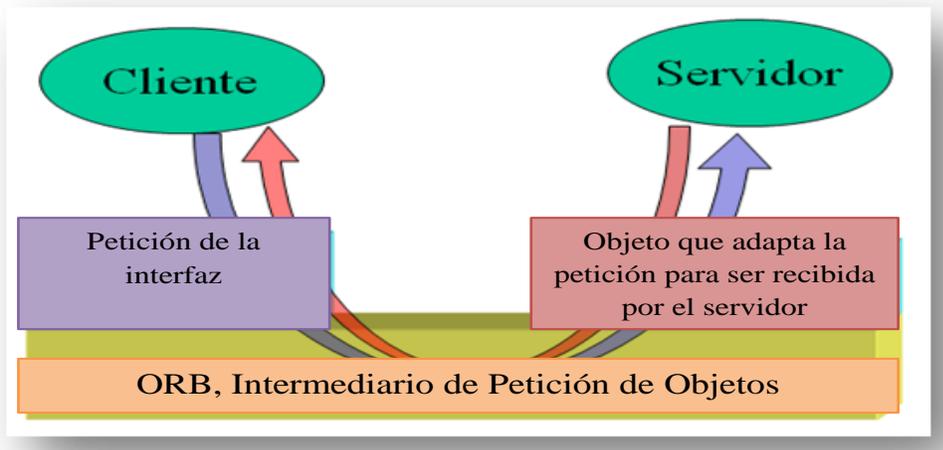


Figura 3.12 Intermediario de petición de objetos.

El ORB, Intermediario de petición de objetos proporciona varios servicios, los cuales son utilizados por las implementaciones de los objetos. Debido a que el ORB no conoce los detalles de las implementaciones fundamentales de los objetos. Un “object adapter” (El Objeto adaptador se encarga de convertir una interfaz en otra interfaz que el cliente espera, lo que permite que aunque se traten de diferentes interfaces, puedan trabajar juntas, lo que de otra manera no podría hacerlo debido a sus interfaces incompatibles) mapea modelos genéricos a implementaciones, logrando así que las implementaciones de los objetos acceden a los servicios provistos por él.

En la tabla 3.10 se mencionan y describen cada uno de los servicios que proporciona la ORB:

Tabla 3.10 Servicios provistos por el ORB

Servicio	Descripción
Object life cycle (Objeto del ciclo de vida).	Define cómo los objetos de CORBA son creados, removidos, movidos y copiados.
Naming (Nombrado).	Define cómo los objetos de CORBA pueden tener nombres simbólicos amigables.
Events (Eventos).	La comunicación entre objetos distribuidos.
Relationships (Relación).	Provee relaciones arbitrarias n-áreas entre tipos y objetos de CORBA.
Externalization (Externalización).	Coordina la transformación de objetos CORBA hacia y desde medios externos.
Transactions (Transacciones).	Coordina el acceso atómico, es decir, que solo puede acceder de un objeto CORBA a la vez.
Concurrency Control (Control de concurrencia).	Provee un servicio de bloqueo para objetos de CORBA para asegurar acceso concurrente.
Property (Propiedades).	Soporta la asociación de pares nombre-valor con objetos CORBA.
Trader (Negociación).	Soporta el encuentro de objetos CORBA basado en propiedades, describiendo el servicio ofrecido por el objeto.
Query (Consulta).	Soporta colas en objetos.

- **IDL (Interface Definition Language - Lenguaje de Descripción de Interfaz):** es un lenguaje de programación pensado exclusivamente para especificar las interfaces que usarán los clientes.

La tarea de una IDL es poner de acuerdo a distintos lenguajes en el formato y tamaño de sus especificaciones, estableciendo un contrato entre cliente y servidor indicando qué servicios van a estar accesibles para el cliente desde el servidor, (ver figura 3.13).

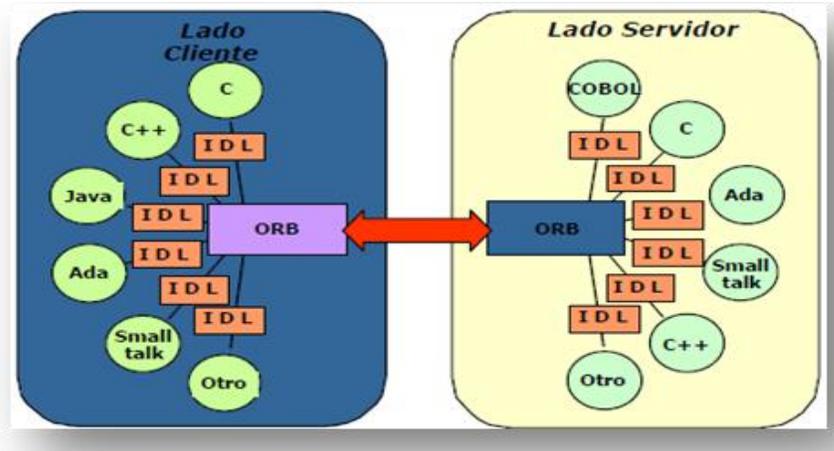


Figura 3.13 Función de una IDL.

- IIOP (Internet Inter ORB Protocol - Interoperabilidad entre ORB):** CORBA es neutral respecto al protocolo de red utilizado para comunicar al cliente con el servidor. Para ello especifica el GIOP (General Inter ORB Protocol - Protocolo Entre ORBs General) que define la comunicación entre ORBs diferentes. Para redes de tipo TCP/IP se emplea una instancia de GIOP conocida como IIOP. Gracias a la IIOP es posible que objetos que emplean ORBs de fabricantes distintos puedan interoperar en redes como Internet. (Ver figura 3.14)

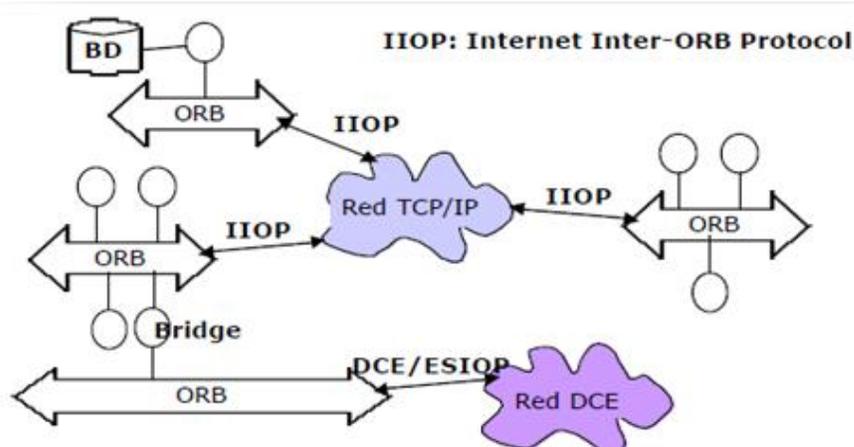


Figura 3.14 Función de la IIOP dentro de CORBA.

Una vez explicados los elementos de CORBA uno a uno, se genera el siguiente diagrama funcional con cada uno de estos elementos, permitiendo así comprender mejor el proceso que se realiza (ver figura 3.15).

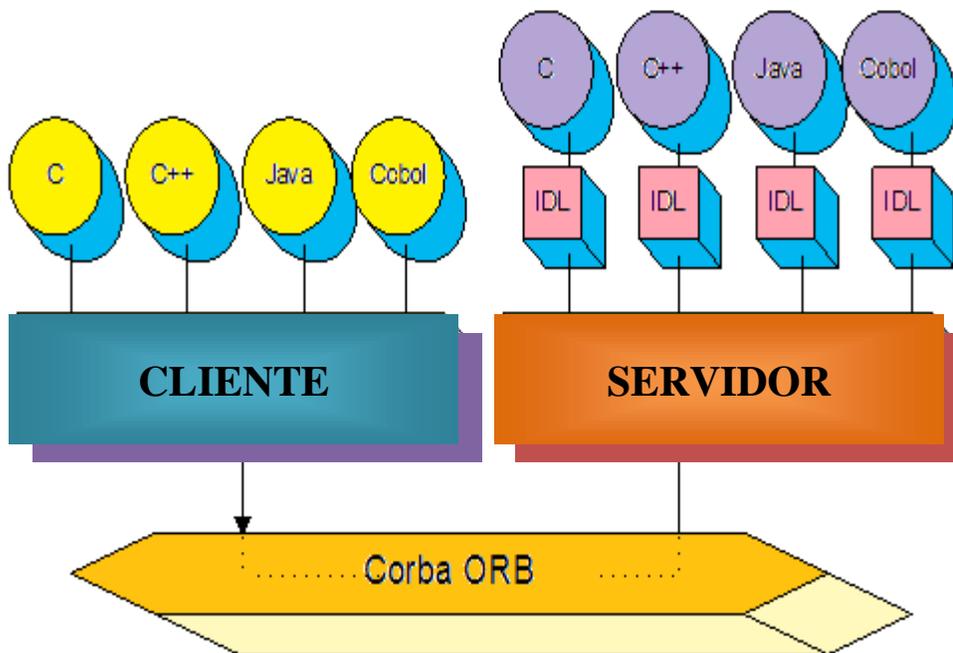


Figura 3.15 Diagrama conceptual de CORBA.

A continuación se muestra el diagrama anterior de manera desglosada (figura 3.16):

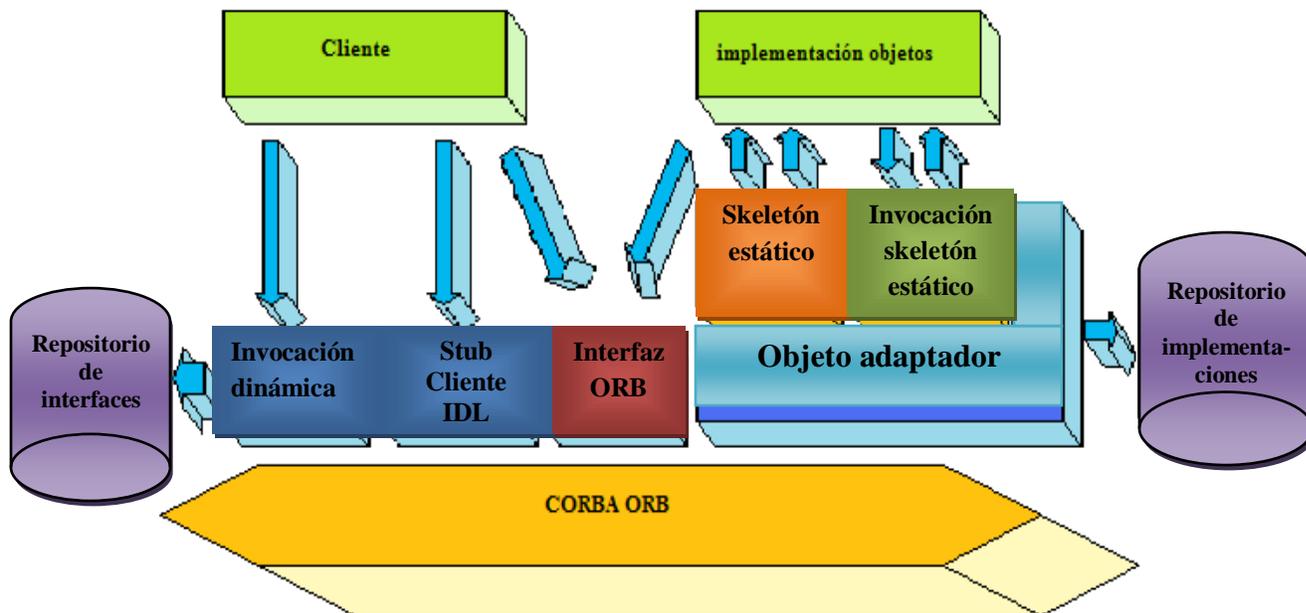


Figura 3.16 Diagrama conceptual extendido de CORBA.

Donde:

- *Skeleton*: es el elemento encargado de la comunicación con el cliente.
- *Stub cliente*: se refiere al representante local del objeto remoto y está encargado de la comunicación con el objeto remoto.

Como se observa en la figura 3.16 existe una interfaz entre aplicaciones clientes y servidoras. Un lenguaje de definición de interfaz (IDL) ha sido definido específicamente para CORBA. Cualquier objeto puede ser un cliente, un servidor o ambos. Para efectos de descripción, CORBA usa el modelo Cliente/Servidor.

Lo que en concreto realiza CORBA es especificar los servicios de middleware que serán usados por las aplicaciones (objetos).

La arquitectura de CORBA presenta algunas características, las cuales se listan a continuación:

- CORBA define una arquitectura para objetos distribuidos.
- El paradigma básico de CORBA es de una solicitud para servicios de objetos distribuidos.
- Todo lo demás definido por el OMG es en términos de este paradigma básico.
- Los servicios que un objeto provee son dados por su interface. Las interfaces son definidas en el Lenguaje de Definición de Interface (IDL) del OMG.
- Los objetos distribuidos son identificados por referencias a objetos, las cuales son definidas por las interfaces IDL.
- Un cliente tiene una referencia a un objeto distribuido. La referencia al objeto es dada por una interface.
- El ORB (Object Request Broker) envía la solicitud al objeto y regresa cualquiera de los resultados al cliente.

Ventajas

- Estandarizado, múltiples implementaciones (no se depende del fabricante).
- Las especificaciones se adoptan por consenso.
- Buena infraestructura para construir aplicaciones distribuidas.
- Permite a las aplicaciones comunicarse con otras, sin importar donde están localizadas y cómo hayan sido desarrolladas.
- Escalonado de aplicaciones, separa interfaz e implementación, además crea transparencia de localización a través del ORB :

- De objetos: la invocación siempre se hace en local.
 - De red: el ORB la gestiona.
 - De activación: los servidores se activan automáticamente.
-
- Es independiente del lenguaje: los objetos clientes y servidores se implementan en cualquier lenguaje (de los soportados).
 - Replicación de servidores.
 - Distribución de la carga computacional.
 - Transparencia en la ubicación.
 - Reutilización de código.
 - Partición de aplicaciones.
 - CORBA es más potente que SNMP y menos complejo que CMIP. A esto se añade la ventaja que supone su proximidad a C++ y Java, dos lenguajes de gran difusión.

Desventajas

- No es la tecnología más sencilla de utilizar.
- Las especificaciones tardan en desarrollarse y en consecuencia las implementaciones tardan en salir al mercado.
- Tecnología más compleja y pesada.
- Nuevos desafíos: gestión de accesos concurrentes y seguridad.
- La mayor dificultad que presenta la integración de CORBA con los sistemas tradicionales de gestión es el modelo de objetos.

CAPÍTULO 4

Integración



“Cualquier poder, si no se basa en la unión, es débil”

Jean de La Fontaine.

4.1 Definición de tecnologías de telecomunicaciones

Las tecnologías de telecomunicaciones agrupan los elementos, técnicas, conocimiento e invenciones utilizadas en el tratamiento y la transmisión de la información que hacen posible la emisión, recepción y/o transmisión de señales electromagnéticas principalmente de informática, internet y telecomunicaciones, a través de medios como ondas de radio, cables de cobre, fibra óptica, etcétera.

En este apartado se da un recorrido por estas tecnologías, describiendo su funcionamiento, características, así como ventajas y desventajas que presenta su utilización, así como también un poco de su historia.

a) PDH (Jerarquía Digital Plesiócrona - Plesiochronous Digital Hierarchy)

PDH es una tecnología usada en telecomunicación, tradicionalmente para telefonía; la cual permite enviar varios canales telefónicos sobre un mismo medio (ya sea cable coaxial, radio o microondas) usando técnicas de multiplexación por división de tiempo y equipos digitales de transmisión.

El término plesiócrono significa "casi síncrono" y ha sido definido por la ITU³² (International Telecommunication Union - Unión Internacional de Telecomunicaciones) de la forma siguiente:

"Dos señales son plesiócronas si sus instantes significativos correspondientes se presentan con la misma cadencia nominal y cualquier variación de esta cadencia se mantiene dentro de unos límites especificados. De esta forma, dos señales que tengan la misma velocidad digital nominal y que no provengan del mismo reloj, serán generalmente plesiócronas".

Se refiere al hecho de que las redes PDH funcionan en un estado donde las diferentes partes de la red están casi, pero no completamente sincronizadas. La tecnología PDH, por ello, permite la transmisión de flujos de datos que, nominalmente, están funcionando a la misma velocidad, pero permitiendo una cierta variación alrededor de la velocidad nominal gracias a la forma en la que se construyen las tramas.

La transmisión plesiócrona se basa en combinar los canales tributarios³³ por un procedimiento de entrelazado de bits, añadiéndole a cada canal tributario unos bits de

³² ITU (Unión Internacional de Telecomunicaciones, International telecommunications Union): Organismo encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

³³ Un equipo multiplicador digital recibe un número N de señales numéricas, llamadas canales tributarios.

relleno o de justificación y unos bits de control para éstos últimos, de manera que en el extremo receptor se puedan distinguir los bits de información de los de relleno. A este proceso se le conoce como justificación, en este caso positiva, y su objetivo es absorber las ligeras diferencias de frecuencias que pueden presentar los distintos tributarios, dados los diferentes relojes utilizados en su constitución.

En un sistema de primera jerarquía (2048 Kbps), las diferencias de frecuencia pueden llegar a variar hasta una tolerancia de +/- 50 partes por millón, admitiendo valores comprendidos entre 2047898 y 2048102 bps. Por lo tanto, a los tributarios más lentos es necesario añadirles más bits de relleno que a los tributarios más rápidos.

En el extremo receptor los bits de relleno son oportunamente reconocidos y eliminados gracias a la información que transportan consigo los bits de control de justificación. Razón por la que la velocidad utilizada por el agregado es mayor que la suma de las velocidades de los canales tributarios.

La referencia de sincronización que se toma para realizar todo el proceso descrito anteriormente es la señal agregada. Por lo tanto, cada etapa de multiplexación tiene su propia referencia de temporización, lo que origina uno de los mayores inconvenientes de la multiplexación plesiócrona, como lo es el hecho de que una vez formada la señal multiplexada, no es posible extraer un tributario concreto sin desmultiplexar completamente la señal.

Jerarquías de transmisión

Existen tres jerarquías plesiócronas diferentes: Europea, Americana y Japonesa. La Europea se basa en una señal de los sistemas de primer orden de 30 canales de 2 Mbps, mientras que la Americana y la Japonesa se basan en la de 24 canales de 1,5 Mbps. (Ver tabla 4.1)

Tabla 4.1 Resumen de las diferentes soluciones normalizadas para cada uno de los tres sistemas.

Nivel Jerárquico	Velocidad de transmisión (Kbits/s) canales					
	Europa, Sudamérica		USA		Japón	
0	64	1	64	1	64	1
1	2048	30	1544	24	1544	24
2	8448	40x4=120	6312	24x4=96	6312	24x4=96
3	34368	120x4=480	44736	96x7=672	32064	96x5=480
4	139264	480x4=1920	139264	672x3=2016	97728	480x3=1440

Estas jerarquías están basadas en multiplexar en el tiempo cuatro tributarios de la jerarquía inmediata inferior, en una señal múltiplex de velocidad aproximadamente cuatro veces mayor. Se denominan, abreviadamente de 2 Mbps a la primera, de 8 Mbps a la segunda, de 34 Mbps a la tercera y de 140 Mbps a la cuarta. Las de 565 Mbps y 2.5 Gbps no están especificadas, aunque se utilizan.

Para las cuatro jerarquías especificadas, la ITU ha definido las características físicas y eléctricas de los interfaces digitales en la recomendación G.703. Como código de línea se suele utilizar AMI o HDB3.

Funcionamiento de PDH

Un equipo multiplicador digital recibe un número N de señales numéricas, llamadas tributarios, que se presentan a su entrada en paralelo y produciendo una señal digital de mayor velocidad de información como mínimo N veces superior a la de los tributarios.

- $f_m \geq N \times f_t$
- f_m = frecuencia múltiplo.
- f_t = frecuencia de tributario.

Los tributarios de entrada deberán estar en fase y en igualdad de frecuencia entre sí, pero en realidad no es así sino que tienen distinta fase entre sí y variación de las frecuencias.

- $f_{t<} = f_t \pm \Delta f_t$
- $f_m = f_m \pm \Delta f_m$

A cada señal tributaria se le añaden unos bits que se llaman de relleno o de justificación y unos bits que se llaman de control de justificación, para que el extremo receptor pueda distinguir los bits que son de información y los que son de relleno. Este proceso es conocido como justificación y tiene por objeto absorber las ligeras diferencias de frecuencia que pueden presentar los distintos tributarios, ya que pueden haberse constituido con fuentes de reloj diferentes. De esta forma, a los tributarios más lentos es necesario añadirles más bits de relleno que a los tributarios más rápidos. En el extremo receptor los bits de relleno son oportunamente reconocidos y cancelados gracias a la información que transportan consigo los bits de control de la justificación.

En consecuencia, la velocidad de la señal agregada es mayor que la suma de las velocidades de las señales tributarias.

- $f_r > N \times f_t \rightarrow f_m = (N \times f_t) + f_r$
- f_r = frecuencia de los bits de redundancia.

Características de PDH

- Señales plesiócronas.
- Multiplexado bit por bit.
- La relación de fases entre la trama y la información útil no se conserva. Por ello no es posible obtener acceso directo a los canales individuales concatenados en la señal múltiplex. El acceso sólo es posible después del proceso de desmultiplexado.

Ventajas

- El multiplexor no se tiene que sincronizar en el lado de los tributarios a la señal de entrada.
- Adaptación del reloj mediante relleno positivo bit por bit.
- Para cada etapa de multiplexación se define una trama de transmisión propia.

Desventajas

- No puede satisfacer los requerimientos de la alta capacidad de transmisión.
- Poca capacidad y estandarización debido a que provoca cuellos de botella en la interconexión entre distintas redes.
- Sólo utiliza códigos regionales en lugar de utilizar los estándares internacionales.
- Difícil interconexión universal debido a que se tienen tres diferentes arquitecturas internacionales.
- Diferentes niveles de velocidad.
- Cada fabricante usa sus propios códigos.
- La localización de las señales es de baja velocidad.

b) SDH (Jerarquía Digital Síncrona - Synchronous Digital Hierarchy)

Es un conjunto jerárquico de estructuras de transporte digitales, normalizadas para el transporte digital por redes de transmisión físicas de cabidas útiles correctamente adaptadas.

Su objetivo es suplir las deficiencias de la jerarquía PDH, debido a la necesidad de manejar velocidades de transmisión mayores y a la preocupación por una operación más confiable, flexible y económica.

Los sistemas SDH pueden utilizarse:

- En las redes actuales como sistemas de transmisión.

- En lugar de los sistemas plesiócronicos sin cambio de la arquitectura de las redes.
- En las futuras redes troncales síncronas en forma de anillos o barras (buses), en las futuras redes de acceso, ofreciendo servicios de alta velocidad y banda ancha (por ejemplo, en aplicaciones de transmisión de video y LAN/MAN/WAN). (Ver figura 4.1)

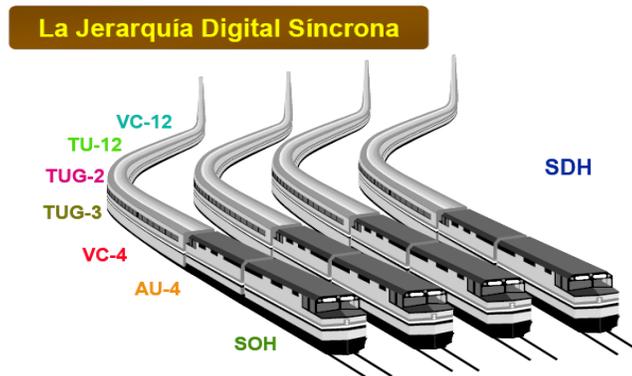


Figura 4.1 Jerarquía Digital Síncrona

Con el propósito de cubrir estos nuevos requerimientos, la UIT-T³⁴, en sus recomendaciones G.707, G.708 y G.709, estandarizó la red de transporte basada en SDH. El grupo de estudio XVIII de la UIT-T (CCITT) comenzó a trabajar en el estándar SDH en junio de 1986. En noviembre de 1988 aparecieron los primeros estándares de SDH, los cuales se resumieron en las recomendaciones G.707, G.708 y G.709.

SDH deriva de SONET (Synchronous Optical Network, Red Óptica Síncrona), otro estándar desarrollado por Bellcore para detener el máximo rendimiento de la transmisión digital sobre medios ópticos y que fue adoptado posteriormente por el Working Group T1X1 de ANSI.

Tres argumentos fueron clave para el desarrollo de estos estándares:

- La necesidad de disponer de métodos para la multiplexación de los sistemas de transmisión óptica.
- Proporcionar accesos económicos para pequeños volúmenes de datos dentro de tramas ópticas.

³⁴ UIT-T: Sector de Normalización de las Telecomunicaciones de la UIT, es el órgano permanente de la UIT que estudia los aspectos técnicos, de explotación y tarifarios y publica normativas sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial.

- Preparar el soporte de futuras demandas como las redes privadas virtuales, reserva dinámica de ancho de banda y soporte de la ISDN basada en ATM.

Funcionamiento de SDH

Una red síncrona es capaz de incrementar sensiblemente el ancho de banda disponible y reducir el número de equipos de red sobre el mismo soporte físico que otro tipo de tecnologías. SDH define una estructura que permite combinar señales plesiócronas y encapsularlas en una señal SDH estándar.

La introducción de las jerarquías síncronas de transmisión (SDH) significa la inmediata simplificación en el manejo de las infraestructuras básicas de comunicaciones utilizadas en redes extensas. Las anteriores técnicas de multiplexación plesiócrona (PDH) obliga a convertir todo el tráfico de bits de igual tamaño, aunque haya sido generado con diferentes relojes, antes de multiplexarlo por los enlaces de alta velocidad.

Cuando se utiliza SDH se elimina la necesidad constante de multiplexar y demultiplexar las señales porque todas las señales son sincronizadas a la misma frecuencia haciendo innecesarios los bits de relleno, siendo posible introducir y extraer dinámicamente las señales de las tramas portadoras mediante los multiplexores denominados add-drop³⁵.

Modelo de capas SDH

SDH puede ser representado en forma de modelos de capas. La jerarquía digital síncrona en términos de un modelo de capas ha sido dividida en cuatro niveles que están directamente relacionados con la topología de red (Ver tabla 4.2).

Tabla 4.2: Modelo de capas SDH

Nivel	Descripción
Interfaz Física (Physical Interface)	Nivel más bajo, el cual representa el medio de transmisión. Éste es usualmente fibra óptica o posiblemente un enlace de radio o un enlace satelital.

³⁵ Este tipo de multiplexores combinan varios flujos de datos de menor ancho de banda en un solo haz de luz.

<p>Sección de Regenerador (Regenerator Section)</p>	<p>Es el camino entre regeneradores. Parte de la cabecera de una trama, está disponible para la señalización necesaria dentro de esta capa. Esta capa especifica los niveles básicos de las tramas para convertir las señales eléctricas en señales ópticas.</p>
<p>Sección de Multiplexación (Multiplexer Section)</p>	<p>Comprende la parte del enlace SDH entre multiplexores. Este nivel es responsable de la sincronización, el multiplexado de los datos en las tramas, la protección de las funciones de mantenimiento y de la conmutación. Parte de la cabecera de una trama es usada para las necesidades de la sección de multiplexación.</p>
<p>Encaminamiento (VC-N Layer)</p>	<p>Nivel responsable del transporte extremo a extremo de los contenedores virtuales (VC2) con la apropiada velocidad de señalización. Encargado de conectar terminales. Los datos son ensamblados al principio y no son desensamblados ni es posible acceder a ellos hasta que no lleguen al final, es decir, los contenedores virtuales están disponibles como carga útil en los dos extremos de esta sección.</p>

Estructura de una trama SDH

SDH tiene una velocidad de transmisión básica de 155 Mbps, alcanzando velocidades hasta 520 Mbps, en una trama que se denomina STM-1 (Synchronous Transport Module). A partir de ella y multiplexando byte a byte de manera que la estructura de la trama permanece inalterada, se obtienen velocidades mayores; se han estandarizado las tramas STM-4 (4x155, 520=622,080 Mbps) y STM-16 (16x155, 520 Mbps=2488,320 Mbps). (Ver figura 4.2)

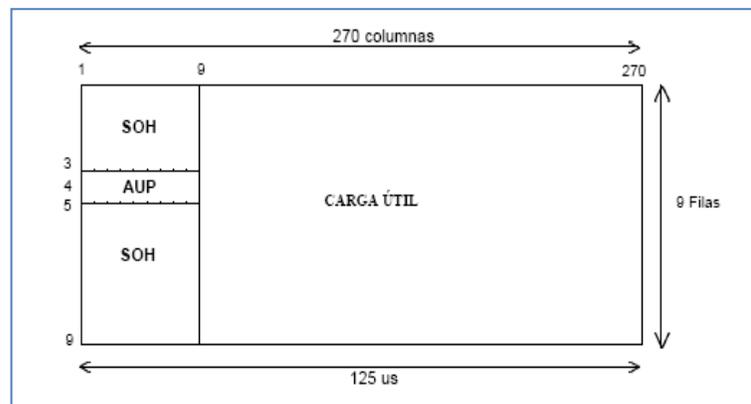


Figura 4.2 Estructura de la trama básica SDH

La trama básica está definida en la recomendación G. 708 de ITU-T. Tiene una duración de 125 micro segundos y corresponde a una matriz de 9 filas por 270 columnas cuyos elementos son bytes. La trama se transmite de izquierda a derecha, de arriba abajo. Cada octeto o byte dentro de la trama representa una velocidad de 64 Kbps.

En términos sencillos, la idea de SDH es que se tiene un vagón de gran capacidad (trama SDH) que debe ser colmado con atributos de diferentes velocidades. El primer paso es adaptar ese tributario asíncrono a la trama que se tiene; este proceso de adaptación equivale a meter el tributario en una "caja" (Ver figura 4.3).

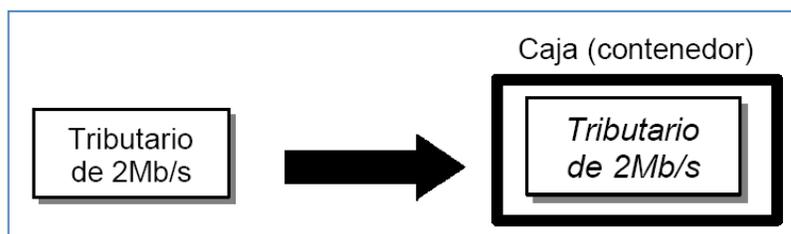


Figura 4.3 Proceso de adaptación SDH.

Características de SDH

- Tratamiento a nivel de byte.
- Duración de la trama uniforme (125 μ s), es decir, la trama se repite 8000 veces por segundo.
- Utilización de punteros para identificar las tramas de los tributarios para adaptación de velocidad (justificación).
- Canales de servicio y supervisión de gran capacidad.
- Un multiplexor SDH puede incorporar tráficos básicos (2 Mbps en SDH) en cualquier nivel de la jerarquía, sin necesidad de utilizar una cascada de multiplexores, reduciendo las necesidades de equipamiento.
- La gestión de red permite la inmediata identificación de una falla en un enlace o nodo de la red.
- La inclusión de canales dentro de una trama SDH posibilita la implementación de un software de control total de la red. Éste permite disminuir el tiempo de respuesta ante fallos y el ahorro de tiempo de desplazamiento a emplazamientos remotos.
- Los estándares SDH permiten la interconexión de equipos de síntesis fabricantes en el mismo enlace.
- Fibra óptica: Éste es el medio físico comúnmente desplegado en las redes de transporte actuales.

- Sincronización: Los operadores de red deben proporcionar temporización sincronizada a todos los elementos de la red para asegurarse de que la información que pasa de un nodo a otro no se pierda.

Ventajas

- Aproximadamente se asigna el 5% de la estructura de la señal para soportar todos los procedimientos que intervienen en el manejo y gestión de red.
- Una señal SDH es capaz de transportar cualquier tributario de los existentes hoy en día.
- El método de multiplexación permite la adaptación flexible de la red al crecimiento del tráfico y el principio de conexión en red permite una gestión de tráfico directa y usan supervisión de funcionamiento punto a punto.
- Normas de alcance mundial: traspasa las fronteras internacionales.
- Técnicas de multiplexación/desmultiplexación simplificadas: el uso de punteros facilita la localización rápida de los tributarios.
- Interfaces normalizadas: disminución de los costos.
- Se introducen servicios de banda ancha.
- Capacidades mejoradas de operación, administración, mantenimiento (OAM) y de gestión de red.
- Redes más flexibles: redes en anillos.

Desventajas

- Hay ciertas incompatibilidades con las redes actuales (por ejemplo, los actuales cross-connects no son compatibles con la SDH).
- La planificación de redes es totalmente distinta.
- La sincronización requiere consideraciones especiales.
- Es preciso disponer de una estrategia de evolución de PDH a SDH.
- La gestión de la red presupone una TMN (Telecommunications Management Network) para sacarle el máximo provecho a la jerarquía digital síncrona.
- La capacidad del STM-1 es mayor que la necesaria (mucho overhead) el overhead es aún mayor a velocidades más elevadas.

c) DWDM (Multiplexación por División en Longitud de Onda - Dense Wavelength Division Multiplexing)

La multiplexación por división en longitud de onda, tiene su origen en la posibilidad de acoplar las salidas de diferentes fuentes emisoras de luz, cada una a una longitud de onda diferente sobre una misma fibra óptica.

Después de la transmisión a través de la fibra, las señales a cada longitud de onda diferente pueden ser separadas entre sí hacia diferentes detectores en su extremo final. El componente encargado de inyectar las distintas fuentes sobre la misma fibra óptica es el multiplexor y el encargado de separarlas es el demultiplexor. El concepto de esta tecnología de transmisión óptica queda reflejado en la figura 4.4.

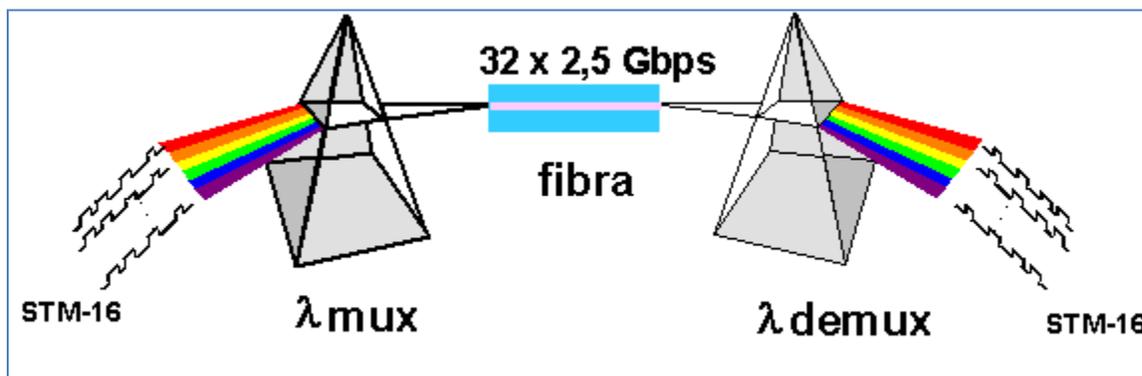


Figura 4.4 Concepto de multiplexación por división en longitud de onda.

Cuando la distancia entre los distintos puntos de la red es muy pequeña, la introducción de nueva fibra puede ser una solución a los problemas de capacidad. No obstante, cuando las distancias aumentan, o bien se tiene una base de fibra instalada, la DWDM es la alternativa más económica.

La transparencia ha sido otro argumento a favor de las redes de transporte DWDM. Mediante DWDM en cada una de las longitudes de onda se pueden ubicar diferentes tasas de bit de distintas capas superiores, como PDH, SDH, ATM e IP. Se puede ver, por lo tanto, cómo una tecnología totalmente óptica es independiente de la tasa de bit y protocolo de las capas superiores.

Evolución de tecnologías para la transmisión digital: Características de DWDM

En efecto, tras la evolución de las comunicaciones analógicas a las digitales y de PDH a SDH, el objetivo está ahora en pasar de SDH a DWDM. SONET en Norte América y SDH o JDS (*Jerarquía Digital Síncrona*) en Europa, son los estándares de transmisión digital a larga distancia que resuelven los problemas de compatibilidad entre equipos de distintos proveedores, la gestión y mantenimiento de los equipos, así como de la inserción y la extracción de las señales de jerarquías inferiores (de menor capacidad), presentados por su predecesor PDH.

Tanto PDH, como SONET y SDH, son tecnologías de transmisión que están basadas en multiplexación en el tiempo (ver figura 4.5), que utilizan la fibra óptica como sistema de

transmisión, pero que realizan las funciones de amplificación, encaminamiento, extracción e inserción de señales, etcétera en el dominio eléctrico, a diferencia de DWDM.

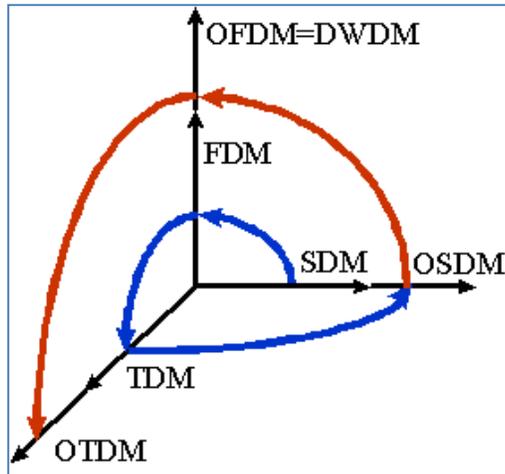


Figura 4.5 Evolución de las técnicas de multiplexación.

Si se considera la capacidad de las diferentes tecnologías como la tasa de transmisión de bits típica utilizada y el factor de multiplexación ofrecido por los nodos de conmutación y multiplexación, se puede ver una clara evolución:

- Inicialmente la transmisión digital era capaz de soportar 2 Mbps (en el primer nivel de multiplexación o multiplexores básicos), teniendo 64 Kbps cada una de las señales tributarias. Estos 64 Kbps conforman la tasa de bit de las redes telefónicas tradicionales.
- El siguiente paso fue mejorar la eficiencia en la transmisión, permitiendo tasas de bit más altas introduciendo *cross-connects*, elementos de conmutación entre puertos de entrada y de salida. La señal agregada pasó a tener una capacidad de 140 Mbps y un factor de multiplexación de 2 Mbps. Por supuesto también hay tasas de bit intermedias, tales como 8 Mbps o 34 Mbps. Esta tecnología es PDH.
- Un paso mayor que está de hecho en desarrollo en todos los países del mundo, es la introducción de SDH. Actualmente el factor de multiplexación es de 150 Mbps y es posible una capacidad de 10 Gbps.
- Una nueva etapa está en el uso generalizado de la DWDM, que aún no ha sido totalmente estandarizado debido a la rápida evolución de estos equipos, lo que imposibilita producir recomendaciones a tiempo y constituye una clara desventaja

frente a SDH. Ya no se está lejos de alcanzar una capacidad de 320 Gbps (32 longitudes de onda), con un factor de multiplexación de 10 Gbps.

Todas estas características hacen de DWDM la mejor técnica a corto plazo para llegar a aprovechar todo el ancho de banda ofrecido por una fibra óptica, sin necesidad de cambiar todos los equipos y enlaces existentes.

Funcionamiento de DWDM

La tecnología DWDM introduce más longitudes de onda distintas en cada fibra. No existe una frontera claramente definida para el calificativo "densa"; puede considerarse a partir de las 10 longitudes de onda. Por otra parte, dado que cada vez es mayor el número de longitudes de onda por fibra, la denominación DWDM es la que generalmente se emplea.

Sin embargo, a medida que el número de longitudes de onda crece, hay que tomar en cuenta varias consideraciones como el ancho y espaciamiento del canal, la potencia óptica que se está transmitiendo por la fibra, efectos no lineales, cross-talk (diafonía), etcétera. La tecnología DWDM (ver figura 4.6) fue posible debido a la fabricación y comercialización de componentes que en la época de CWDM (Coarse Wavelength Division Multiplexing - Multiplexación por División en Longitudes de Ondas Ligeras), la cual se refiere a una técnica de transmisión de señales a través de fibra óptica, eran únicamente ideas o experimentos.

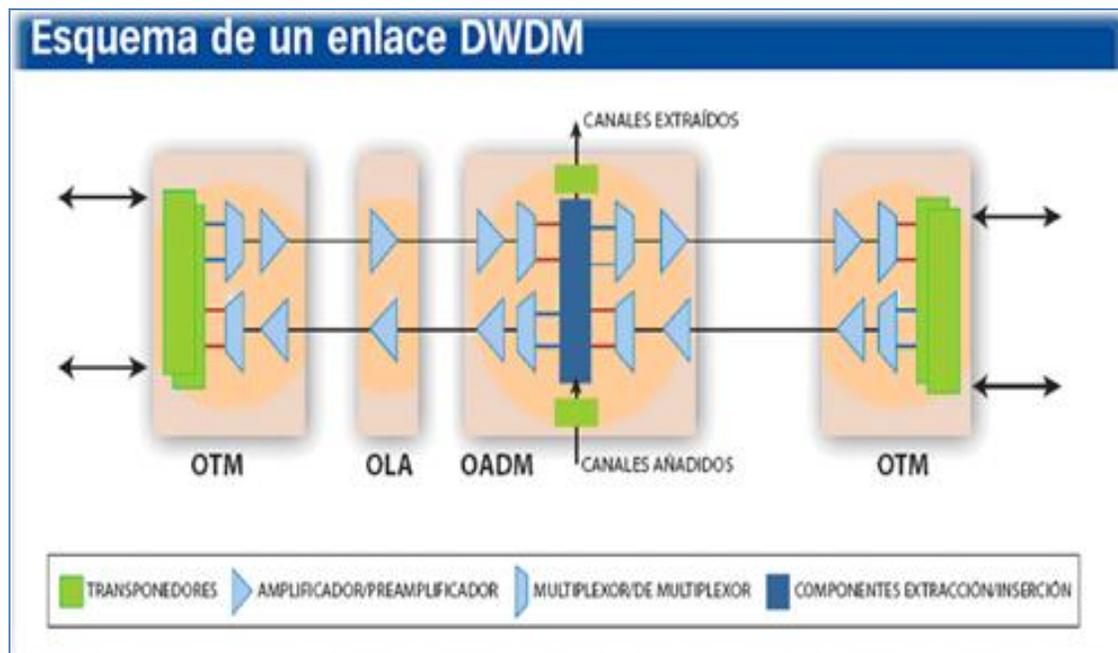


Figura 4.6 Esquema de un enlace DWDM.

Donde:

- **OTM (Multiplexor Terminal Óptico - Optical Terminal Multiplexer):** se encarga de multiplexar en la transmisión y demultiplexar en la recepción la totalidad de canales ópticos del enlace que están instalados.
- **OLA (Optical Line Amplifier - Amplificador Óptico de Línea):** amplifica la señal DWDM conjunta en el dominio óptico (sin ningún tipo de regeneración eléctrica de cada uno de los canales individuales) para su transporte a larga distancia.
- **OADM (Optical Add & Drop Multiplexer - Multiplexor Óptico Añadir y Borrar):** extrae información de un determinado canal óptico, e inserta nueva información reutilizando dicho canal, sin alterar el resto de canales multiplexados y sin ningún tipo de conversión electroóptica.

Ventajas

- **Transparencia:** como el DWDM es la capa física de la arquitectura, puede soportar TDM y formatos de datos como ATM, Gigabit Ethernet, ESCON, y Fibre Channel - Canales de Fibra (que son los que se usan para sincronizar las Redes de Área de Almacenamiento (Storage Area Network), entre los Centros de Procesamiento de Datos (Data Centers) con interfaces abiertas sobre una capa física común.
- **Aprovisionamiento dinámico:** aprovisionamiento rápido, simple y dinámico de conexiones de red que le permiten proveer servicios de alta capacidad rápidamente.

Desventajas

- Debido a que el tráfico en las redes de transporte se continúa incrementando y aunque DWDM es una tecnología relativamente joven con amplias y óptimas aplicaciones, no será suficiente para afrontar la gran avalancha de tráfico que se puede predecir para un futuro muy cercano, causado principalmente por la transmisión de datos.
- Por ser una tecnología aún en desarrollo se continúa con el avance y pruebas de algunos dispositivos o componentes para DWDM y como resultado, en un principio las implementaciones y funcionamiento de sistemas DWDM sería costoso, por lo que su uso se limitaría a sistemas de largas distancias y en cables submarinos.

4.2 Definición de tecnologías de telefonía

Las tecnologías de telefonía agrupan los elementos, técnicas, conocimiento e invenciones utilizadas en el tratamiento y la transmisión de la información que hacen posible la emisión, recepción y/o transmisión de señales de voz, audio y video a través de cable o vía internet, que son soportados y suministrados por empresas que ofrecen servicios de telefonía.

En este apartado se indaga sobre las diversas tecnologías que se han desarrollado para dar servicios de telefonía, describiendo su funcionamiento y características, así como las ventajas y desventajas que presentan.

a) SS7 Protocolo de señalización

El sistema de señalización de canal común número 7 (es decir, SS7 o C7) es un estándar global para las telecomunicaciones definidas por el sector de estandarización de las telecomunicaciones (ITU-T) de la unión de telecomunicaciones Internacionales (ITU). El estándar define el protocolo y los procedimientos mediante los cuales los elementos de la red de telefonía conmutada pública (PSTN, Public Switched Telephone Network) intercambian información sobre una red digital para efectuar el ruteo, establecimiento y control de llamadas. La definición de ITU para SS7 permite variantes nacionales tales como el Instituto de Estándares Nacionales Americanos (ANSI, American National Standards Institute) y Bell Communications usados en Norteamérica y el Instituto de Estándares de Telecomunicaciones Europeos (ETSI, European Telecommunications Standards Institute) usado en Europa.

El sistema SS7 ha sido concebido para satisfacer las necesidades tanto de voz como de datos, permitiendo una amplia gama de conexiones, incluyendo el modo circuito, el modo paquete, Frame Relay y ATM. Además permite toda la gama de servicios suplementarios. Los canales dedicados a señalización de control hacen más fácil modificar las características de una llamada durante su fase de comunicación y permiten la separación de la parte de conmutación de la parte de control.

Funcionamiento SS7

El protocolo SS7 se basa en una capacidad común para el transporte de señalización, llamada la parte de transferencia de mensaje (MTP) y la parte de usuario ISDN (llamada ISDN-UP). MTP y la parte de control de señalización de conexión (SCCP) forman la parte de los servicios de red (NSP), que realiza las funciones correspondientes a las primeras 3 capas del modelo OSI (ver figura 4.7). MTP representa un sistema de transferencia de

mensajes que permite transmitir información de señalización a través de la red hacia el punto de destino.

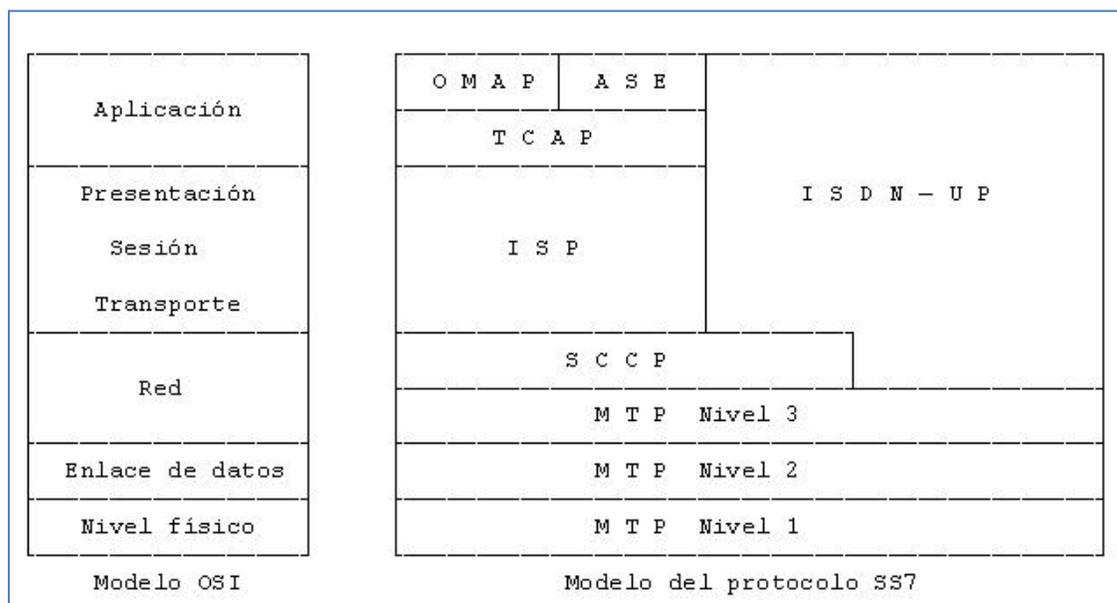


Figura 4.7 Relación SS7 con el modelo OSI.

Cada punto de señalización (signaling point), en la red SS7 (elemento de la red), se identifica mediante un código numérico único llamado point code (código del punto). Los point codes son llevados y traídos en los mensajes intercambiados entre los puntos de señalización a fin de identificar la fuente y el destino de cada mensaje. Cada punto de señalización utiliza una tabla de ruteo para seleccionar la ruta apropiada para que un mensaje pueda alcanzar su destino. Más o menos de la manera en la que un ruteador funciona en una red de cómputo.

Hay tres clases de puntos de señalización en una red SS7:

- SSP (Service Switching Point. Punto de Intercambio de Servicio).
- STP (Signal Transfer Point. Punto de Transferencia de Señal).
- SCP (Service Control Point. Punto de Control de Servicio).

Los SSPs son switches en los que se originan, terminan o se reenvían las llamadas. Un SSP envía mensajes de señalización a otros SSPs a fin de establecer, gestionar y liberar los circuitos de voz que se requieren para completar una llamada. Por otro lado, también pudieran enviar peticiones a alguna base de datos centralizada (un SCP), a fin de determinar cómo reenviar una llamada, un ejemplo de esto son los números 800 y 900. Un SCP responde con el número telefónico real, asociado con el número 800/900 marcado.

Así mismo, es común que se use un número alternativo si es que el primario se encuentra ocupado o si la llamada no se responde en un tiempo establecido.

El tráfico de la red entre los puntos de señalización puede enrutarse por medio de un switch de paquetes conocido como STP, cuya tarea es la de tomar cada paquete entrante y enviarlo hacia uno de los tantos enlaces de señalización (signaling link), basándose en la información de ruteo contenida en el mensaje SS7. En virtud de que actúa como un concentrador, el STP brinda un uso mejorado de la red SS7 al eliminar la necesidad de tener enlaces directos entre los diversos puntos de señalización. Así mismo, un STP puede llevar a cabo la traducción de los títulos mundiales (global title translation), que es un procedimiento por el cual el elemento de red destino se determina por medio de los dígitos presentes en el mensaje. También un STP puede hacer las veces de un firewall para controlar los mensajes SS7 que se intercambian con otras redes.

Debido a que la red SS7 es crítica para el procesamiento de las llamadas, tanto los SCPs como los STPs se despliegan en pares, separados físicamente para asegurar que la red permanezca en funcionamiento aunque alguno de estos elementos falle. Los enlaces entre los puntos de señalización también se instalan en pares por lo que el tráfico se comparte, sobre todos los enlaces. Si uno de los enlaces falla es reenviado por otro enlace. El protocolo SS7 brinda capacidades de retransmisión y corrección de errores.

Características SS7

- Establecimiento básico, gestión y finalización de llamadas.
- Servicios celulares tales como los de comunicaciones personales (PCS), roaming y autenticación de suscriptores.
- Portabilidad de números locales (LNP).
- Servicios 800 y 900.
- Características ampliadas tales como reenvío de llamadas, identificación de llamadas y conferencias entre varios participantes.
- Telecomunicaciones seguras a nivel mundial.
- Los mensajes SS7 se intercambian entre los elementos de red brindando: Mejores tiempos en el establecimiento de las llamadas.
- Uso más eficiente de los circuitos de voz.
- Soporte para los servicios de redes inteligentes (IN), que requieren la señalización a los elementos de red sin necesidad de emplear los canales de voz.
- Control sobre el uso fraudulento de la red.

Ventajas

- Señalización estandarizada, por canal común.
- Flexibilidad.
- Robustez y confiabilidad: red de telecomunicaciones más confiable y mejor gestionada.
- Posibilidad de evolucionar.
- Capacidad de interconexión.
- Soporte para nuevos y variados servicios.
- Mejor aprovechamiento de los enlaces entre centrales
- Hace posible la introducción de nuevos servicios (Red Digital de Servicios Integrados y Red Inteligente).
- Mayor rapidez, lo que permite ofrecer al usuario mejor calidad.
- Facilita la interconexión con redes IP.

b) VoIP (Voice Over Internet Protocol)

Como dice el término, Voz sobre IP (VoIP, Voice over IP) intenta permitir que la voz viaje en paquetes a través del protocolo de Internet (IP, Internet Protocol) y obviamente a través de Internet. Es un método para tomar las señales analógicas del teléfono y transformarlas en datos que pueden ser transmitidos por internet. Tiene la capacidad de hacer llamadas de larga distancia de manera gratuita. Los sistemas de telefonía existentes son impulsados por un método muy fiable, pero poco eficiente para la conexión de llamadas conocido como conmutación de circuitos.

Se trata de transportar la voz previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y por ende desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.

La VoIP por lo tanto, no es en sí mismo un servicio sino una tecnología que permite encapsular la voz en paquetes para poder ser transportados sobre redes de datos sin necesidad de disponer de los circuitos conmutados convencionales conocida como la PSTN, que son redes desarrolladas a lo largo de los años para transmitir las señales vocales. La PSTN se basaba en el concepto de conmutación de circuitos, es decir, la realización de una comunicación requería el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica.

Funcionamiento VoIP

La figura 4.8, muestra los principales componentes de una red VoIP. El gateway convierte las señales desde las interfaces de telefonía tradicional (POTS, T1/E1, ISDN, E&M trunks) a VoIP. Un teléfono IP es un terminal que tiene soporte VoIP nativo y puede conectarse directamente a una red IP. En este trabajo de investigación, el término 'terminal' será usado para referirse a un gateway, un teléfono IP, o una PC con una Interface VoIP.

El servidor provee el manejo y funciones administrativas para soportar el enrutamiento de llamadas a través de la red. En un sistema basado en H.323, el servidor es conocido como un gatekeeper. En un sistema SIP, el servidor es un servidor SIP. En un sistema basado en MGCP o MEGACO, el servidor es un Call Agent (Agente de llamadas). Finalmente, la red IP provee conectividad entre todos los terminales. La red IP puede ser una red IP privada, una Intranet o el Internet. (Figura 4.8)

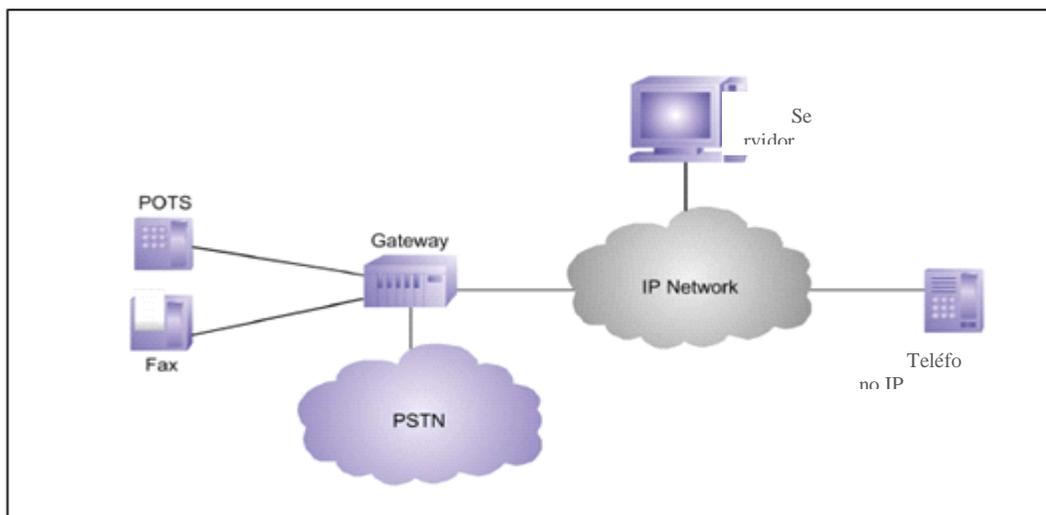


Figura 4.8 Componentes de una red VoIP.

Ventajas

- Reducción significativa en el tamaño de información enviada.
- Pueden enviarse 3 o 4 llamadas en el mismo espacio que ocuparía una llamada convencional.
- Existe la posibilidad de comprensión de datos, lográndose un ahorro mayor de espacio.
- La tecnología ya está bien definida.
- Precio menor.
- Mayor flexibilidad.
- Requerimientos menores en infraestructura.

Desventajas

- VoIP es dependiente de alimentación eléctrica.
- Debido a que usa internet, está sujeto a los mismos problemas asociados:
 - Latencia.
 - Pérdida de paquetes.
 - Susceptible a malware.

- Depende de las características del hardware de la computadora.

c) ISDN (Red Digital de servicios Integrados - Integrated Services Digital Network)

Se define la RDSI como una evolución de las redes actuales que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

Se les dice Servicios integrados porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes, etcétera.); es digital porque se basa en la transmisión digital, integrando las señales analógicas mediante la transformación Analógico - Digital, ofreciendo una capacidad básica de comunicación de 64 Kbps.

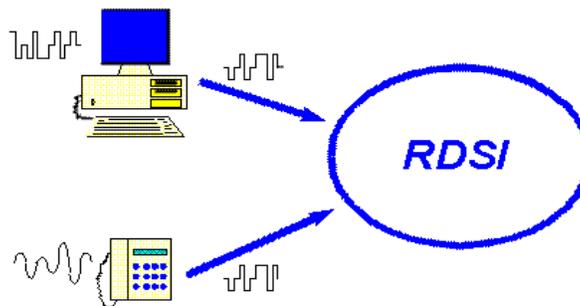


Figura 4.9 Integración de señales en RDSI.

Como se observa en la figura 4.9, en el caso del teléfono se efectúa la conversión analógico digital. En el caso de equipos digitales, como un ordenador, se transforma el código original a otro más adecuado a la comunicación (Transformación de código).

Corresponde a un sistema de protocolo con el que es posible establecer conexiones, y también romperlas, con un conmutador de circuito, así como también, puede otorgar características avanzadas, como videotelefonía, identificación de los usuarios que están

hablando, marcación directa de extensiones, marcación abreviada para las llamadas a los clientes, información de tarificación, etcétera.

A través de las conexiones con que cuenta este sistema se envían señales, que no son análogas, sino digitales. Es gracias a esto último que la velocidad de transferencia aumenta con es de sistema, pero si además de contar con el sistema ISDN en la central telefónica es posible adquirir un software adecuado, capaz de resistirlo, entonces las ventajas que el usuario podrá disfrutar serán mucho mayores.

Como se observa, el uso de sistema ISDN es frecuente en oficinas relacionadas a los más diversos rubros. Para su implementación, como ya se ha esbozado, es necesario contar con equipamiento especial entre lo que es necesario tener una línea ISDN, así como también con un modem ISDN, los que se utilizan a fin de enviar y recibir información. En su mayoría, las oficinas, utilizan este sistema ya contando con una red local y necesitan tener un acceso a Internet más rápido, lo que se puede lograr con un router o modem de esta tecnología; asimismo, algunos proveedores para hogares ofrecen este servicio que puede ser conveniente en cuanto a precios y velocidad.

Funcionamiento ISDN

El acceso básico está dividido en varios canales completamente independientes entre sí, aunque comparten el mismo cable para su comunicación. Cada canal está pensado para un uso en concreto.

Existen dos tipos de canales los cuales se pueden agrupar, desde el punto de vista de instalación del cliente, bien en la modalidad más sencilla o acceso básico (dos canales B y un canal D) o en forma de acceso primario, excesivo para un usuario doméstico (30 canales B y un canal D, en este caso de 64 Kbps).

Los canales B son los que se emplean para la transmisión de la portadora.

El canal D es un canal por el que se envían señales adicionales de datos, que aunque en principio no afecta a nivel de usuario, resulta vital para el correcto funcionamiento de la RDSI. Por ese canal viajan todos los datos referentes al número llamante, así como la confirmación de que los datos que se envían y reciben por los canales B han llegado a su destino con éxito.

Los canales B poseen un ancho de banda máximo de 64000 bps cada uno de ellos. A la hora de contratar una línea RDSI se asigna un número de teléfono, el cual es el número de

la línea digital. Se le denomina número de cabecera y es el encargado de identificar la línea cuando se llama al exterior y el que se debe marcar cuando se desea conectar desde fuera.

También es posible la contratación de números adicionales al de cabecera, los cuales se pueden enlazar a distintos servicios ofrecidos por la línea RDSI. De esta forma y con un aparato adecuado es posible hacer que al marcar el número de cabecera se conecte a través de un canal digital de 64000 bps, y marcando los números adicionales se acceda a funciones como línea de voz o un aparato de fax. Todo ello, sin tener que recurrir a discriminadores de voz/datos/fax, como ocurre con las actuales líneas analógicas.

Ventajas

- Puede transportar voz, video y datos simultáneamente.
- Configura la llamada más rápidamente que un módem.
- Sus tasas de transmisión de datos son mayores que las de las conexiones vía módem.

Desventaja

- SDN tiene la enorme desventaja de la agregación de canales. Si un canal agregado (bonded) queda inactivo durante una conferencia, toda la llamada fallará.

d) xDSL (Línea de abonado digital - Digital Subscriber Line)

La evolución histórica de las tecnologías xDSL quedó marcada a partir de 1983, cuando inicialmente se diseñó para video bajo demanda y aplicaciones de TV interactiva sobre el par de cobre. En 1987, la compañía Bell Communications Research (Bellcore) saca a la luz sus primeras especificaciones y en 1996 se les dio un nuevo impulso cuando se aprobó la ley de Reforma de Telecomunicaciones.

xDSL es un grupo de tecnologías de comunicación que permiten transportar información multimedia a mayores velocidades que las que se obtienen actualmente vía modem, simplemente utilizando las líneas telefónicas convencionales.

Existen diferentes tipos de tecnologías DSL, cada una para un propósito particular. Ellas son usualmente referidas a xDSL para incluir ADSL, HDSL, RDSL y VDSL en un grupo general.

Tienen en común que utilizan el par trenzado de hilos de cobre convencionales de las líneas telefónicas para la transmisión de datos a gran velocidad.

Funcionamiento de xDSL

Puesto que la red telefónica también tiene grandes limitaciones, tales como la de que su ancho de banda tan solo llega a los 4KHz, no permite el transporte de aplicaciones que requieran mayor amplitud de banda, es por esto que nace la tecnología DSL, que soporta un gran ancho de banda con unos costos de inversión relativamente bajos y que trabaja sobre la red telefónica ya existente.

Convierte la línea analógica convencional en una línea digital de alta velocidad, son unas tecnologías de acceso punto a punto a través de la red telefónica pública (circuitos locales de cable de cobre) sin amplificadores ni repetidores de señal a lo largo de la ruta de cableado, que soportan un gran ancho de banda entre la conexión del cliente y el primer nodo de la red, que permiten un flujo de información tanto simétrico como asimétrico y de alta velocidad sobre el bucle de abonado.

xDSL es una tecnología en la que se necesita un dispositivo módem xDSL terminal en cada extremo del circuito de cobre, que acepte flujo de datos en formato digital y lo superponga a una señal analógica de alta velocidad. De todas las variantes, el ADSL es la que predomina por ser más factible económicamente, aunque se prevé que VSDL, tomará el lugar prominente por permitir mayores velocidades.

Estas tecnologías utilizan modernas técnicas de modulación y codificación como son: 2B1Q, CAP, DMT, DWMT, que trabajan a velocidades del cliente hacia la red en un rango de 13 a 55 Mbps.

Descripción de las tecnologías xDSL

Existen diferentes tipos de tecnologías xDSL que se clasifican en cuanto a su evolución, características y ventajas, las cuales son: (ver tabla 4.3)

Tabla 4.3 Descripción de las tecnologías xDSL

Tecnología xDSL	Descripción
HDSL (High Bit Digital Subscriber Line - Línea	Es una tecnología simétrica, es decir, provee el mismo ancho de banda en los dos sentidos y la transmisión se

<p>Digital de Abonado de alta velocidad).</p>	<p>realiza de modo full dúplex. Instalando repetidores se puede incrementar dicho alcance, sin elevar excesivamente los costos.</p>
<p>SDSL (Single High Bit Rate Subscriber Line – Línea de Abonado Digital Simétrica).</p>	<p>DSL Simétrico o par único. SDSL utiliza sólo un par de hilos, pero tiene su tope en los tres Km, al menos en sus especificaciones de diseño. No obstante, las velocidades son las mismas que en HDSL. SDSL es HDSL sobre un solo par de cobre.</p>
<p>ADSL (Asimetric Digital Subscriber Line – Línea de Abonado Digital Asimétrica).</p>	<p>Esta tecnología es asimétrica Utiliza un ancho de banda en recepción (down stream) mayor que en transmisión (upstream). Las velocidades son de hasta 8 Mbps en sentido descendente y en el ascendente, entre 640 b/s y 1.5 Mb/s; es apropiada para aplicaciones donde se descargue desde la red más información que la que se trasmite hacia ella.</p>
<p>R-ADSL (Rate Adaptative- Asymetrical Digital Subscriber Line - Velocidad de Adaptación - Línea de Abonado Digital Asimétrica).</p>	<p>Opera con las mismas velocidades de transmisión que ADSL, pero se adapta dinámicamente a las variaciones en la longitud y otros parámetros de las líneas de pares trenzados. La velocidad de la conexión se puede seleccionar cuando se inicia, durante la conexión o bien cuando la señal llega a la oficina central.</p>
<p>ADSL Lite (Asimetric Digital Subscriber Line, Lite – Línea de Abonado Digital Asimétrica Ligera)</p>	<p>Es una versión más económica de ADSL, aunque más lenta, Surgió para disminuir los costos de instalación y para ahorrar trabajo al ajustar los splitters. Por esto surgieron dos variantes de fabricación; una en que se coloca el teléfono en serie como un microfiltro, que no necesita ajustes, y otras variantes en la que no se coloca filtro alguno.</p>
<p>VDSL (Very High Speed Digital Subscriber Line – Línea de Abonado Digital de muy Alto Índice de Datos).</p>	<p>Una alternativa para alcanzar altas velocidades de transmisión de datos es la combinación de cables de fibra óptica que alimentan a las unidades ópticas de la red en los sectores residenciales y la conexión final a través de la red telefónica de cobre.</p>

4.3 Definición de comunicaciones inalámbricas

Las comunicaciones inalámbricas, son aquellas, en la que los extremos de la comunicación, emisor y receptor, no se encuentran unidos por un medio de propagación físico, sino que se utiliza la propagación de información por medio de ondas electromagnéticas a través del aire.

El uso de redes inalámbricas facilita la comunicación en lugares donde no es posible tener una red cableada, sin embargo, éstas transmiten a una velocidad superior a las inalámbricas.

Características de las comunicaciones inalámbricas

- Acceso a la información en tiempo real.
- Son de fácil instalación e incrementan la movilidad.
- Resulta más fácil la incorporación de nuevos usuarios y equipo.
- Resulta más económica que una red cableada.

Algunos tipos de comunicación inalámbrica son los siguientes:

a) Estándar IEEE 802.11

IEEE 802.11 se refiere a un estándar internacional que define las características de una red de área local inalámbrica. El término 802.11 y WiFi se usan de la misma manera, pero no es correcto³⁶. WiFi es una certificación de interoperabilidad de la industria que se basa en un subconjunto del estándar IEEE 802.11.

Sin embargo, la palabra WiFi es conocida como Wireless Fidelity, que se refiere al estándar 802.11, creado en 1997 por la IEEE, en donde se definen las capas de enlace de datos y física del modelo OSI.

Así la expresión WiFi se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11.

Existen distintas variaciones del estándar 802.11, las cuales se describen a continuación³⁷:

³⁶ Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 4: Acceso a la WAN*, p. 320. México: Pearson Prentice Hall.

³⁷ Tanenbaum, A.S. (1997). *Redes de computadoras*, p. 295. México: Pearson Education.

1. 802.11a: fue aprobado y creado por la IEEE en 1999, también es conocido como WiFi5. Soporta velocidades de hasta 54 Mbps y trabaja a una frecuencia de 5 GHz, esto implica una mayor dificultad para atravesar muros y objetos. Su técnica de modulación es OFDM (Orthogonal Frequency Division Multiplexing – Multiplexación por División de Frecuencias Ortogonales).
2. 802.11b: se publicó en septiembre de 1999 por la IEEE. Se pueden seleccionar tasas de transmisión entre 1, 2, 5.5 y 11 Mbps. Tiene un alcance en el rango de 100-300 metros y trabaja en la banda de frecuencia de 2.4 GHz. La técnica de modulación que utiliza es DSSS (Direct Sequence Spread Spectrum - Espectro Ensanchado por Secuencia Directa).
3. 802.11c: permite conectar dos redes entre sí, lo que implica un ahorro en cuanto al cableado.
4. 802.11e: incluye características como QoS (Quality of Service – Calidad de Servicio) y soporte de multimedia en tiempo real, y es compatible con los estándares a y b. Su objetivo es introducir nuevos mecanismos a nivel de capa MAC (Media Access Control - Control de Acceso al Medio) para soportar los servicios que requieren garantías de calidad de servicio.
5. 802.11f: especifica un protocolo para los puntos de acceso, el cual, permite a un usuario cambiarse de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la red.
6. 802.11g: fue aprobado en junio de 2003 y utiliza la banda de los 2.4 GHz, con una tasa máxima de transferencia de 54 Mbps y una velocidad real de 24.7 Mbps. Es compatible con el estándar b y utiliza las mismas frecuencias.
7. 802.11i: mejora la seguridad en las redes WLAN (Wireless Local Area Network – Red Inalámbrica de Área Local), añadiendo el algoritmo de cifrado AES (Advanced Encryption Standard – Estándar de Cifrado Avanzado).
8. 802.11n: los trabajos comenzaron a partir de enero del 2004 y finalmente se aprobó en septiembre de 2009, con una velocidad teórica de 600 Mbps y alcanzando una real de 300 Mbps. Puede trabajar en bandas de frecuencia de 5 y 2.4 GHz.

Existen otros estándares 802.11, sin embargo, se describieron los más utilizados en el mercado.

A continuación se muestra en la tabla 4.4 las características principales de los tres estándares 802.11 más utilizados en el mercado:

Tabla 4.4 Características principales de los estándares 802.11 comerciales.

Característica	802.11a	802.11b	802.11g
Banda de frecuencias	5 GHz	2.4 GHz	2.4 GHz
Velocidad de transmisión	54 Mbps	11 Mbps	54 Mbps
Técnica de modulación	OFDM	DSSS	OFDM y DSSS
Área de cobertura	50 metros	100-300 metros	50 kilómetros

Componentes de una red 802.11

Una red 802.11 está basada en una arquitectura celular, donde el sistema está dividido en celdas, denominadas Conjunto de Servicios Básicos (BSS, Basic Service Set), a las cuales, se les considera la unidad básica del estándar. Cada una de estas celdas está controlada por una estación base denominada Punto de Acceso (AP, Access Point). Los puntos de acceso estarán conectados a través de un Sistema de Distribución (DS, Distribution System).

La red completa, incluyendo las diferentes celdas, sus puntos de acceso y el sistema de distribución, es denominada como Conjunto Extendido de Servicios (ESS, Extended Service Set). (Ver figura 4.10)

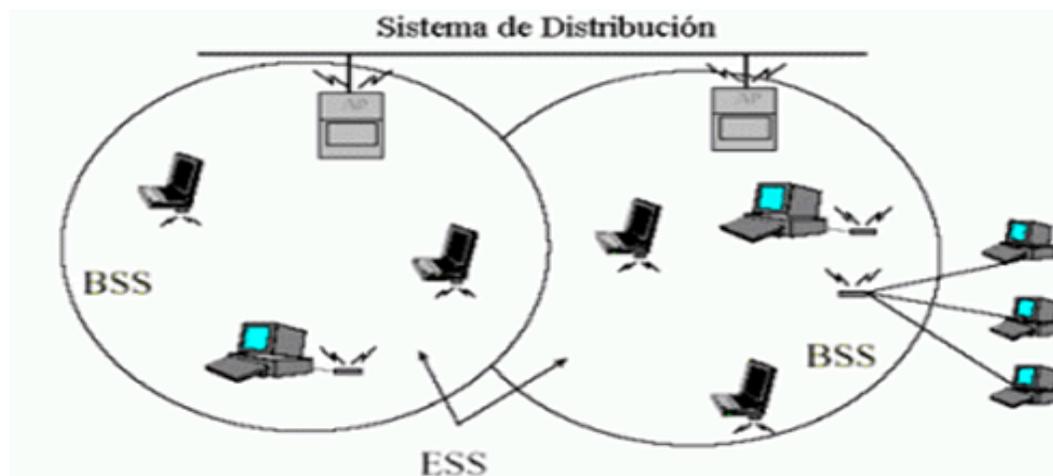


Figura 4.10 Componentes de una red 802.11.

b) Estándar IEEE 802.16

El nombre comercial para el estándar 802.16 es conocido como WiMax, que significa, interoperabilidad mundial para el acceso por microondas (Worldwide Interoperability for Microwave Access). Se trata de un protocolo para redes de área metropolitana (MAN, Metropolitan Area Network), que utiliza la arquitectura punto – multipunto.

Sin embargo, 802.16 se trata de un grupo de estándares inalámbricos IEEE. Tecnología desarrollada por WiMax Forum, cuyos dos miembros más representativos son Intel y Nokia.

El estándar 802.16 ha existido desde finales de la década de 1990, pero la atención se concentró en él en enero de 2003.

Es importante señalar que existen diferentes versiones de este estándar: acceso fijo, es decir, el servicio se ofrece desde una estación, dentro de su radio hasta el usuario. En este perfil se consiguen velocidades cercanas a 70 Mbps con un ancho de banda de 20 MHz, éste se comparte entre los usuarios de la celda, y el acceso móvil, el cual permite al usuario desplazarse de una manera similar a GSM.

A continuación se describen todos los estándares:

1. 802.16: fue publicado en el año 2002. Trabaja en el rango de 10 a 66 GHz, necesita línea de visión directa, con una capacidad de hasta 134 Mbps.
2. 802.16a: fue publicado en el año 2003. Trabaja en el rango de 2 a 11 GHz, con sistemas sin línea de vista (NLOS) y con línea de vista (LOS).
3. 802.16b: incrementó el espectro de 5 a 6 GHz y principalmente se caracterizó por aportar una fuerte calidad de servicio.
4. 802.16c: fue publicado en enero del año 2003. Opera en el rango de frecuencias de 10 a 66 GHz y su principal evolución es que mejoró la interoperabilidad entre sistemas.
5. 802.16-2004: es conocido como la versión fija del estándar WiMax y fue aprobado en junio de 2004. Opera en frecuencias de 2 a 11 GHz y permite una velocidad de transmisión de 70 Mbps.

6. 802.16e: es conocido como la versión móvil de WiMax y fue publicado en diciembre de 2005. Permite utilizar el sistema de comunicaciones inalámbricas con terminales en movimiento.

Componentes de una red WiMax

Una red WiMax consta de dos componentes principales³⁸ (figura 4.11):

1. Estación base WiMax: consiste en una torre WiMax conceptualmente similar a una torre de telefonía celular. Puede brindar cobertura a un área de 7500 kilómetros cuadrados.
2. Un receptor WiMax: debe contener una antena por separado para recibir la señal o puede ser una tarjeta de red inalámbrica en una laptop o computadora de escritorio. Al receptor también se le denomina equipo local del cliente (CPE).

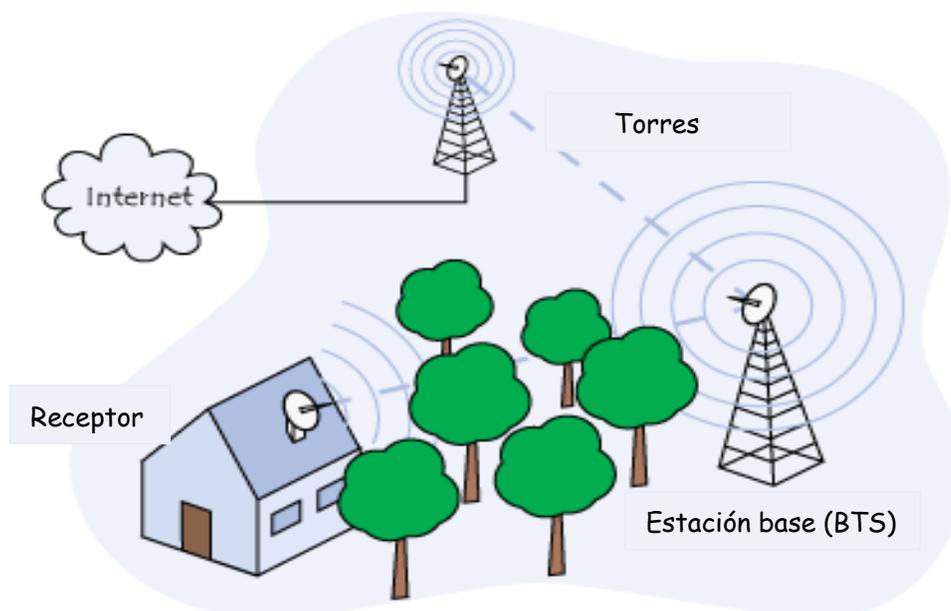


Figura 4.11 Ejemplo de una red WiMax.

Funcionamiento WiMax

WiMax ofrece dos formas de servicio:

³⁸ Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 4: Acceso a la WAN*, p. 317. México: Pearson Prentice Hall.

1. Conexión con línea de vista (LOS, Line of Sight): la señal viaja a través de un camino directo y sin obstrucciones desde el transmisor hasta el receptor. (Ver figura 4.12)



Figura 4.12 Enlaces LOS WiMax

2. Conexión sin línea de vista (NLOS, Non Line of Sight): la señal alcanza al receptor por medio de reflexiones, difracciones y dispersiones. Las señales que alcanzan al receptor poseen distintos retardos y atenuaciones. (Ver figura 4.13)

Existen algunas ventajas que hacen que las aplicaciones NLOS sean muy requeridas, tales como:

- La utilización en proyectos muy estrictos y restricciones de altura de antenas que a menudo no permiten a la misma estar posicionada para LOS.
- La tecnología NLOS también reduce los gastos de instalación y facilita la adecuada ubicación de equipos CPE.
- Permite el uso de equipos CPE en interiores.

NLOS (No Línea de Vista Directa)

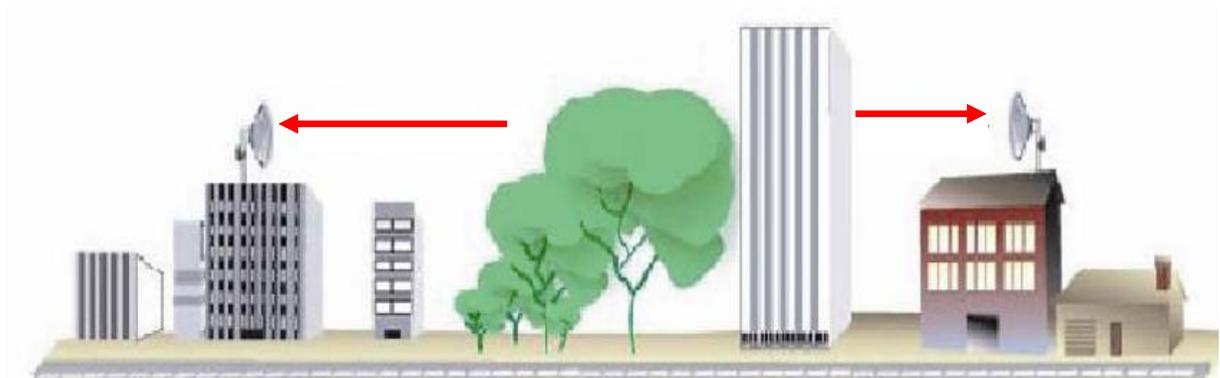


Figura 4.13 Enlaces NLOS WiMax

Características

- Gran ancho de banda: una sola estación de base puede admitir de manera simultánea más de 60 enlaces con conectividad T1/E1³⁹ o cientos de conexiones tipo DSL.
- Es independiente de protocolo: es decir, puede transportar IP, Ethernet, ATM (Asynchronous Transfer Mode - Modo de Transferencia Asíncrona) y otros. Eso hace que sea compatible con otros estándares como WiFi, Ethernet o Token Ring.
- Seguridad: incluye medidas para la autenticación de usuarios y la encriptación de los datos mediante los algoritmos Triple DES (Data Encryption Standard – Estándar de Cifrado de Datos) y RSA (Rivest, Shamir y Adleman).
- Operación en un amplio rango de frecuencias de los 450 MHz a los 5.8 GHz (inicialmente en 2.3, 2.5 y 3.5 GHz, por ejemplo en Latinoamérica).
- Escalabilidad al poder trabajar con canales de 1.25 a 10 MHz de ancho de banda.
- Buena eficiencia a nivel de red.

En la siguiente tabla (tabla 4.5) se muestran las ventajas y desventajas del uso de WiMax:

Tabla 4.5 Ventajas y desventajas del uso de redes WiMax

Ventajas	Desventajas
1. Velocidad: en circunstancias ideales y sin obstáculos que interfieran en los enlaces establecidos, la conexión puede alcanzar una distancia cercana a los 50 kilómetros y la velocidad de transferencia de los datos puede llegar a los 70 Mbps.	1. Implementación todavía complicada por falta de elementos para tener una red móvil administrable y operable en forma eficiente.
2. Modos de ahorro de energía y de dormir “sleep” de los dispositivos móviles.	2. La falta de un marco regulatorio adecuado, por lo que los costos de las licencias pueden tener un impacto negativo.

³⁹ E1 o Trama E1 es un formato de transmisión digital, el cual cuenta con un ancho de banda de 256 kilobytes transmitiendo a una velocidad de 2048 Mbps.

T1 también es un formato de transmisión de datos y voz digitales, transmite a una velocidad de 1544 Mbps.

3. Ofrece excelente cobertura en esquemas NLOS, usando diferentes elementos como OFDM.

4. Puede transmitir servicios como: VoIP, datos o videos. Además de que ofrece soporte de IPv6, QoS y VoIP.

3. Requerimiento de algoritmos y funciones de procesamiento más complejos, lo que implicaría incrementar algunos costos.

4. Limitación de potencia para prever interferencias con otros sistemas y el alto consumo de batería que se requiere.

c) **TDMA**

El Acceso Múltiple por División de Tiempo por sus siglas en inglés Time Division Multiple Access, es una tecnología inalámbrica de segunda generación, cuyo objetivo, es proveer un medio de transmisión para su uso en ambientes y situaciones variadas, desde usuarios fijos en una oficina, hasta usuarios móviles viajando a gran velocidad.

Se trata de una técnica de multiplexación que divide un único canal de frecuencia de radio en varias ranuras de tiempo (6 en D-AMPS y PCS, 8 en GSM). Así a cada persona que hace una llamada se le asigna una ranura de tiempo específica para la transmisión, lo que hace posible que varios usuarios utilicen un mismo canal simultáneamente sin inferir entre sí (figura 4.14).

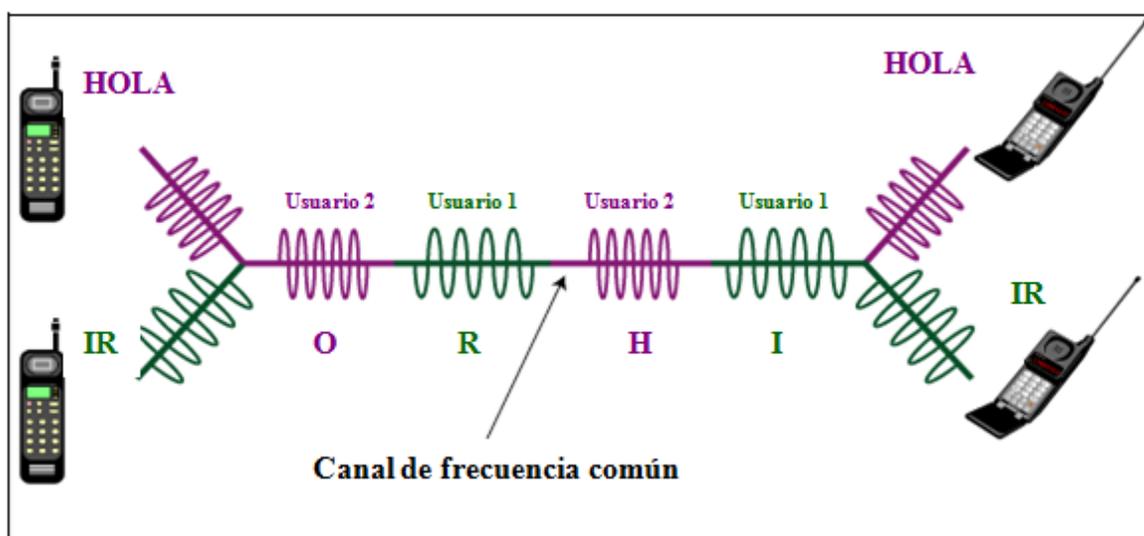


Figura 4.14 Funcionamiento de TDMA⁴⁰.

⁴⁰ TDMA. (s.f.). Extraído el 16 de abril de 2012 desde <http://www.ustudy.in/node/3200>

En un inicio fue definido por el estándar IS-54 y ahora es especificado en la serie IS-13x de especificaciones de la EIA/TIA.

Características

- Cuando el tiempo concedido a un usuario se agota, se pasa el servicio a otro, y así sucesivamente hasta regresar al primero.
- En México se maneja con frecuencia de 850 MHz y velocidad de 120 Kbps.
- Integra servicios como indicador de mensaje de espera en celulares e identificador de llamadas.
- Provee comunicación entre una ubicación central y múltiples ubicaciones remotas en lo que se denomina topología estrella.
- Se utiliza con modulaciones digitales.
- Adecuada para la conmutación de paquetes.
- Requiere una sincronización estricta entre emisor y receptor.

En la tabla 4.6 se muestran las ventajas y desventajas del uso de TDMA:

Tabla 4.6 Ventajas y desventajas del uso de TDMA.

Ventajas	Desventajas
1. Cuenta con el mayor número de radio base, lo que implica mayor cobertura y recepción.	1. No aprovecha el ancho de banda del canal de frecuencias, al segmentar el total de éste en 3, lo que permite tener activos menos usuarios.
2. Su frecuencia atraviesa mejor los obstáculos, provocando buena recepción en interiores.	2. Cuando el tiempo de un usuario se agota, al asignársele otro canal, puede cortarse la llamada.
3. No hay interferencia entre usuarios, ya que todos están separados por tiempos diferentes.	3. La frecuencia no filtra adecuadamente los ruidos circundantes, provocando menor calidad en llamada de voz.
4. Un solo transmisor-receptor sirve para todos los usuarios.	4. Transmisión de datos lenta y muy limitada.
5. Tecnología fácil de usar.	5. Menor cifrado que otras tecnologías.

d) CDMA

El Acceso Múltiple por División en Código, por sus siglas en inglés, Code Division Multiple Access, fue adoptado como estándar en julio de 1993 por la TIA (Asociación de la Industria de Telecomunicaciones - Telecommunications Industry Association) como el estándar CDMA IS-95 y sufrió una pequeña modificación en 1995.

Esta tecnología aparece como la solución a los problemas que presentaban en común los sistemas móviles de primera y segunda generación (FDMA y TDMA respectivamente).

Se trata de una técnica que hace una división asignando a cada usuario un código diferente, de esta manera es posible que varios usuarios puedan transmitir de manera simultánea sobre el mismo canal (ver figura 4.15).

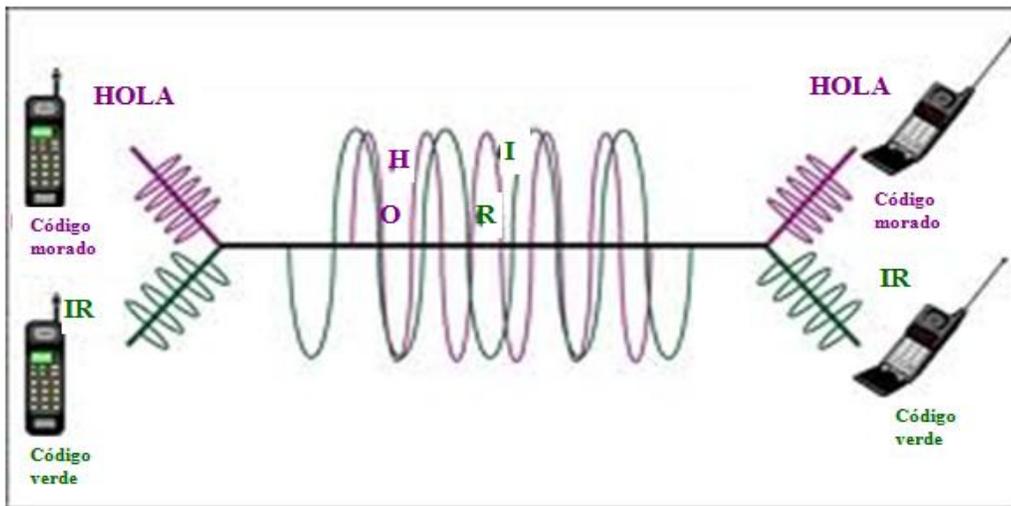


Figura 4.15 Funcionamiento de CDMA⁴¹.

Cada usuario tiene un código pseudoaleatorio el cual es usado para transformar la señal de un usuario en una señal de banda ancha mediante la técnica de Spread Spectrum (Espectro Extendido). Si el receptor recibe múltiples señales de banda ancha se usará el código asignado a un usuario en particular para transformar la señal de banda ancha recibida de ese usuario y recuperar la información original.

Los usos tradicionales del espectro ensanchado son militares debido a que una señal ensanchada es muy difícil de bloquear, de interferir y de identificar. Esto es así porque la potencia de estas señales está distribuida en un gran ancho de banda y sólo aparecen como un ruido ligero. Lo contrario ocurre con el resto de tecnologías que concentran la potencia de la señal en un ancho de banda estrecho, fácilmente detectable.

⁴¹ Hightman. A., Chung. E., y Galvan. A. (s.f.). *CDMA Background*. Extraído el 16 de abril de 2012 desde <http://cnx.org/content/m41832/latest/?collection=col11388/latest>

Características

- Transmisión a través de todo el ancho de banda.
- Varias llamadas son sobrepuestas en el canal y cada una tiene un código de secuencia único.
- No hay reuso de frecuencias, ya que se otorga una frecuencia fija hasta que concluye la llamada.
- En México se utiliza una frecuencia de 1900 MHz.
- Utiliza canales distintos para transmisión de voz y datos.
- Mayor nivel de cifrado desde su diseño.
- Es posible comprimir entre 8 y 10 llamadas digitales.
- Privacidad debido a los códigos aleatorios desconocidos.

En la tabla 4.7 se muestran las ventajas y desventajas de CDMA:

Tabla 4.7 Ventajas y desventajas del uso de CDMA.

Ventajas	Desventajas
1. Filtra el ruido de fondo, la diafonía y la interferencia, de modo que el usuario disfruta de una mayor calidad de voz, privacidad y mejor calidad de llamadas.	1. La frecuencia traspasa con dificultad obstáculos, por lo que pueden presentarse algunos problemas de recepción en interiores.
2. Proporciona la mayor cobertura de la industria inalámbrica, permitiendo construir redes con menos instalaciones base. Lo que significa reducción de gastos.	2. Cuando existe gran solicitud del servicio (se genera un número alto de códigos), el canal se satura y se crean huecos en la cobertura.

e) **GSM**

Los primeros trabajos con GSM los inició en 1982 un grupo dentro del Instituto Europeo de Normas de Comunicaciones (ETSI, European Telecommunications Standards Institute). Originalmente, este organismo se llamaba Grupo Social Móvil (Groupe Sociale Mobile), lo que dio pie al acrónimo GSM.

Por sus siglas en inglés significa, Global System for Mobile Communications - Sistema Global para las comunicaciones Móviles, es un estándar abierto de tecnología celular y es el estándar más popular de telefonía móvil en el mundo.

Este estándar pertenece a la segunda generación de tecnologías celulares. Permite realizar llamadas de voz y transferencia de datos, además el servicio de mensajes cortos (SMS, Short Message Service) está implementado sobre este esquema de comunicación.

El objetivo de este proyecto era poner fin a la incompatibilidad de sistemas en el área de las comunicaciones móviles y crear una estructura de sistemas de comunicaciones a nivel europeo.

GSM se diseñó para incluir una amplia variedad de servicios que incluyen transmisiones de voz y servicios de manejo de mensajes entre unidades móviles o cualquier otra unidad portátil.

Componentes de GSM

1. Centro de conmutación móvil (MSC, Mobile Switching Center), es el elemento principal de todo sistema GSM, se encarga de establecer, gestionar y despejar conexiones, así como de enrutar las llamadas a la celda correcta. Proporciona la interfaz con el sistema telefónico.
2. Celda, es la parte en la que está dividida una región de cobertura, tienen un tamaño aproximadamente de 35 Km, pero puede variar.
3. La unidad móvil (MS, Mobile Station), se refiere a la terminal del usuario, la cual está constituida por una tarjeta SIM (Subscriber Identity Module - Módulo de identificación del suscriptor), que permite identificar de manera única al usuario y a la terminal móvil, es decir, al dispositivo del usuario.
4. Controlador de estaciones base (BSC, Base Station Controller), determinan en qué celda se encuentra un usuario específico.
5. Estación de transmisión-recepción base (BTS, Base Transceiver Station), se encarga de transmitir y recibir señales a los dispositivos que se encuentran dentro de su celda. Está bajo el control del BSC.
6. Registro de ubicación de origen (HLR, Home Location Register), es una base de datos que contiene información sobre el usuario, como posición geográfica.
7. Registro de ubicación de visitante (VLR, Visitor Location Register), es una base de datos que contiene información administrativa seleccionada proveniente del HLR,

necesaria para el control de la llamada y provisión de servicios suscritos para cada móvil localizado en el área geográfica controlada por el VLR.

8. Registro de identificación del equipo (EIR, Equipment Identity Register), es una base de datos que contiene la lista de terminales móviles.
9. Centro de validación (AUC, Authentication Center), verifica las identidades de los usuarios, protegiéndolos así de accesos no autorizados. (Ver figura 4.16)

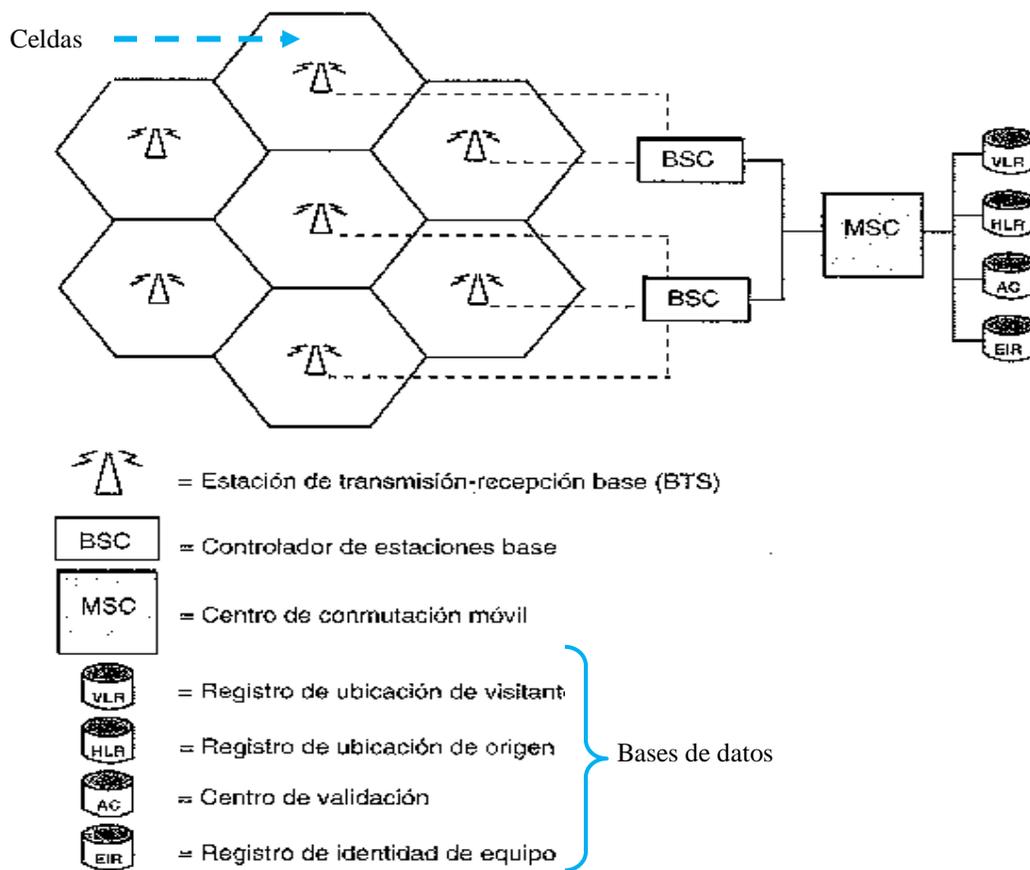


Figura 4.16 Esquema de componentes GSM.

Funcionamiento

En la figura 4.17 se observa que en cada celda los proveedores colocan una BTS para poder transmitir y recibir señales a dispositivos que se encuentran dentro de su celda.

Varias BTS son administradas por un controlador de estación base (BSC), las cuales determinarán en qué celda se encuentra un usuario específico.

Una BSC y las BTS son conocidas en conjunto como sistema de estación base (BSS).

Los BSS están a su vez conectados a un centro de conmutación móvil (MSC, Mobile Switching Center), el cual se encargará de establecer y cortar llamadas.

GSM utiliza una combinación de multiplexado en la frecuencia y el tiempo, es decir, FDM y TDM, lo que implica que en cada celda existen subcanales tanto de frecuencia como de tiempo.

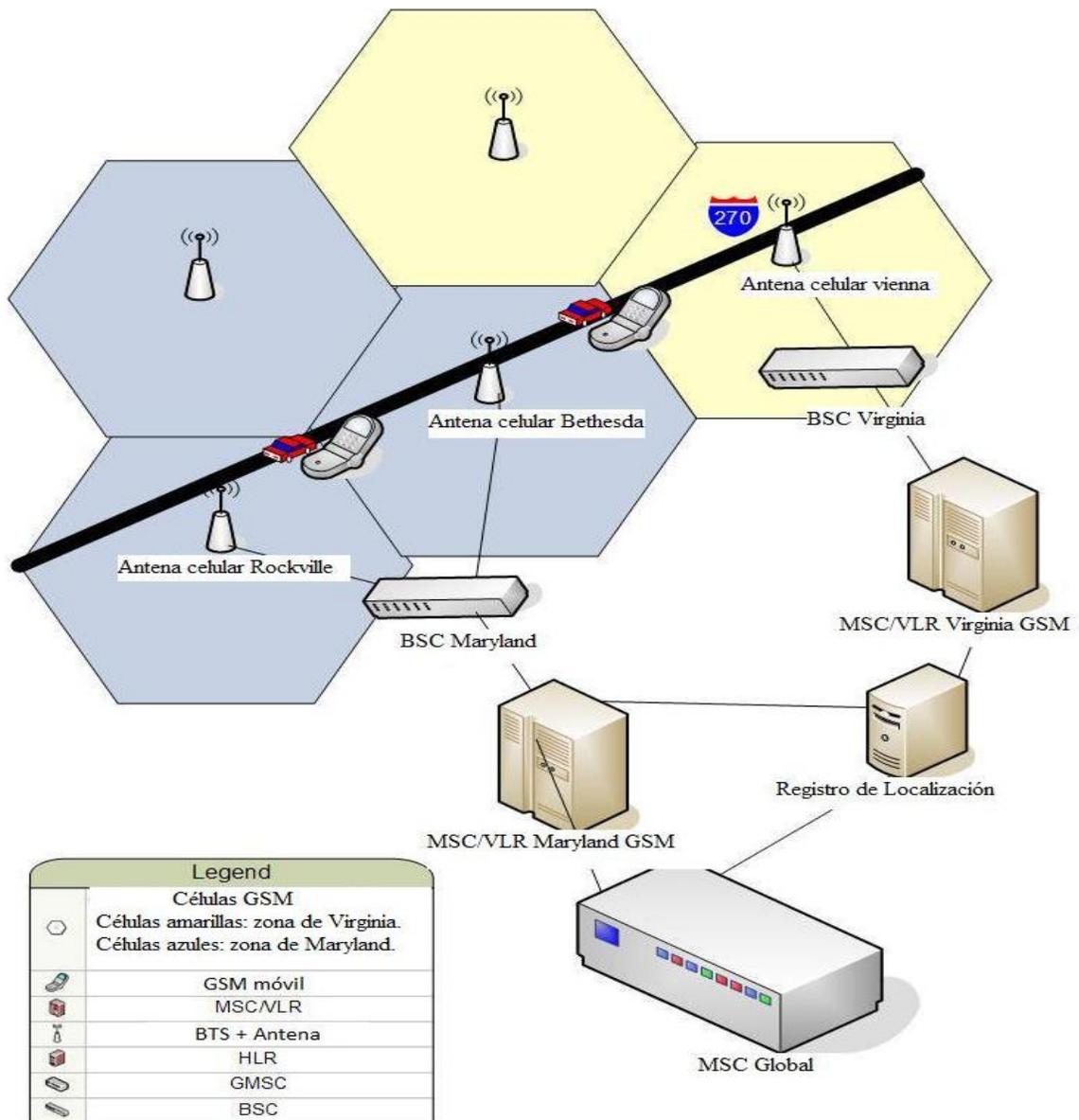


Figura 4.17 Funcionamiento de una red GSM.

Desarrollo de una llamada GSM

1. Un usuario de telefonía llama a la unidad móvil a través de la red pública.
2. La llamada se enruta a un MSC, el que se encarga de examinar los dígitos marcados y determina que no puede enrutar la llamada más lejos.
3. El registro de ubicación HLR interroga al usuario llamado.
4. El HLR interroga el registro de ubicación del visitante VLR que actualmente está dando servicio al usuario.
5. El VLR devuelve un número de enrutamiento al HLR que lo devuelve al MSC.
6. Con este número de enrutamiento, el MSC enruta la llamada al MSC terminal.
7. El MSC pide al VLR correlacionar la llamada con el suscriptor.
8. El VLR realiza la acción que se le solicite.
9. La BSS recibe una solicitud de notificación del MSC Terminal y envía una señal de notificación.
10. Cuando la señal de usuario regresa, la llamada se completa. (Ver figura 4.18)

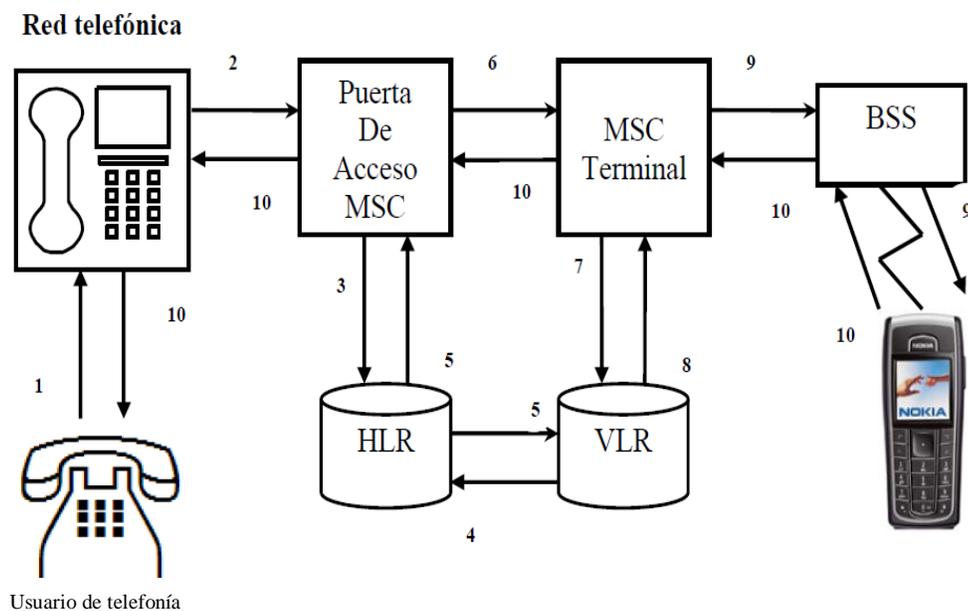


Figura 4.18 Ejemplo de enrutamiento de una llamada GSM.

Características

- Mayor calidad de voz (mejor que la de los sistemas analógicos existentes).
- Unidades móviles de bajo costo operacional, de compra y de servicio, convirtiéndose en un sistema universal.
- Posee un nivel de seguridad alto, preservando la confidencialidad, previniendo así los fraudes.
- Roaming internacional (válido en todo el mundo).
- Terminales personales portables.
- Crea nuevos servicios de todo tipo y da facilidades de red.

En la tabla 4.8 se presentan las ventajas y desventajas del uso de GSM:

Tabla 4.8 Ventajas y desventajas del uso de la tecnología GSM.

Ventajas	Desventajas
1. En el sistema GSM existe un centro de autenticación que es el encargado de autorizar al móvil a introducirse a la red, en donde cada usuario tiene una clave secreta que es asignada al momento de la contratación.	1. Posible pérdida de cobertura, por falta de antenas o por estar en una zona donde no llegue la cobertura, por ejemplo en hospitales.
2. Cada móvil posee un serial eléctrico denominado IMEI que es único para cada terminal, se realiza la consulta al registro de identidad de equipos. Obteniendo un estado de una de tres listas: <ul style="list-style-type: none"> • Blanca: IMEI autorizados para funcionar legalmente. • Negra: IMEI reportados como robados o con adeudos. • Gris: IMEI en observación pero que sí son permitidos para usar la red. 	2. Existen problemas cuando hay un gran uso de mensajes SMS, puede colapsarse la red, por ejemplo, en la celebración de año nuevo.
	3. Requiere un número considerado de radio base para brindar una buena cobertura.
	4. Posee un nivel de seguridad más bajo que CDMA.

f) *GPRS*

La necesidad de mayores tasas de transmisión, junto con la amplia disponibilidad de la red GSM, dio lugar al desarrollo de la red GPRS, normalizada a inicios de 1994 por el Instituto de Estándares de Telecomunicaciones de Europa (ETSI, European Telecommunications Standards Institute), como una tecnología de generación 2.5G de transmisión inalámbrica de datos. Por lo que es considerada como el punto de lanzamiento hacia las redes de tercera generación.

El sistema GPRS (General Packet Radio Service) o servicio general de paquetes vía radio, es una extensión de GSM, para la transmisión de datos no conmutada o por paquetes. Se encarga de actualizar los servicios de datos GSM para hacerlos compatibles con redes de área local (LANs), redes de área extendida (WANs) e Internet.

La conmutación de circuitos establece un camino entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación, es decir, tiene un ancho de banda fijo.

Esta tecnología permite que varios usuarios puedan compartir un mismo canal. La información es fraccionada en el origen y transmitida en pequeños bloques, siendo reagrupada posteriormente en su destino. (Figura 4.19)

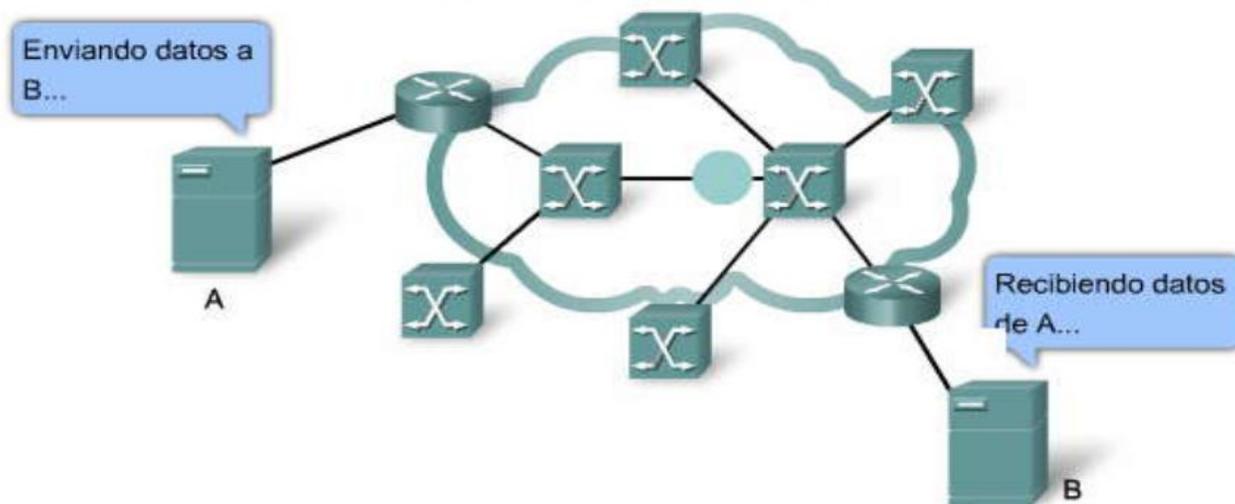


Figura 4.19 Conmutación de paquetes

Componentes de GPRS

Aunque GPRS utiliza la infraestructura del subsistema de la red GSM, para permitir la transmisión de paquetes de datos es necesario introducir nuevos elementos en la red GSM, tales como (ver figura 4.20):

1. Nodos de soporte GPRS (GSN, Gateway Support Node), son los responsables de enrutar los paquetes de datos entre estaciones móviles y redes de datos externas. Los nodos son los siguientes:
 - Nodo de Soporte de Servicio GPRS (SGSN, Serving GPRS Support Node), es el responsable de la gestión de la conexión del terminal móvil a la red GPRS.
 - Nodo de Soporte de Entrada GPRS (GGSN, Gateway GPRS Support Node), actúa como interfaz con la red externa de datos. Proporciona el acceso a las redes de datos basadas en IP.
2. A nivel de BTS y BSC, se deberá realizar la actualización del software para soportar tráfico de paquetes.
3. Nuevo hardware en el controlador de estación BSC; se implementará la Unidad de Control de Paquetes (PCU), que es la encargada de manejar la comunicación de paquetes.
4. Terminales móviles (MS) las cuales se categorizan de acuerdo con sus capacidades para soportar diferentes modos de operación simultáneamente para GSM y GPRS.
 - Clase A: soporta llamadas GSM y transmisión de datos GPRS, simultáneamente.
 - Clase B: igual que la clase A, con la diferencia que se da un servicio a la vez.
 - Clase C: soporta solo llamadas GSM o solo transmisión de datos GPRS.
5. La red troncal GPRS o backbone basado en IP.

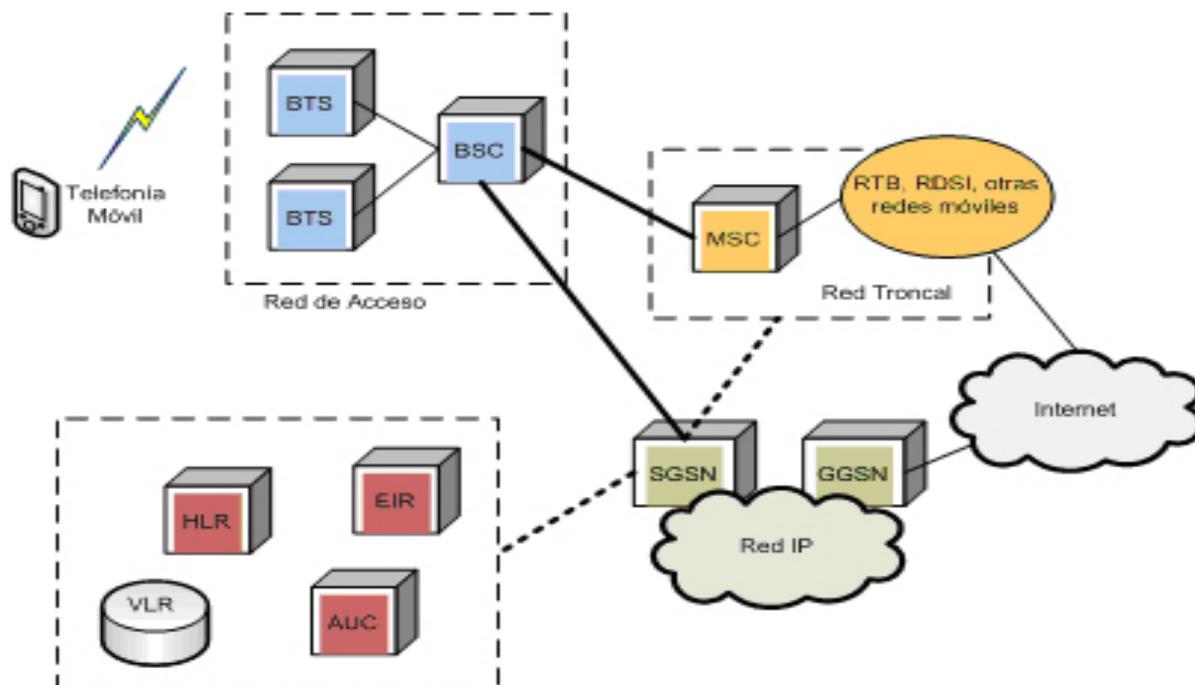


Figura 4.20 Diagrama de una red GPRS

Funcionamiento

GPRS no utiliza las centrales de conmutación GSM para el transporte de datos, sino que las estaciones base de radio están directamente conectadas a la red IP a través de dos nuevos tipos de servidores, también denominados nodos GSN, el SGSN y el GGSN.

Cuando un terminal GPRS desea enviar o recibir datos, busca la señal con mayor potencia y localiza la estación base más fuerte, notificando al sistema la ubicación de la celda de la cual está recibiendo la señal. El terminal evalúa periódicamente la calidad de las señales de estaciones vecinas. Cuando se deteriora la calidad de transmisión de la celda y si el terminal GPRS determina que existe otra estación base con mayor potencia que su estación base actual, éste comienza a escuchar la nueva estación base. El proceso de cambio de una estación a otra se llama handoff.

Se realizan los siguientes pasos para poder establecer la comunicación (ver figura 4.21):

1. Al conectar un dispositivo GPRS lo primero que éste hace es escanear canales GPRS.
2. Localizado un canal envía al SGSN una petición de conexión a la red.

3. El SGSN autentica al usuario usando el HLR:
 - Comprobación de que el usuario es válido.
 - Obtención del perfil de servicio.
 - Obtención de claves de cifrado.
4. Con el perfil de usuario SGSN determina el GGSN usado para encaminar los paquetes. Comunicándose con él.
5. El GGSN determina una IP dinámica para el dispositivo, permitiendo su direccionamiento en Internet.

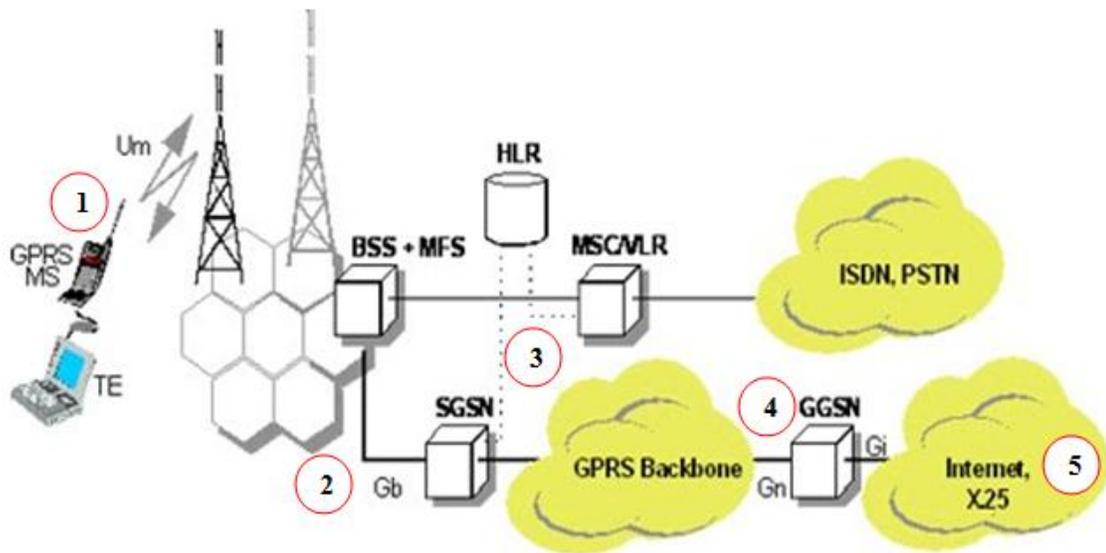


Figura 4.21 Comunicación en redes GPRS.

Características

- El tiempo de establecimiento de la conexión es prácticamente instantáneo, por lo que el usuario percibe que siempre está conectado.
- La facturación no se realiza por establecimiento o tiempo de conexión sino por volumen de información intercambiada.
- Utiliza varios canales asignados, con lo que la velocidad de transmisión de datos es mayor, la cual, va desde 21.2 Kbps a 144 Kbps por comunicación.
- Los canales de comunicación se comparten entre los usuarios dinámicamente, de modo que un usuario sólo tiene asignado un canal cuando está realmente transmitiendo datos. Logrando así, el uso eficiente de los recursos de la red.

- GPRS es una tecnología orientada a los protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet).
- Alcanza una velocidad de transferencia de hasta 144 Kbps. La conexión es permanente y su pago es por la cantidad de información transmitida.
- Existe la posibilidad de realizar y recibir llamadas de voz mientras se esté conectado o utilizando cualquiera de los servicios disponibles con GPRS, a esto se le conoce como, capacidad dual.

En la tabla 4.9 se muestran las ventajas y desventajas de GPRS:

Tabla 4.9 Ventajas y desventajas del uso de GPRS.

Ventajas	Desventajas
1. Es una tecnología que brinda al usuario una mayor velocidad de conexión y la ventaja de estar siempre conectado.	1. Capacidad limitada, debido a que la voz y las llamadas utilizan los mismos recursos de la red. En algunos tiempos puede que no haya canales disponibles.
2. Se factura por información transmitida y no por tiempo de conexión.	2. Las velocidades en la práctica son menores que el máximo teórico.
3. La integridad de los datos es segura, puesto que antes de comenzar la transferencia de datos el terminal móvil y el nodo SGSN se ponen de acuerdo en la clave a utilizar para la codificación y decodificación.	3. Retraso del tráfico en cada nodo, lo que conlleva un retardo que es mayor que en conmutación de circuitos, además de que algunos paquetes se pueden perder o corromper durante una transmisión.

4.4 INTERNET2

Es una red para la transmisión de datos con capacidades mayores de la Internet comercial actual, la cual fue creada en 1996. Forma parte de la iniciativa NGI (Next Generation Internet – Próxima Generación de Internet).

Su origen está basado en la colaboración de varias universidades del mundo para desarrollar aplicaciones que faciliten las misiones de investigación y educación de las universidades. Es llevado por 212 universidades de Estados Unidos y otras 60 compañías como Comcast, Microsoft, Intel, Sun Microsystems y Cisco Systems.

Internet2 no pretende reemplazar a la red actual, su meta es unir a las instituciones con los recursos y posibilidades para desarrollar nuevas tecnologías que puedan desplazarse dentro de la Internet Global.

Componentes de INTERNET2

En la figura 4.22 se muestra la arquitectura completa de Internet2, cuyo elemento clave es el *gigapop* (gigabit capacity point of presence - punto de presencia con capacidad de gigabits), un punto de interconexión de tecnología avanzada y alta capacidad donde los participantes de Internet2 pueden intercambiar tráfico de servicios avanzados con otros participantes del proyecto. Las universidades de una determinada región geográfica se unirán en un gigapop regional para conseguir una variedad de servicios Internet.

Cada universidad instalará un circuito de alta velocidad al gigapop que le corresponda, a través del cual obtendrá el acceso tanto a los servicios de la Internet comercial como a los avanzados de Internet2.

Los gigapops, por tanto, se unirán para adquirir y gestionar la conectividad entre los mismos en una organización cuya estructura y forma legal aún está por determinarse, pero que provisionalmente se llama "Entidad Colectiva" (Collective Entity, CE).

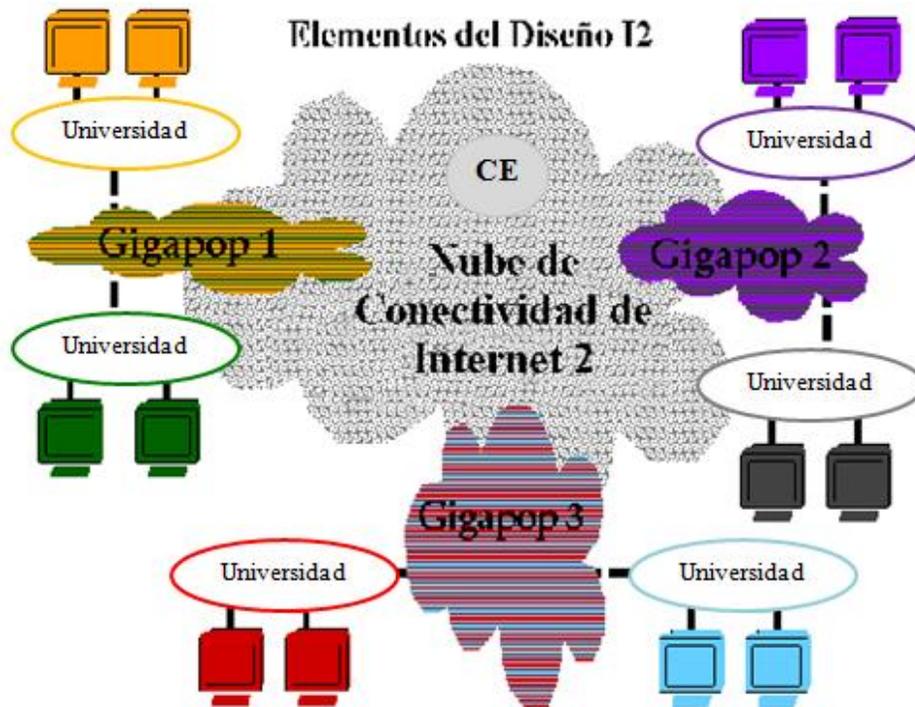


Figura 4.22 Arquitectura INTERNET2

Características

- Calidad de Servicio (QoS).
- Utiliza protocolos especializados, como el H.323.⁴²
- IPv6.
- Topologías dedicadas, seguras y flexibles.
- Está construida de fibra óptica.
- Ofrece una velocidad de 622 Mbps.
- Multicast, con lo cual, optimiza la red, ya que, desde un nodo que transmite se puede enviar información hacia otros nodos participantes en comunicación, sin necesidad de duplicar los envíos en la red.

A continuación se listan las ventajas y desventajas de Internet2

Tabla 4.10 Ventajas y desventajas del uso de Internet2

Ventajas	Desventajas
1. Asegura que tanto la tecnología hardware como software se basen en estándares abiertos y puedan ser usados por otros, incluidas las redes comerciales y los proveedores de servicios de Internet.	1. Existen muchas limitaciones de infraestructura que dificultan la estandarización y mayor difusión de Internet2 en instituciones educativas y organizaciones de investigación.
2. Posibilita el desarrollo de aplicaciones mucho más rápidas.	2. El acceso a esta red se encuentra limitado.
3. Ofrece calidad y nitidez para la utilización de videoconferencias como medio de comunicación en tiempo real.	3. Requiere equipos sofisticados y de redes avanzadas para funcionar.
4. Permite escanear, procesar y compartir imágenes con rapidez. Además de almacenar y compartir gigantescas bases de datos de forma remota.	4. Las aplicaciones creadas para Intternet2 no pueden funcionar en las computadoras de usuarios finales como cualquier otra aplicación.

⁴² H.323, son una serie de recomendaciones del ITU, que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red. Es utilizado comúnmente para Voz sobre IP y para videoconferencia basada en IP.

4.5 Videoconferencia

Es una tecnología que proporciona un sistema de comunicación bidireccional de audio, video y datos que permite que las sedes receptoras y emisoras mantengan una comunicación simultánea interactiva en tiempo real a cualquier parte del mundo sin trasladarse a un punto de reunión.

Componentes de una videoconferencia

1. Red de comunicaciones: es necesaria para realizar cualquier tipo de comunicación, el emisor y receptor deben contar con un medio de transmisión, el cual, tiene que ser digital, bidireccional y de alta velocidad.
2. Sala de videoconferencia: es el área especialmente acondicionada en la cual se alojará el personal de videoconferencia, así como también, el equipo de control, audio y video, que permitirá capturar y controlar las imágenes y los sonidos que habrán de transmitirse.
3. Codec: las señales de audio y video se encuentran en forma de señales analógicas, por lo que para poder transmitir esta información a través de una red digital, ésta debe ser transformada mediante algún método a una señal digital, una vez realizado esto, se debe comprimir y multiplexar para su transmisión. El dispositivo que se encarga de este proceso es el CODEC (Codificador / Decodificador).

Características

- Requiere de algún tipo de software que soporte videoconferencia como, Netmeeting, Cuseeme, Skype, Google talk o Messenger.
- El equipo requiere de entrada de video o cámara web.
- Es necesaria una salida de video, como, monitor, televisión o proyector.
- Requiere de una entrada y salida de audio, micrófono, reproductor CD/DVD, bocinas, audífonos o auricular.
- Algunos protocolos que utiliza son los siguientes:
 - **H.324** Para voz, video y datos a través de líneas de teléfono analógico regulares.
 - **H.320** Para transmitir contenido multimedia (Audio/Video/Datos) a través de redes basadas en ISDN.

- **H.264** Es un estándar para codificación avanzada de video (compresión de video).
- **H.262** Es un estándar para la compresión de video, también es llamado MPEG-2, el DVD estándar ocupa esta codificación de video.
- **H.323** Es el conjunto de protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

En la siguiente tabla (tabla 4.11) se muestran las ventajas y desventajas del uso de videoconferencias.

Tabla 4.11 Ventajas y desventajas del uso de videoconferencia.

Ventajas	Desventajas
1. Permite reunir personas situadas en diferentes lugares geográficos, lo que implica un ahorro de dinero.	1. Hardware muy costoso.
2. Aumenta la productividad y evita la pérdida de tiempo.	2. Renta de canales de comunicación.
3. Educación a distancia.	3. Se necesitan espacios adecuados para el equipo.
4. Obtener soporte inmediato en productos o servicios extranjeros.	4. Requiere servicios de mantenimiento e infraestructura.

4.6 Qué es la evaluación de proyectos

Un proyecto es la búsqueda de una solución inteligente al planteamiento de un problema con tendencia a resolverse.

La evaluación de un proyecto es un proceso que se encarga de identificar, cuantificar y valorar los costos y beneficios que se generen de éste en un determinado periodo de tiempo.

Así, la evaluación de un proyecto tiene por objetivo conocer su rentabilidad económica y social, de tal manera que se asegure resolver una necesidad humana en forma eficiente, segura y rentable. Por lo cual, se le considera como una actividad orientada a mejorar la eficacia de los proyectos en relación con sus fines, además de promover mayor eficiencia

en la asignación de recursos. Entonces se precisa que la evaluación de proyectos no es un fin en sí misma, más bien es un medio para optimizar la gestión de los proyectos.

Si se presentan varias alternativas de inversión, la evaluación de proyectos es un medio útil para fijar un orden de prioridad entre ellas, seleccionando los proyectos más rentables y descartando los que no lo son con el fin de llegar a una eficiente asignación de recursos.

Así surgen distintos tipos de evaluación que se describen a continuación:

a) Tipos de evaluación de proyectos

1. Según el nivel de gestión:

- Política – Estratégica: trata de la parte social y política así como su consistencia para trascender en el tiempo y que sea en cierta forma equitativo.
- Administrativa: se refiere a la racionalización de todos los recursos, el logro de sus planes, objetivos, metas, actividades y programas.
- Técnica: es una mezcla de lo anterior y lo propio, ya que incide hoy en día al mejor logro de los dos puntos anteriores. Dependerá de cada ciencia qué enfoque científico y técnico aplicará.

2. Según la naturaleza de la evaluación:

- Evaluación privada: está conformada también por la evaluación económica, la cual asume que el proyecto está totalmente financiado con capital propio, por lo que no hay que pedir ningún tipo de crédito y por otro lado, la evaluación financiera que incluye el financiamiento externo.
- Evaluación social: aquí los puntos relevantes son los bienes y servicios reales utilizados y producidos por el proyecto.

3. Según el momento en que se realiza:

- Evaluación ex – ante: se realiza antes de la aprobación del proyecto y busca conocer su pertinencia, viabilidad y eficiencia potencial. Este tipo de evaluación consiste en seleccionar de entre varias alternativas técnicamente factibles a la que produce el mayor impacto al mínimo costo.
- Evaluación de proceso, operativa, de medio término o continua: se realiza durante el desarrollo del proyecto y guarda estrecha relación con el

monitoreo del proyecto. Con lo cual se puede conocer el avance de los objetivos.

- Evaluación *ex – post*, de resultados o de fin de proyecto: se lleva a cabo cuando el proyecto es concluido. Se enfoca en indagar el nivel de cumplimiento de los objetivos, asimismo busca demostrar que los cambios producidos son consecuencia de las actividades del proyecto (exclusivamente o en interacción con otras fuentes); para lo que recurre a un diseño experimental. No sólo indaga en cambios positivos, también analiza efectos negativos e inesperados.
- Evaluación de impacto: es la que se enfoca en los cambios permanentes y las mejoras de la calidad de vida producidos por el proyecto, es decir, conoce la sostenibilidad de los cambios alcanzados y los efectos imprevistos (positivos o negativos).

Cabe mencionar que las evaluaciones *ex – ante* y *de proceso* son consideradas como evaluaciones formativas debido a que se producen mientras se da la preparación o ejecución del proyecto y sus conclusiones sirven para optimizar la ejecución del mismo.

Las evaluaciones *de resultados* y *de impacto* son conocidas como evaluaciones sumativas que ocurren al culminar el proyecto, permitiendo que sus conclusiones sirvan para ser transferidas a otras experiencias pero ya no podrán tener una aplicación directa en el proyecto que ha concluido.

b) Criterios utilizados para evaluar proyectos

- Pertinencia o relevancia: se encarga de observar la congruencia entre los objetivos del proyecto y las necesidades identificadas y los intereses de la población e instituciones.
- Eficacia: es el grado en que se han cumplido los objetivos.
- Eficiencia: muestra el modo en que se han organizado y empleado los recursos disponibles en la implementación del proyecto.
- Sostenibilidad: establece la medida en que las instituciones mantienen vigentes los cambios logrados por el proyecto una vez concluido.

c) Requisitos que debe cumplir una buena evaluación de proyectos

- Objetivo: se deben medir y analizar los hechos definidos tal como se presentan.

- **Imparcial:** la generación de conclusiones del proceso de evaluación debe ser neutral, transparente e imparcial. Es decir, que quien realiza la evaluación no debe tener intereses personales o conflictos con quien ejecuta el proyecto.
- **Válido:** debe medirse lo que se ha planificado medir, respetando las definiciones establecidas.
- **Confiable:** las mediciones y observaciones deben ser registradas adecuadamente.
- **Creíble:** cada una de las partes involucradas en el desarrollo del proyecto deben tener confianza y certeza de la identidad e imparcialidad de todos los participantes de la evaluación.
- **Oportuno:** debe realizarse en el momento adecuado, evitando los efectos negativos que produce el paso del tiempo
- **Útil:** deberá elaborarse en un lenguaje conciso y directo, entendible para todos los que lo lean para que puedan tener conocimiento de la situación del proyecto.
- **Participativo:** debe incluirse a todos los involucrados en el proyecto, reflejando así sus experiencias, necesidades, intereses y percepciones.
- **Retroalimentador:** debe garantizar la diseminación de los hallazgos y su asimilación por parte de los involucrados en el proyecto.
- **Costo:** debe establecerse una relación positiva entre su costo (económico, de tiempo y de recursos) y su contribución en valor agregado para la experiencia de los involucrados en el proyecto.

d) Preparación de proyectos

Preparar un proyecto significa la construcción de un flujo de costos y beneficios durante el proceso de evaluación. Este flujo tendrá como base la realización de los siguientes cinco estudios: de mercado, técnico, ambiental, legal y económico.

- **Estudio de mercado:** se analiza el comportamiento histórico de la demanda, oferta y precios de los bienes y servicios involucrados en el proyecto.
- **Estudio de factibilidad técnica:** se detallan y cuantifican los costos de inversión, mantenimiento y operación de la alternativa seleccionada. Además, se verifica si la tecnología es la más adecuada para llevar a cabo el proyecto.

- Estudio de factibilidad ambiental: se determina el impacto, negativo o positivo, y las acciones para prevenir o mitigar cualquier efecto adverso que el proyecto provoque en el ambiente.
- Estudio de factibilidad legal: se verifica que las acciones del proyecto estén dentro del marco jurídico vigente y por consiguiente, puedan llevarse a cabo.
- Estudio económico: se determina la conveniencia económica de llevar a cabo la alternativa seleccionada, mostrando los riesgos posibles de su ejecución.

e) Metodología

La metodología para la evaluación de proyectos para centros de cómputo es una adaptación del método tradicional, desarrollado en 1950 por la ONU (Organización de las Naciones Unidas).

Esta metodología consta de 4 etapas, las cuales se describen a continuación (ver figura 4.23):

1. Estudio de mercado o cuantificación de las necesidades del servicio: hace referencia a los servicios que se desean prestar, esto se basa en las necesidades del usuario y se consideran los recursos, dispositivos, personal y el objetivo de estos servicios como el almacenar, permitir, comunicar, compartir, etcétera.

La demanda del servicio se puede medir mediante:

- a) Relación de cada uno de los servicios que ofrece la red, con el tiempo se efectúa un análisis de regresión entre cada uno de los factores con el tiempo.
 - b) Efectuar una regresión múltiple asignando los bytes demandados como una dependiente de otros. Que puede ser, cantidad de usuarios, tiempo de respuesta, tiempo de años, etcétera.
 - c) Métodos cualitativos como encuestas.
2. Estudio técnico: se toma en cuenta la localización de las instalaciones, riesgos y daños del lugar físico donde se instalarán.

Se emplea el método de puntos ponderados (listado de los factores relevantes) donde se asigna un peso a cada factor.

3. Análisis económico: determina cuál es el monto de los recursos económicos necesarios para la realización del proyecto, debe tomar en cuenta los siguientes aspectos:
 - a) Determinación de los costos totales de prestación de servicios.
 - b) Inversión inicial, es decir, el costo de todos los activos tangibles e intangibles.
 - c) Depreciación y amortización.
 - d) Capital de trabajo, los ingresos que se perciben o si sólo es un apoyo para las otras actividades de la empresa.
 - e) Punto de equilibrio.
 - f) Balance general.
 - g) Financiamiento de la inversión.
 - h) Estado de resultado.
 - i) Determinación de la tasa mínima aceptable de rendimiento.

4. Evaluación económica: toma la decisión entre al menos dos alternativas posibles y que una persona o grupo seleccione aquella alternativa que, habiendo cumplido con todas las necesidades tecnológicas de operación tenga el menor costo. Se considera:
 - a) Obtener el valor neto tomando en cuenta el rendimiento esperado por el inversionista.
 - b) Analizar el rendimiento de la inversión y sus riesgos para así tomar una decisión sobre bases firmes.
 - c) Presentar el estado de equilibrio y los estados financieros anteriores.



Figura 4.23 Metodología de la evaluación de proyectos.

CAPÍTULO 5

Dirección



“Comienzo con la premisa de que la función del líder es producir más líderes, no más seguidores.”

Ralph Nader

5.1 Dirección general

Es la ejecución de los planes de acuerdo con la estructura organizacional mediante la guía de los esfuerzos del grupo social a través de la motivación, la comunicación y la supervisión.

Un ejecutivo es una empresa que guía y dirige el trabajo de un grupo de personas y que entrega resultados a través de la acción de éstas.

En toda dirección existe un proceso administrativo que consta de 2 partes (ver figura 5.1):



Figura 5.1 Partes del procesos administrativo de cualquier dirección.

A continuación se muestran características de cada una de las partes del proceso administrativo⁴³ (ver tabla 5.1).

Tabla 5.1 Características de las partes del proceso administrativo.

Parte del proceso administrativo	Características
Planeación	<ul style="list-style-type: none"> • Orientada hacia la construcción de objetivos específicos y medibles. • Basada en la información actual respecto al entorno y las expectativas futuras. • Involucra a los subordinados y asegura su comprensión e

⁴³ Gido. J. y Clements. J. Traducción: Peralta. P. (2006). Administración exitosa de proyectos, p. 292-309. (3ª ed.). México: Cengage Learning.

	<p>interacción.</p> <ul style="list-style-type: none"> • Asigna tareas, responsabilidades y plazos. • Establece la base para el control.
Organización	<ul style="list-style-type: none"> • Defínase como un conjunto de técnicas conducentes para obtener una empresa estructurada en forma tal que la correspondiente división de actividades y la debida organización de éstas permita una máxima rentabilidad. • Se adecúan los recursos para conseguir los objetivos. • Determinar funciones, relaciones, puestos de trabajo, clasificación de puestos, etcétera.
Integración	<ul style="list-style-type: none"> • Implementación de todos los recursos de hardware, software y recursos humanos. • Reclutamiento de personal. • Selección de recursos y personal. • Contratación. • Ascenso de puesto. • Evaluación de los recursos. • Compensación. • Capacitación.
Dirección	<ul style="list-style-type: none"> • Se define como la función para impulsar, vigilar y coordinar e impulsar las acciones de cada miembro de la organización para alcanzar los objetivos señalados en los planos. • Autoridad y mando. • Comunicación. • Delegación. • Supervisión.
Control	<ul style="list-style-type: none"> • Se define como las técnicas que permiten medir los resultados obtenidos en relación con los esperados, esto implica detección de desviaciones y corrección de las mismas. • Se considera el establecimiento de normas y criterios de desempeño. • Medición de resultados por desempeño. • Corrección de las desviaciones con respecto a los planes de la organización.

5.2 Habilidades directivas del administrador

La administración es un proceso que comprende la coordinación e integración de actividades de trabajo para que se lleven a cabo eficientemente por medio de las personas implicadas en determinado proyecto, para lograr lo anterior es necesario desarrollar habilidades administrativas las cuales plantean los siguientes puntos:

1. **Objetivo:** Resultados por alcanzar en un campo determinado.
2. **Meta:** Resultado por alcanzar en un plazo determinado.
3. **Plan:** camino determinado de acción para alcanzar una meta.

En el siguiente esquema se integran los aspectos clave que forman parte de la vida diaria de un administrador, algunas de las habilidades que requerirá para el éxito de sus actividades, los roles que deberá desempeñar y algunas de las labores administrativas que lo llevarán a participar de manera activa dentro de su grupo de trabajo (ver Figura 5.2).

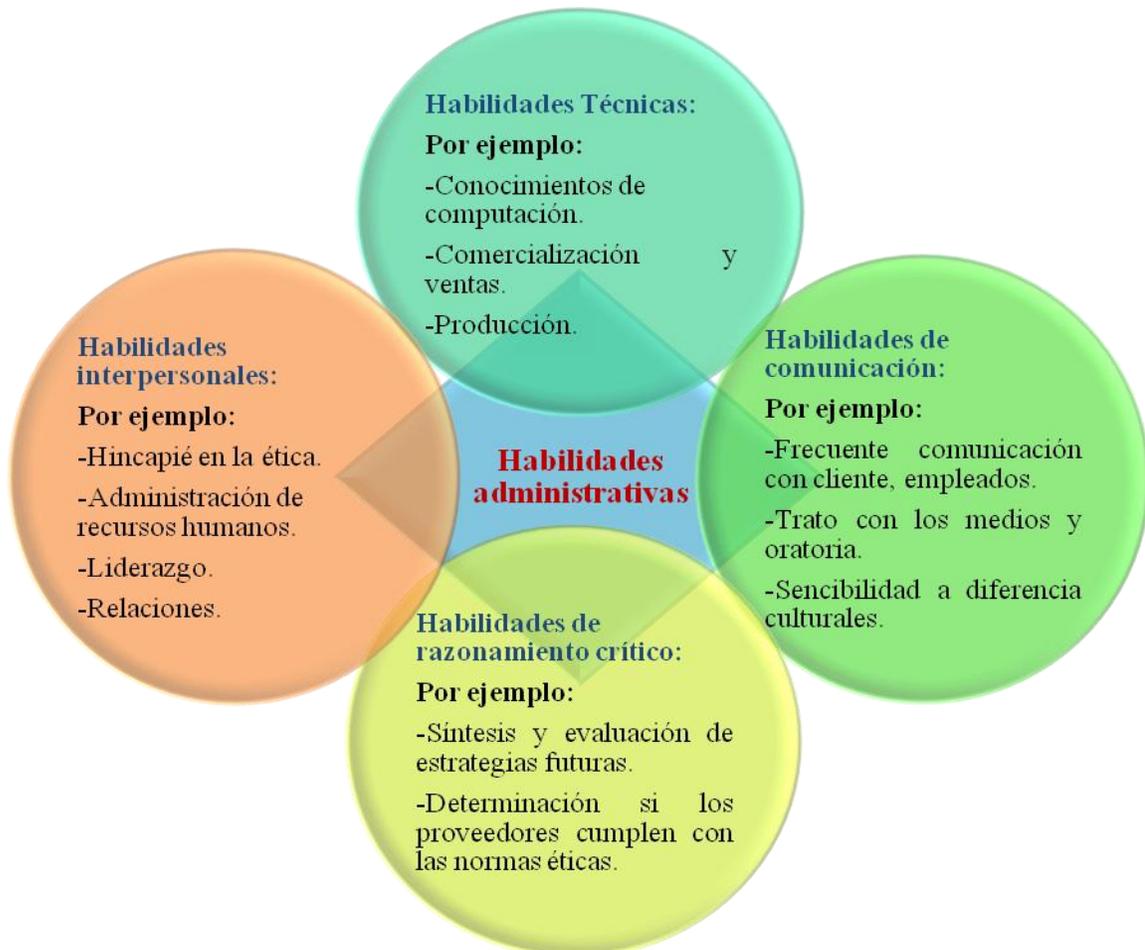


Figura 5.2 Habilidades administrativas.

5.3 Cómo lograr que un equipo de trabajo sea efectivo

Un trabajo colaborativo es el objetivo principal del trabajo en equipo, el cual se concibe como una estrategia que destaca fortalezas y debilidades propias, así como oportunidades y amenazas a las que se debe enfrentar en la práctica cotidiana. Por lo tanto, es de suma importancia ya que ayuda a las organizaciones a alcanzar los objetivos deseados.

Las razones más frecuentes para trabajar en equipo están relacionadas con factores que cubren diferentes tipos de necesidades, como lo son (ver tabla 5.2):

Tabla 5.2 Características para lograr un trabajo colaborativo.

a) Seguridad	<ul style="list-style-type: none"> Plena confianza y opinión favorable en que una persona o grupo será capaz y deseará actuar de manera adecuada en una determinada situación y pensamientos.
b) Estatus	<ul style="list-style-type: none"> Si se considera la posición de un miembro dado en un grupo como su lugar en el sistema, esta posición cuenta con un papel (rol) asociado.
c) Autoestima	<ul style="list-style-type: none"> Capacidad de desarrollar una confianza y un respeto saludables por uno mismo y por los demás.
d) Afiliación	<ul style="list-style-type: none"> Condición y sentimiento de pertenencia a un grupo.
e) Poder	<ul style="list-style-type: none"> Facultad, facilidad o potencia para llevar a cabo los planes y proyectos, así como de manejar recursos humanos.
f) Obtención de metas	<ul style="list-style-type: none"> Obtención satisfactoria de los objetivos planteados.
g) Empatía	<ul style="list-style-type: none"> La capacidad o proceso de penetrar profundamente, a través de la imaginación, dentro de los sentimientos y motivos del otro.
h) Asertividad	<ul style="list-style-type: none"> Habilidad social que indica la capacidad para poder expresarse socialmente de forma adecuada.

Es importante considerar que en un equipo de trabajo efectivo existe un nivel de conocimiento global del equipo y que todos los miembros son capaces de aportar y sugerir ideas, así como de escuchar dialogar y debatir. Cada uno está dispuesto a llegar a un acuerdo, se es capaz de vincularse y comprometerse con la organización. Existe una capacidad para ejercer el liderazgo; y es de suma importancia la credibilidad personal y profesional.

Así para que en determinado equipo de trabajo lo anterior sea posible y sean alcanzados los objetivos deseados por la organización se establece lo siguiente:

Métodos para el buen funcionamiento de un equipo de trabajo:

- **Satisfacción Laboral:** está relacionada al clima organizacional de la empresa y al desempeño laboral.
- **Comunicación:** es la base para las buenas relaciones organizacionales, cuando una organización mantiene una buena comunicación con su equipo de trabajo, obtiene buenos resultados.
- **Lluvia de ideas:** es una herramienta de trabajo grupal que facilita el surgimiento de nuevas ideas sobre un tema o problema determinado. La lluvia de ideas es una técnica de grupo para generar ideas originales en un ambiente relajado.
- **Grupos nominales:** es una estrategia para conseguir información de una manera estructurada, en la cual las ideas son generadas en un ambiente exento de tensión, donde las personas exponen sus ideas tanto de forma oral como escrita.
- **Técnica Delphi (no presencial):** consiste en encuestar (consultar) a un grupo de expertos de manera iterativa y en el anonimato, con el propósito de obtener sus juicios y propuestas, buscando puntos en común y organizando las respuestas para llegar a un consenso de sus opiniones.

Cabe destacar que en todo trabajo colaborativo existe un líder.

El liderazgo se refiere al conjunto de capacidades que un individuo tiene para influir en un conjunto de personas, haciendo que éste trabaje con entusiasmo en el logro de los objetivos comunes. En otras palabras, se entiende como la capacidad de tomar la iniciativa, gestionar, convocar, promover, incentivar, motivar y evaluar a un grupo o equipo.

Existe una regla fundamental en el liderazgo que es la base para que un buen líder, cualquiera que éste sea, lleve a cabo un liderazgo efectivo, la cual se enuncia a continuación: *“No pongas a las personas en tu lugar: ponte tú en el lugar de las personas”*.

Lo único que puede distinguir a un líder es que tenga seguidores: sin seguidores no hay líder.

Existen distintos tipos de liderazgo, los cuales se listan a continuación con sus respectivas características:

a) Según la formalidad en su elección:

- Liderazgo formal: preestablecido por la organización. Son elegidos por los jerarcas de la organización para llevar adelante, mediante su autoridad, los planes prefijados.
- Liderazgo informal: emergente en el grupo, ellos poseen el don del carisma. Esto es, son elegidos inconscientemente por el resto del grupo como líder.

b) Según la relación entre el líder y sus seguidores:

- Liderazgo dictador: fuerza sus propias ideas en el grupo en lugar de permitirle a los demás integrantes a hacerse responsables, permitiéndoles ser independientes. Es inflexible y le gusta ordenar, lo que provoca la destrucción de la creatividad de los demás.
- Liderazgo autocrático: el líder es el único en el grupo que toma decisiones acerca del trabajo y la organización del grupo sin tener que justificarlas en ningún momento. La comunicación es unidireccional: del líder al subordinado.
- Liderazgo democrático: el líder toma decisiones tras potenciar la discusión del grupo, agradeciendo las opiniones de sus seguidores, así también, los criterios de evaluación y las normas son explícitas y claras. Cuando hay que resolver un problema, el líder ofrece varias soluciones entre las cuales el grupo tiene que elegir.
- Liderazgo paternalista: tiene confianza por sus seguidores, toma la mayor parte de las decisiones entregando recompensas y castigos a la vez. Su labor consiste en que sus empleado trabajen más y mejor, incentivándolos, motivándolos e ilusionándolos a posibles premios si logran el objetivo.
- Liderazgo liberal (laissez faire): el líder adopta un papel pasivo, abandona el poder en manos del grupo. En ningún momento juzga ni evalúa las aportaciones de los demás miembros del grupo. Los miembros del grupo gozan de total libertad y cuentan con el apoyo del líder sólo si se lo solicitan.

c) Según el tipo de influencia del líder sobre sus subordinados:

- Liderazgo transaccional: los miembros del grupo reconocen al líder como autoridad y proporciona los recursos considerados válidos para el grupo.
- Liderazgo transformacional o carismático: el líder tiene la capacidad de modificar la escala de valores, las actitudes y las creencias de los seguidores.
- Liderazgo auténtico: es aquel líder que se concentra en liderarse en primer lugar a sí mismo. Tiene mucho autoconocimiento, ecuánime, espiritual, compasivo y generoso. Solo una vez que se lidera la propia mente se puede liderar a los demás.
- Liderazgo lateral: se realiza entre personas del mismo rango dentro de una organización o también se puede definir como el proceso de influir en las personas del mismo nivel organizacional para lograr objetivos en común.
- Liderazgo en el trabajo: en los negocios se evalúan dos características en los ejecutivos, con la intención de verificar su capacidad de dirección: por un lado, la aptitud y, por otro, la actitud. La primera se obtiene con el aprendizaje de nuevos métodos y procedimientos. Pero en muchos casos estos conocimientos no son aplicables, porque los gerentes carecen de una buena actitud, es decir, de un comportamiento adecuado que intente implementar dichos métodos.

d) Según la autoridad:

- Líder tradicional: es aquél que hereda el poder por costumbre o por un cargo importante o que pertenece a un grupo familiar de élite que ha tenido el poder desde hace generaciones.
- Líder legítimo: se trata de una persona que adquiere el poder mediante procedimientos autorizados en las normas legales.
- Líder ilegítimo: el líder adquiere su autoridad a través del uso de la ilegalidad. A este tipo de líder ni si quiere se le puede considerar como tal, ya que, una de las principales características del liderazgo es la capacidad de convocar y convencer.
- Líder carismático: es el que tiene la capacidad de generar entusiasmo. Es elegido como líder por su manera de dar entusiasmo a sus seguidores.

e) Según el liderazgo desarrollador (ver figura 5.3):

- Líder autócrata: es aquel que asume toda la responsabilidad de la toma de decisiones, inicia las acciones, dirige, motiva y controla al subalterno.
- Líder emprendedor: adopta el estilo participativo utilizando la consulta para practicar el liderazgo. No delega su derecho a tomar decisiones finales y señala directrices específicas a sus subalternos, pero consulta sus ideas y opiniones sobre decisiones que les incumben.
- Líder liberal: el líder delega a sus subalternos la autoridad para tomar decisiones.
- Líder proactivo: este tipo de liderazgo promueve el desarrollo del potencial de las personas.
- Líder audaz: este tipo de persona es capaz de relacionarse con muchas instituciones y personas, persuasivo, crítico, con mirada positiva. Tiene la capacidad de consultar a las demás personas para luego tomar decisiones.



Figura 5.3 Liderazgo desarrollador.

f) Liderazgo según sus habilidades:

- Liderazgo individual (ejemplo a seguir).
- Liderazgo ejecutivo (planeamiento, organización, dirección y control de un proyecto).
- Liderazgo institucional: tiene a su cargo toda una institución de tal manera que de él depende el estatus de la misma, también delega responsabilidades.

5.4 Definición de conflicto

Es un proceso que se inicia cuando una parte percibe que otra ha afectado de manera negativa o que está a punto de afectar alguno de sus intereses.

Un conflicto humano es una situación en que dos o más individuos o grupos con intereses contrapuestos entran en confrontación, oposición o emprenden acciones mutuamente antagonistas, con el objetivo de neutralizar, dañar o eliminar a la parte rival, para lograr así la consecución de los objetivos que motivaron dicha confrontación.

Los conflictos interpersonales e inter-grupales se presentan en todas las organizaciones y son parte de las relaciones sociales, ejemplos de ellos se dan entre individuos de un mismo grupo, una persona y su jefe, entre uno o más departamentos de una organización, entre el sindicato y la administración, etcétera.

Existen dos enfoques principales que definen lo que es un conflicto. Uno de ellos es el clásico o tradicional, que ha prevalecido hasta hoy. El segundo es un enfoque más reciente y se conoce como enfoque inter-relacional (ver tabla 5.3):

Tabla 5.3 Enfoques con los que se puede observar un conflicto

Enfoque	Descripción
Tradicional	Supone que todo conflicto es malo, es visto negativamente y es utilizado como sinónimo de violencia, destrucción e irracionalidad.
Inter-relacional	Sostiene que el conflicto es una consecuencia natural y parte de la vida cotidiana en todos los grupos y organizaciones.

A partir de estos dos enfoques surge la siguiente clasificación de los conflictos:

- **Funcionales:** Permiten llegar a un acuerdo por el bien del grupo, va encaminado a los intereses colectivos. “Conflicto positivo”.
- **Disfuncionales:** no permiten llegar a acuerdos, los miembros del grupo creen tener la razón y quieren imponer su verdad, van encaminando a intereses personales. “Conflicto negativo”.

Dentro de un conflicto las personas pueden adoptar las siguientes actitudes (ver tabla 5.4):

Tabla 5.4 Actitudes durante el conflicto.

Intención	Característica
Competidor	En busca de la satisfacción de los propios intereses independientemente del impacto que produzca en las otras partes del conflicto.
Colaborador	Situación donde las partes de un conflicto desean satisfacer plenamente los intereses de ambas partes.
Evasivo	Se observa el deseo de retirarse de un conflicto o acabarlo, tratando de ignorar el conflicto y evitando a las personas con quienes no se está de acuerdo.
Acomodático	Implica la disposición de una de las partes para colocar los intereses de la otra parte por encima de los propios con objeto de conservar la relación.
Conciliación	Situación donde las partes en conflicto están dispuestas a ceder en algo.

Un conflicto sigue una secuencia de pasos, los cuales se muestran en el siguiente diagrama (figura 5.4):

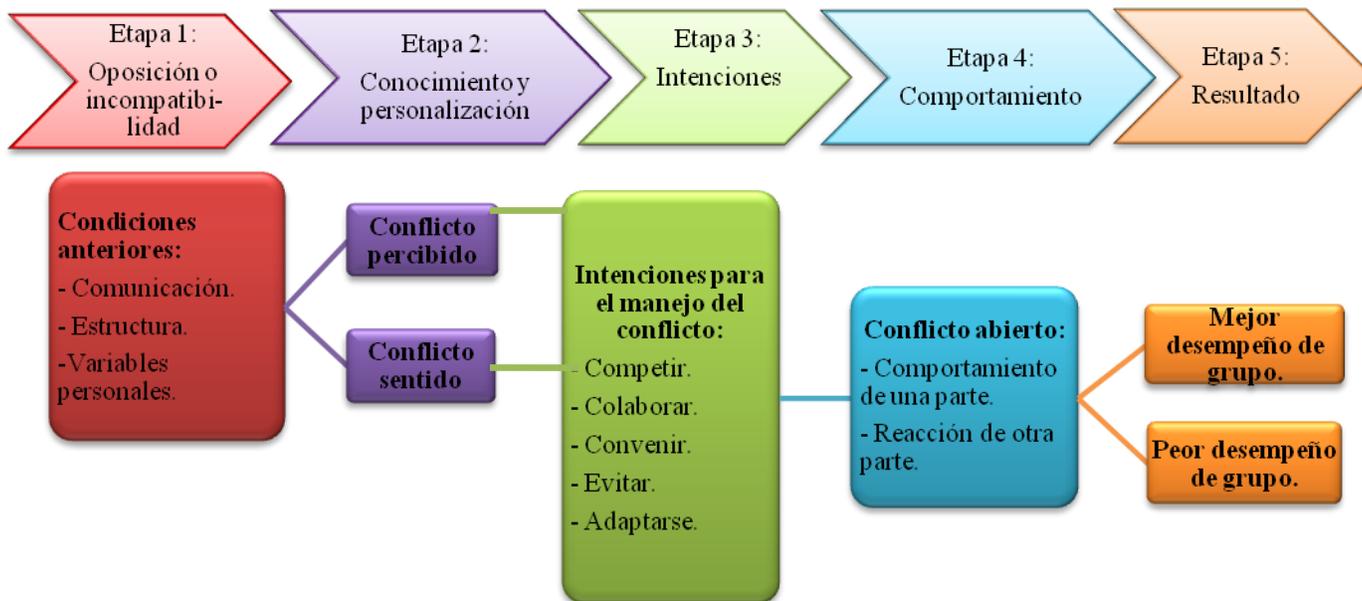


Figura 5.4 Etapas del proceso de un conflicto.

Una vez que un conflicto ha sido generado es necesario buscar la forma de solucionarlo o bien llegar a un acuerdo, es por ello que surgen ciertas habilidades para poder resolverlos.

Existen diferentes alternativas para resolver los conflictos. Algunas van desde las radicales que pretenden eliminarlos, pasando por las que aceptan su existencia y proponen el uso de métodos pacíficos. A continuación se listan las principales formas para solucionar un conflicto:

- Eliminar a los adversarios.
- Por agotamiento, cuando el conflicto se prolonga y los involucrados se cansan.
- Porque los afectados deciden buscar una salida negociada.
- Porque una tercera parte interviene ayudando a buscar una solución.

Una forma bastante conocida y utilizada para resolver conflictos es a través de la intervención de una tercera parte no involucrada (mediador) directamente en el conflicto, o lo que se conoce como "mediación", no se trata de que el mediador imponga soluciones o le otorgue la razón a una u otra parte sino de buscar satisfacer las necesidades de las partes en disputa, regulando el proceso de comunicación, para ello se siguen los siguientes pasos:

2. **Presentación:** es la fase dedicada a crear confianza entre el equipo de mediación y las partes implicadas en el conflicto, también se presenta el proceso y las normas a seguir en la mediación.
3. **Cuéntame:** es la fase en la que las personas que son mediadas exponen su versión del conflicto con los sentimientos que le acompañan. Las partes han de ser escuchadas.
4. **Aclarar el problema:** fase dedicada a identificar los nudos conflictivos, los puntos de coincidencia y de divergencia del mismo.
5. **Proponer soluciones:** aquí se realiza la búsqueda creativa de soluciones y la evaluación de las mismas por las partes.
6. **Llegar a un acuerdo:** se definen con claridad los acuerdos. Éstos han de ser equilibrados, específicos, posibles. También se suele dedicar un tiempo a consensuar algún procedimiento de revisión y seguimiento de los mismos.

Se usa también otra metodología conocida como "Construcción de paz", la cual ha sido muy utilizada por muchas organizaciones en diferentes partes del mundo (ver tabla 5.5).

Tabla 5.5 Construcción de la Paz.

Tipo de acción	Acción
Mantenimiento de la paz	<ul style="list-style-type: none">• Se usa en caso de conflictos violentos.• Su objetivo es detener la violencia y agresión entre los involucrados.
Realización de la paz	<ul style="list-style-type: none">• Mantener la calma y tranquilidad.• Facilitar procesos de negociación.
Construcción de la paz	<ul style="list-style-type: none">• Intenta resolver las causas que dieron origen a los conflictos.

El tipo de acciones que se tomen depende del tipo de situación, pero sobre todo de la buena voluntad de los sectores involucrados para buscar soluciones duraderas al conflicto. En otras palabras, si no se trabaja para modificar las causas, difícilmente se resuelve el conflicto.

CAPÍTULO 6

Control



“Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores”

Kevin Mitnick.

6.1 Definiciones de seguridad en redes

Empresas, organizaciones y personas tienen la necesidad de utilizar a diario redes de datos para poderse comunicar, es por ello, que la seguridad de las redes se torna esencial para proteger la información enviada por este medio.

Aunado al crecimiento de las redes, también crecieron las formas en que se puede violar la seguridad de éstas, poniendo en riesgo los bienes de determinada empresa o persona. La importancia que posee la protección de un bien radica en qué tan necesario o valioso sea para el propietario, ya que la información representa el principal activo de toda empresa u organización, surge el concepto de seguridad informática, y de la mano con éste, el de seguridad en las redes.

Para poder entender qué es la seguridad de una red, es necesario definir la palabra seguridad, la cual significa conjunto de protecciones que permiten resguardar un bien. Por lo que, la seguridad en redes, se define como el conjunto de protecciones para resguardar toda información transmitida por medio de las redes de computadoras.

De esta manera se ilustra el siguiente diagrama que permite definir e identificar el conjunto y subconjuntos de las definiciones de seguridad (ver figura 6.1).

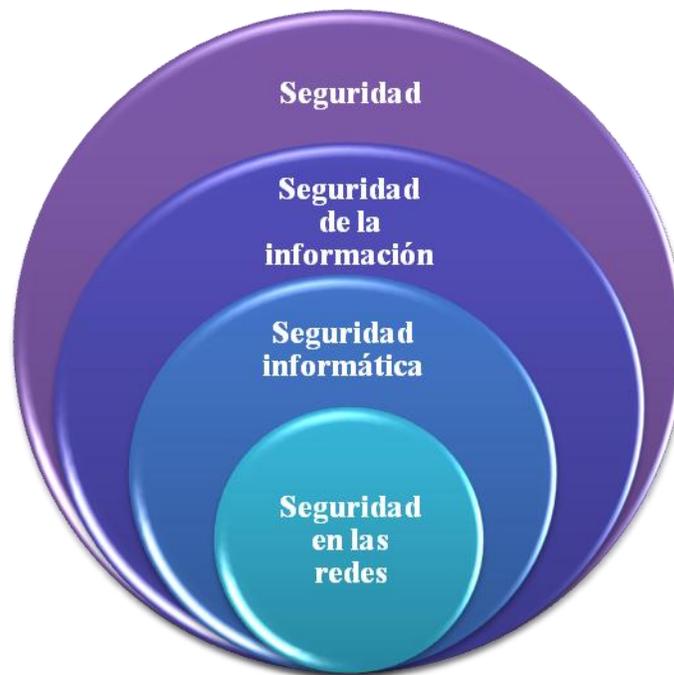


Figura 6.1 Diagrama de definiciones de seguridad.

- a) **Seguridad:** conjunto de protecciones que permiten resguardar un bien.
- b) **Seguridad de la información:** se encuentra sumamente relacionada a las medidas implementadas para la prevención y protección de la información, de daños como la modificación, el robo, la revelación a personal no autorizado y la destrucción.
- c) **Seguridad informática:** cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.
- d) **Seguridad en las redes:** ya que el activo más importante de las empresas es la información, se debe asegurar la privacidad de la misma y proteger de daños no intencionados como deliberados.

Sin embargo, para poder sumergirnos en el mundo de la seguridad y decidir qué herramientas son las adecuadas para proteger los bienes, en este caso la información, es necesario responder a las siguientes cuestiones (figura 6.2):



Figura 6.2 Cuestionamientos necesarios para la elección de herramientas de seguridad.

A continuación se definen las amenazas y vulnerabilidades que pueden atentar contra la información, así como los ataques a los que está expuesta:

1. Amenazas

Una amenaza es todo aquello que pretende o intenta destruir o dañar un bien. Se encuentra latente y representa sólo una posibilidad de poder manifestarse.

Existen cinco tipos de amenazas, las cuales se describen a continuación (ver figura 6.3):

a) **De humanos:** es la fuente de amenaza más latente. Puede ocurrir debido a:

- Descuido.
- Negligencia.
- Inconformidad.
- Ignorancia.

Pueden ser ejecutadas a través de:

- Ingeniería social: se manipula a las personas para convencerlas de que ejecuten acciones que normalmente no realizan, de tal forma que revelen datos que permitan superar las barreras de la seguridad.
- Ingeniería social inversa: consiste en que el intruso se gane la confianza del usuario, haciéndolo creer que de alguna manera es capaz de brindarle ayuda, de esta forma podrá solicitar información para solucionar el problema tanto del usuario como el suyo.
- Robos: es común que empleados roben información de la organización, ya que es muy sencillo copiarla, esto puede ser por descontento o bien con fines de lucro.
- Fraude: a través de la compañía y de su equipo los empleados pueden realizar sustracciones de dinero.
- Sabotaje: es el peligro más temido dentro de una organización, lo puede realizar un empleado o una persona ajena a la empresa.

Es común que se recurra a los imanes para afectar la integridad de la información. También partículas de metal o gasolina pueden introducirse por los conductos de aire acondicionado o bien cortar las líneas de comunicación.

b) **De tipo lógico:** se refiere a códigos mal programados, los cuales pueden causar problemas o código malicioso, por ejemplo:

- Caballos de Troya: es un programa aparentemente útil que contiene funciones escondidas y una vez que es ejecutado puede explotar los privilegios de un usuario, permitiendo al intruso acceder al equipo de manera remota.
 - Virus: son programas que tienen la capacidad de replicarse o copiarse a sí mismos. Se pueden propagar a través de archivos adjuntos en un correo electrónico, una transferencia por FTP (File Transfer Protocol - Protocolo de Transferencia de Archivos), unidades de almacenamiento o bien por descargas de Internet.
 - Gusanos: son programas que se propagan ellos mismos a través de la red. Un gusano hace una copia de sí mismo y lo realiza cuando es ejecutado.
- c) **Errores de hardware:** se da por fallas físicas que presente cualquier elemento de hardware de los dispositivos que forman parte de un sistema. Algunas de ellas pueden ser:
- Deterioro de los equipos por el uso.
 - Falla del suministro de energía.
- d) **Errores de la red:** sucede cuando alguno de los elementos de la red falla, pueden ser de tipo lógico, como amenazas de monitorización, escaneo, ataques de autenticación, obtención de contraseñas, denegación de servicios, fisgoneo, uso de diccionarios para obtener contraseñas, o bien, pueden ser físicos, como interferencia, cables cortados o dañados que pueden alterar la integridad de los datos.
- e) **Desastres naturales:** provienen de las fuerzas naturales y el ser humano no tiene control de su ocurrencia. Algunos de ellos son:
- Inundaciones.
 - Terremotos.
 - Incendios.
 - Viento.
 - Tormentas eléctricas.

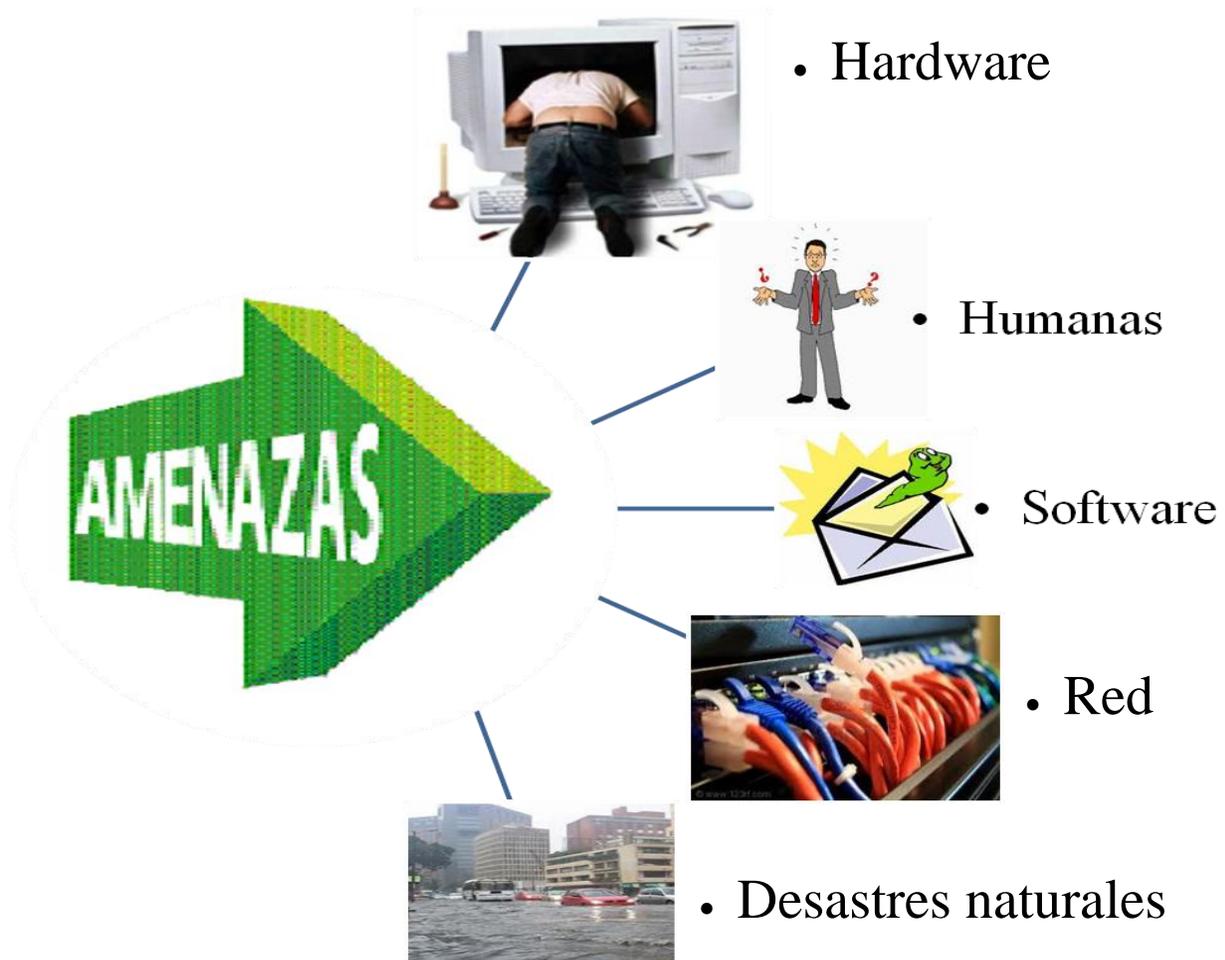


Figura 6.3 Tipos de amenazas.

2. Vulnerabilidades

Una vulnerabilidad es una debilidad que puede ser o es explotada por una o varias amenazas. En pocas palabras, se trata de un “talón de Aquiles” del sistema o del activo.

Una vulnerabilidad se puede identificar porque es todo aquello que no se ha considerado o que no se ha implementado, pudiendo causarle un daño al activo al ser explotado por una amenaza.

Una amenaza puede explotar una o más vulnerabilidades. Existen seis tipos de vulnerabilidades, los cuales se mencionan a continuación:

- a) **De humanos:** están relacionadas con cualquier error que pueda presentarse como producto de descuidos o intencionales por el personal, por ejemplo:

- No tener personal suficiente para cubrir todas las áreas.
 - Descuido.
 - Cansancio.
 - Maltrato al personal.
 - Falta de capacitación.
 - No contar con guardias de seguridad.
 - No tener un control de acceso.
- b) **De tipo lógico:** se refiere a las fallas o debilidades existentes en los programas de un sistema que facilite las labores de intrusión al mismo, incluye todos los errores de programación en el sistema operativo u otros tipos de aplicaciones que permitan atacar al sistema operativo desde la red, explotando así la vulnerabilidad en el sistema.
- c) **Errores de hardware:** se presentan cuando no se tienen las precauciones necesarias con los equipos de hardware, como por ejemplo, olvidar verificar las características técnicas de los dispositivos junto con sus especificaciones, por lo que, se puede exponer al equipo a un mal uso, incorrecta instalación o en el peor de sus casos daño de éste.
- d) **Errores de la red:** debido al enorme crecimiento de las redes y la necesidad de intercambiar información y recursos a través de ellas, es que aumenta considerablemente el riesgo al que se encuentra sometido el sistema. Ejemplo de ello, son:
- Interceptar información que es transmitida desde o hacia el sistema.
 - Fallas debido a una mala estructura y diseño del cableado estructurado por no seguir los estándares necesarios.
 - No contar con plantas emergentes.
- e) **Desastres naturales:** se refiere al grado en que el sistema puede verse afectado por desastre naturales o ambientales, tales como terremotos, inundaciones, lluvias eléctricas, etcétera. Algunos ejemplos de estas vulnerabilidades son los siguientes:
- No contar con un respaldo de la información en otro lugar geográfico.
 - No disponer de reguladores, UPS⁴⁴ (Uninterrupted Power System – Sistema de Alimentación Ininterrumpida) o plantas de energía eléctrica alterna.

⁴⁴ UPS: es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de sus funciones es filtrar las subidas y bajadas de voltaje.

- No contar con un sistema adecuado de ventilación y calefacción para que los equipos trabajen en temperaturas de 18 y 21 °C y se mantenga la humedad entre 48 y 65 %.
- Que no se cuente con materiales contra incendios, como el piso y las paredes.
- No contar con el equipo para la extinción de incendios.

f) **Física:** hace referencia al control de acceso físico al lugar donde se encuentra el sistema para robar, modificar o destruir el mismo.

3. Ataques

Un ataque se define como la culminación de una amenaza, es decir, cuando una amenaza se aprovecha de una o varias vulnerabilidades, por lo que se presenta un daño ya sea en menor o mayor medida.

Los ataques se pueden clasificar de varias formas:

Clasificación de ataques:

- a) En algunas ocasiones el daño es visible, sin embargo, en ocasiones, es posible que no se note que se ha atacado. Por lo que los ataques se pueden clasificar como pasivos y activos. (Ver figura 6.4)

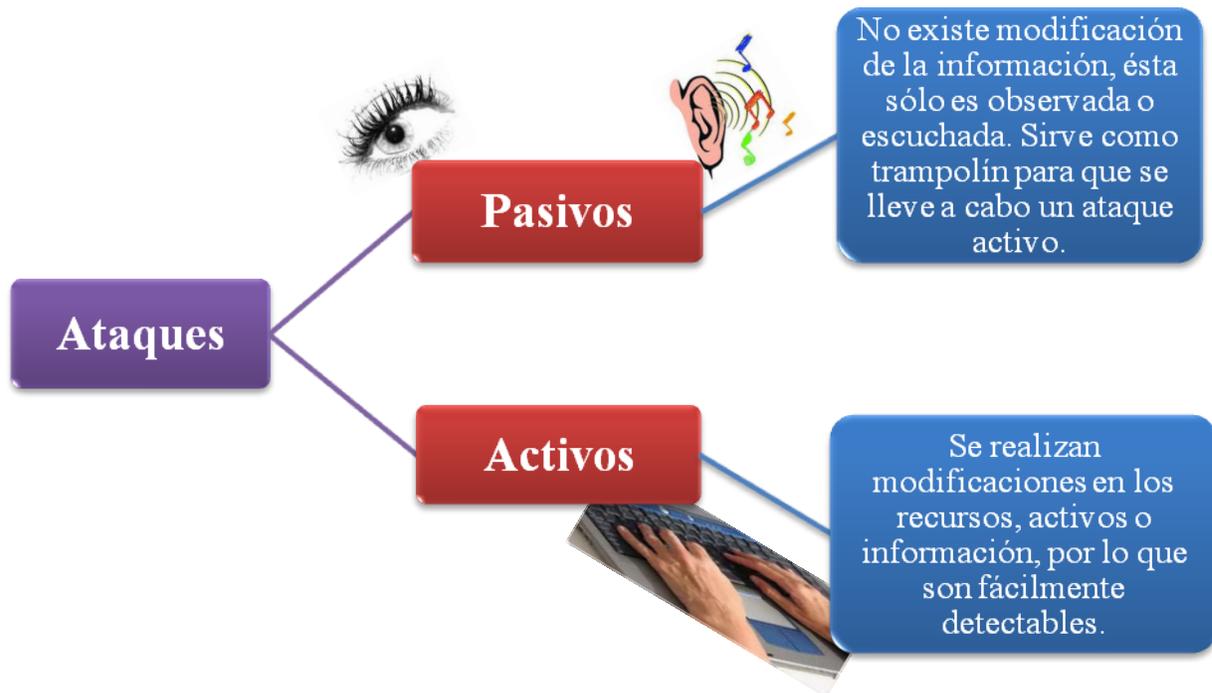
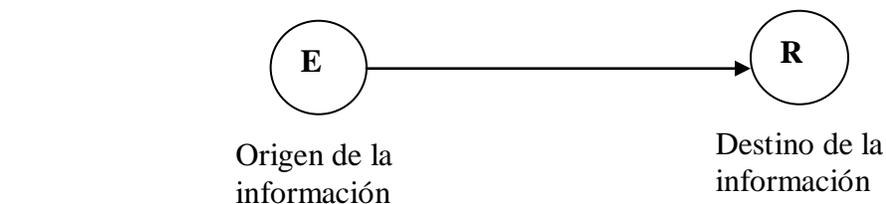


Figura 6.4 Clasificación de ataques.

- b) Otra clasificación de los ataques se da con base en el efecto que el ataque le causa al flujo normal de la información (figura 6.5), ya que no debe existir ningún tipo de obstáculos para que la información llegue al destinatario.



Donde:

E = emisor

R = receptor

P = perpetrador

Figura 6.5 Flujo normal de información.

Existen cuatro categorías que se listan en la siguiente tabla (ver tabla 6.1):

Tabla 6.1 Clasificación de ataques

Ataque	Diagrama
<p>1. Interrupción: un recurso del sistema es destruido se torna no disponible. Atenta contra la disponibilidad.</p>	
<p>2. Modificación: se refiere a que una entidad no autorizada (perpetrador) acceda al recurso y haga cambios en dicho recurso. Atenta contra la integridad.</p>	
<p>3. Suplantación o falsificación: un perpetrador inserta objetos falsificados en el sistema. Atenta contra la autenticidad.</p>	
<p>4. Intercepción o destrucción: un perpetrador consigue acceso a un recurso, sólo escucha o lee la información sin que el emisor y el receptor lo sepan. Atenta contra la confidencialidad.</p>	

Para que un ataque se pueda llevar a cabo, se contemplan tres etapas principales (ver figura 6.6):

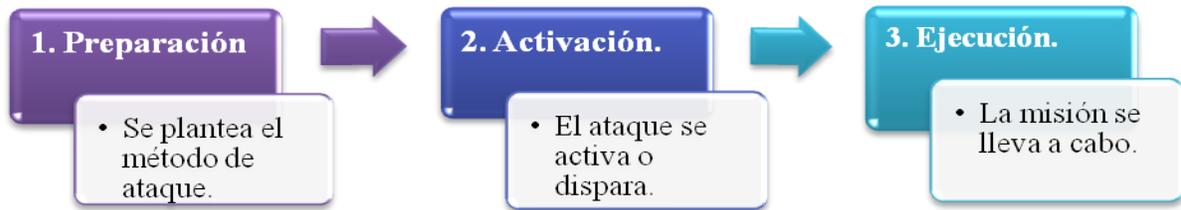


Figura 6.6 Método de ataque

4. Mecanismos de seguridad

Los mecanismos de seguridad también reciben el nombre de controles o herramientas de seguridad, pues permiten implementar uno o varios servicios de seguridad.

Un servicio de seguridad permite proveer un nivel de seguridad en la organización. Están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio. Los servicios de seguridad se clasifican en seis grandes rubros y los mecanismos utilizados se clasifican con base en el tipo de servicio que están implementando, esto es:

- a) **Integridad:** provee controles que aseguran que el contenido de los datos no haya sufrido modificación alguna, y que la secuencia de los datos se mantenga durante la transmisión, con lo que, se evita la inserción, borrado o cualquier tipo de modificación.
- b) **Confidencialidad:** asegura que sólo las personas autorizadas tengan acceso a los recursos. Mantiene la información secreta para proteger la información contra el descubrimiento intencional o accidental.
- c) **Disponibilidad:** se refiere a que las personas autorizadas puedan acceder a la información deseada cuando lo requieran y tantas veces como sea necesario.
- d) **No repudio:** evita que alguien niegue alguna actividad realizada.
- e) **Autenticación:** verifica que la persona o proceso es quien dice ser⁴⁵. La autenticación se realiza a través de:
 - Algo que se sabe, por ejemplo, una contraseña.
 - Algo que se tiene, como una identificación.

⁴⁵ Tanenbaum, A.S. (1997). *Redes de computadoras*, p. 785. México: Pearson Education.

- Algo que se es, ya sea la voz, la retina o la huella digital.
- f) **Control de acceso:** se podrá acceder a la información o servicio siempre y cuando se tengan los permisos para ello. Por lo que, cada entidad que requiera el acceso a cualquier recurso del sistema deberá identificarse y después autenticarse.
5. Otra clasificación de los mecanismos de seguridad, se basa, en el tipo de herramienta:
- a) Físicos, tales como, lector de huella digital, de retina, reconocedor de voz, etcétera. Es decir, son elementos tangibles.
 - b) Lógicos, como, firewall, antivirus, etcétera. Se trata de elementos intangibles.

6.2 Normatividad en seguridad informática

En seguridad existen estándares que permiten mantener un cierto nivel de protección de los bienes en las organizaciones, un estándar o norma es un documento que contiene especificaciones técnicas u otros criterios para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito, específicamente en el área de redes los más reconocidos a nivel mundial son:

a) Criterios Comunes

Los Criterios Comunes para la evaluación de seguridad de tecnología de la información (Common Criteria for Information Technology Security – CCIT-SE) mejor conocido como CC, fueron creados con base en criterios europeos, canadienses y norteamericanos, por lo cual, se definen como una norma internacional para evaluar la seguridad de los productos de tecnología, cuyo objetivo principal es proporcionar protección a la información como, no revelar secretos sin autorización, perder información por el uso y modificar la información.

Historia

Tienen como antecedente dos criterios de evaluación:

1. TCSEC (Trusted Computer Security Evaluation Criteria – Criterio de Evaluación de Seguridad de Cómputo Confiable), o mejor conocido como, el libro naranja. Tiene su origen en 1980 y establece la aplicación de políticas de seguridad del departamento de defensa de Estados Unidos. Se preocupa fundamentalmente de la confidencialidad de la información clasificada a nivel nacional.

- 2. ITSEC (Information Technology Security Evaluation Criteria – Criterio de Evaluación de la Seguridad de las Tecnologías de la Información), o mejor conocido como el libro blanco, surgió en 1991, proveía niveles de seguridad donde se definía la funcionalidad del producto desarrollado.

Al probar que tanto TCSEC como ITSEC, no eran satisfactorios, surge la iniciativa para crear un nuevo esquema de evaluación de la seguridad, de esta manera los CC reemplazan a TCSEC e ITSEC a finales de 1998.

En un principio surgió la versión 2.0 de CC y para agosto de 1999, se aprueba la versión 2.1 de CC la cual fue adoptada por la ISO y que actualmente se hace referencia a él como el estándar ISO/IEC 15408.

Dentro de la evaluación de las propiedades de seguridad de los productos intervienen tres grupos, los cuales se encuentran representados mediante la figura 6.7.

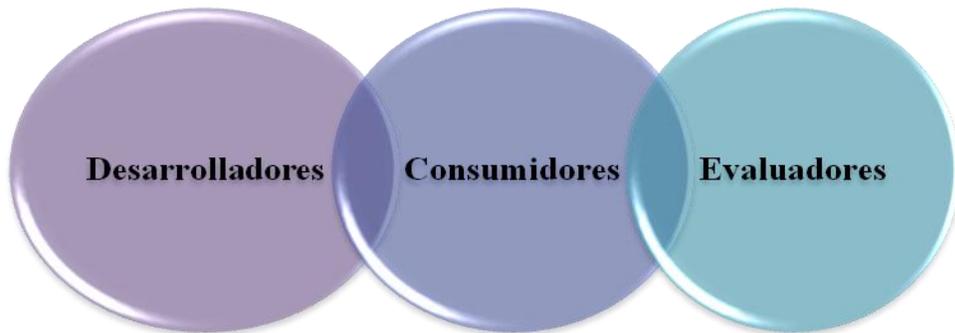


Figura 6.7 Grupos que intervienen en la evaluación de las propiedades de seguridad de los productos.

Estructura

Los criterios comunes están formados por tres partes (ver figura 6.8):



Figura 6.8 Partes fundamentales de los criterios comunes

- 1. Introducción general:** en esta parte se encuentran contenidos los conceptos generales y el formato de los criterios comunes. Se describe cómo fueron establecidos los CC y para quiénes están destinados. También incluye las estructuras y descripciones de los Perfiles de Protección (PP, Protection Profile) y metas de seguridad (ST, source target).
- 2. Requerimientos de seguridad funcional:** esta parte tiene como destino los usuarios y desarrolladores, ya que establecen un conjunto de componentes de seguridad funcional como un estándar que expresa los requerimientos de seguridad funcional para los productos de tecnologías de la información.

Se encuentran organizados en once clases que reciben el nombre de “Clases de requerimientos funcionales”, las cuales a su vez se encuentran divididas en una o más familias funcionales.

- 3. Requerimientos de garantía:** están enfocados en establecer el criterio de confiabilidad que los evaluadores tendrán para calificar el desempeño de los desarrolladores y sus productos.

Cuenta con siete niveles de evaluación de garantía (EAL, Evaluation Assurance Level) los cuales son usados como escala para clasificar la evaluación obtenida por los productos. Así un alto EAL especifica un nivel alto de confianza de que las funciones de seguridad del producto serán ejecutadas de manera correcta y efectiva.

Los CC siguen una metodología llamada Perfiles de protección (ver figura 6.9) que muestra lo que se requiere.

La metodología PP contiene un conjunto de requerimientos de seguridad, ya sea de los CC o indicados de forma explícita. Éstos fueron creados con el fin de presentar de manera rigurosa un determinado problema de seguridad y los requerimientos necesarios para la solución del mismo.

Un PP se define como un documento mediante el cual se diseña un esquema de seguridad, es decir, es un conjunto estándar de requerimientos de seguridad los cuales deben satisfacer los productos y sistemas de una organización con el objetivo de responder a las necesidades en el ámbito de la seguridad informática.

En palabras más sencillas, un PP es una descripción detallada de lo que requiere el usuario, se encarga de establecer lo que se necesita, por lo que, debe ser redactado con un lenguaje común, así como definir claramente las necesidades. (Ver figura 6.9)

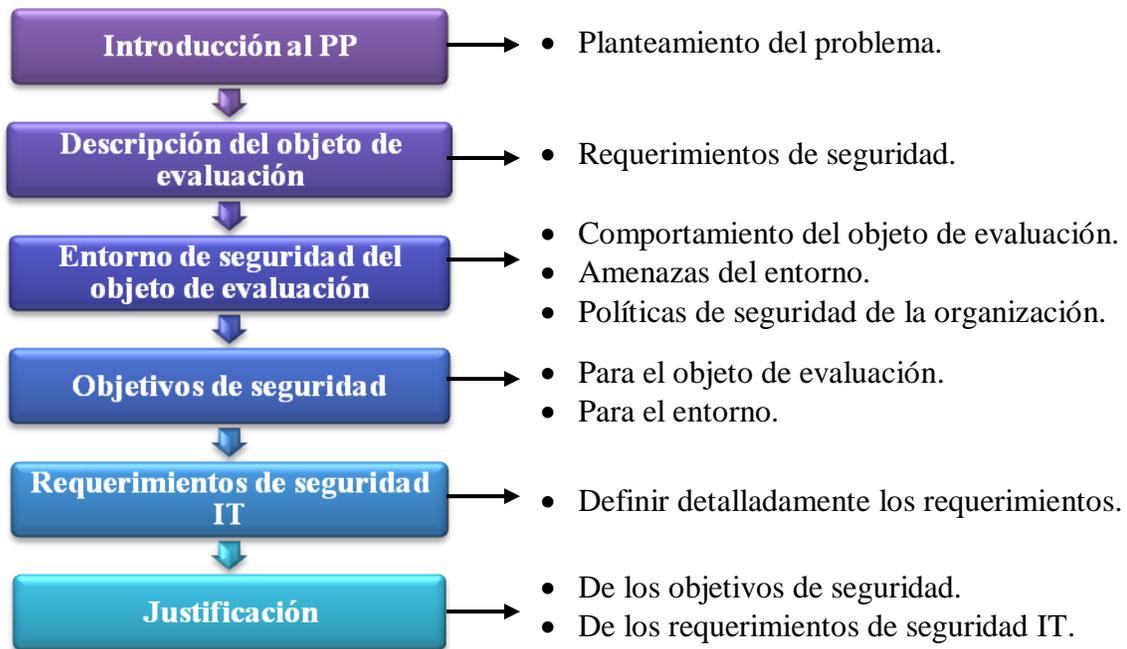


Figura 6.9 Pasos de la metodología de Perfiles de protección PP

Así mediante el uso de los CC se ofrecen ventajas tanto a consumidores como a desarrolladores:

1. Para los consumidores: mediante los resultados de las evaluaciones de seguridad deciden si el producto o sistema satisface sus necesidades de seguridad.
2. Para los desarrolladores: proveen medios para mostrar al mundo que se tiene un producto adecuado y seguro. Los CC proveen una guía detallada de la información y de los requerimientos de seguridad.

b) Serie ISO 27000

La serie ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO, e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Desde el año 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR⁴⁶ en España) es responsable de la publicación de importantes normas como:

⁴⁶ Asociación Española de Normalización y Certificación.

- 1979 Publicación BS 5750 - ahora ISO 9001.
- 1992 Publicación BS 7750 - ahora ISO 14001.
- 1996 Publicación BS 8800 - ahora OHSAS 18001.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1988, la que establece los requisitos de un sistema de seguridad (SGSI⁴⁷) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido, así como el año de publicación formal de la revisión. (Ver figura 6.10)

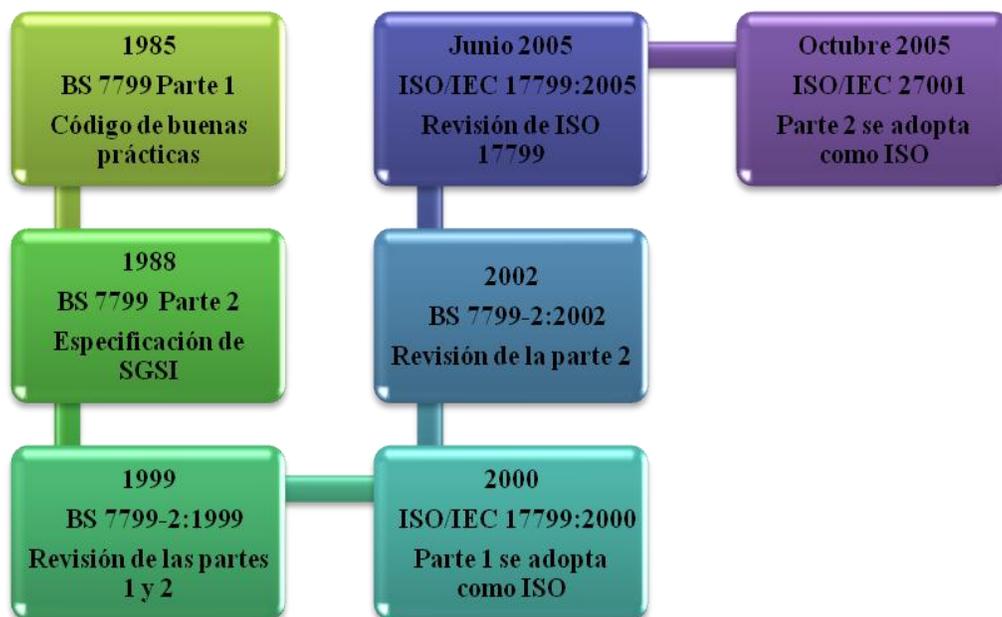


Figura 6.10 Evolución de la norma ISO/IEC 27001.

⁴⁷ Sistema de Gestión de la seguridad de la Información.

La serie ISO 27000 se encuentra formada por varias normas que aseguran que se han implementado medidas que garantizan la gestión adecuada de la seguridad de la información. Los rangos de numeración reservados para esta serie van de 27000 a 27019 y de 27030 a 27044. De los cuales se presenta una breve descripción en la siguiente tabla (ver tabla 6.2):

Tabla 6.2 Estándares que componen la serie ISO 27000

Estándar	Descripción
1. ISO 27000	Contiene los términos y definiciones empleadas en toda la serie 27000, ya que la aplicación de cualquier estándar requiere que el vocabulario esté claramente definido para evitar errores o ambigüedades.
2. ISO 27001	Se trata de la norma principal de la serie y contiene los requisitos requeridos para la implementación del sistema de gestión de seguridad de la información (SGSI). Proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.
3. ISO 27002	Conforma una guía de buenas prácticas que describe los objetivos de control y los controles recomendados para mantener e incrementar los niveles de seguridad de la información en la organización. No es certificable.
4. ISO 27003	Consiste en una guía de implementación de SGSI e informa acerca del uso del modelo PDCA (Modelo “Plan, Do, Control y Act”) y de los requerimientos de sus diferentes fases.
5. ISO 27004	Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y utilizar) del ciclo PDCA.
6. ISO 27005	Consiste en una guía de técnicas para la gestión de riesgos en la seguridad de la información. Se diseñó para apoyar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Esta norma servirá de apoyo a la ISO 27001 y a la implementación de un SGSI.
7. ISO 27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

8. ISO 27007	Consiste en una guía de auditoría de un SGSI.
9. ISO 27011	Proporciona una guía de gestión de seguridad de la información específica para el área de las telecomunicaciones. Está dirigida a los organismos que proporcionan procesos de apoyo e información en las telecomunicaciones, instalaciones de redes y líneas telefónicas, ya que dichos componentes suponen activos importantes para la empresa.
10. ISO 27031	Contiene una guía de continuidad de negocio en cuanto a tecnología de la información y comunicaciones.
11. ISO 27032	Proporciona una guía relacionada con la ciberseguridad.
12. ISO 27033	Se trata de una norma dividida en siete secciones: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPN's y diseño e implementación de seguridad en redes.
13. ISO 27034	Proporciona una guía de seguridad en aplicaciones.
14. ISO 27799	Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 27002. Aquí se definen las normas para apoyar la interpretación y aplicación en la salud informática de la norma ISO 27002 por lo que se dice que ISO 27799 es un complemento de la norma ISO 27002.

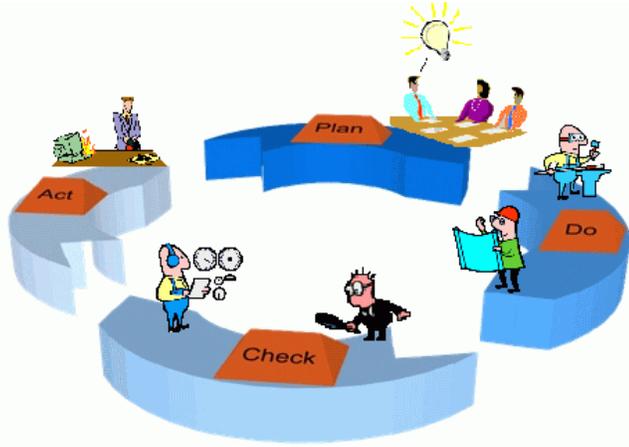
Por tratarse del estándar principal de la serie ISO 27000 a continuación se describe a mayor detalle el estándar ISO 27001:

ISO 27001

Se trata de un estándar internacional de sistemas de gestión de seguridad de la información, el cual permite a las organizaciones evaluar riesgos e implementar controles apropiados para preservar la confidencialidad, integridad y disponibilidad de la información.

El estándar 27001 se realizó con el fin de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad (SGSI) según el conocido “Ciclo de Deming” PDCA (Plan, Do, Check, Act – Planear, Hacer, Verificar, Actuar).

Donde el ciclo Deming se define como una estrategia de mejora continua de la calidad en cuatro pasos. (Ver figura 6.11).



Plan (planificar): establecer el SGSI.

Do (hacer): implementar y utilizar el SGSI.

Check (verificar): monitorear y revisar el SGSI.

Act (actuar): mantener y mejorar el SGSI.

Figura 6.11 Implementación de SGSI mediante el ciclo Deming.

Las secciones principales que conforman al estándar ISO 27001 se listan a continuación:

1. Políticas de seguridad: proporciona a la alta dirección apoyo para la seguridad de la información.
2. Organización de la seguridad: ayuda a administrar la seguridad de la información dentro de la empresa u organización.
3. Clasificación y control de activos: provee las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la organización.
4. Seguridad del personal: necesaria para reducir los riesgos de errores humanos, robo, fraude o mal uso de las instalaciones y equipo.
5. Seguridad física y ambiental: previene el acceso físico no autorizado a los sistemas de información, así como posibles daños a las instalaciones y a la información del negocio.
6. Administración de comunicaciones y operaciones: permite garantizar la operación correcta y segura de las instalaciones de procesamiento de la información.
7. Control de acceso: previene el acceso lógico y cambio, no autorizado, a la información y a los sistemas de información, otorgando confidencialidad en la información, para evitar interrupciones en los procesos normales de producción.

8. Desarrollo y mantenimiento de los sistemas: permite incorporar la seguridad a los sistemas de información.
9. Gestión de Incidentes en la Seguridad de la Información: define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas.
10. Administración de la continuidad del negocio: contrarresta las interrupciones a las actividades del negocio y protege los procesos críticos del negocio contra los efectos causados por fallas mayores o desastres.
11. Conformidad: contribuye a evitar infracciones a las leyes civiles, jurídicas, obligaciones reguladoras o contractuales y cualquier otro requerimiento de seguridad.

El hecho de certificar un SGSI según la norma ISO/IEC 27001 puede aportar las siguientes ventajas a la organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza los procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayudan a supervisar continuamente el rendimiento y la mejora.

6.3 Auditoría Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos.

Los objetivos de la auditoría informática son (ver figura 6.12):

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.



Figura 6.12 Objetivos de la auditoría informática.

La auditoría informática sirve para manejar ciertas características en la empresa como:

- **Eficiencia:** se refiere a operar de modo que los recursos sean utilizados de forma adecuada, en otras palabras, es lograr las metas establecidas con la menor cantidad de recursos.
- **Eficacia:** es hacer lo necesario para alcanzar o lograr los objetivos propuestos. No se trata del proceso para obtener los resultados esperados sino del cumplimiento de las metas establecidas.
- **Rentabilidad:** es la capacidad que tiene algo, ya sea un producto, empresa o persona para generar suficiente utilidad o beneficio, es decir, un negocio es rentable cuando genera más ingresos que egresos.
- **Seguridad:** se trata del conjunto de protecciones a un bien determinado con el fin de preservar la confidencialidad, disponibilidad e integridad de los bienes de la empresa u organización.

Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoría informática. En general se siguen los siguientes pasos para llevar a cabo una auditoría:

1. **Planeación.** Ésta consiste en la elaboración de los programas de trabajo que se llevarán a cabo durante la revisión a la entidad auditada.
2. **Trabajos preliminares.** Consisten básicamente, de una serie de entrevistas con el cliente, las cuales tienen como objetivo dejar en claro las características básicas del trabajo que se va a realizar, qué es lo que quiere el cliente y que hará, en términos generales, el auditor.
3. **Diagnóstico administrativo.** El diagnóstico administrativo tiene por objetivo, proporcionar una panorámica de cómo la empresa percibe y practica la administración.
4. **Investigación previa.** Aquí se dará a conocer la empresa y de ser posible se validará la problemática que fue expuesta por el cliente. Después de esta fase se estará en posibilidades de hacer una mejor estimación del tiempo y de los honorarios, si es que no se pudo hacer en la primera fase.

5. **Elaboración del programa de la AI.** Todo buen administrador debe planear sus actividades y el auditor no debe ser la excepción, el programa señala las actividades que han de realizarse, fechas de inicio y término, así como los tiempos.
6. **Obtención de la Información.** En esta fase se obtendrá toda la información pertinente sobre el caso estudiado, pudiendo recurrir a herramientas como: entrevistas, encuestas, observación, etcétera, dependiendo del tipo de información que se requiera.
7. **Análisis, clasificación y evaluación de la información.** Se llevará a cabo de la siguiente forma:
 - El análisis y clasificación de la información podrá realizarse por métodos estadísticos
 - Evaluación: es aquí en donde se pone a prueba el talento del auditor, para entender e interpretar la información y continuar con el siguiente paso.
8. **Informe, elaboración y presentación del informe final.** Deberá contener los siguientes aspectos:
 - En él se informará de manera clara y concisa, sobre los resultados de la AI. No debe olvidarse que a los ojos del cliente él paga por recibir un informe, y en él debe encontrar valiosas recomendaciones que habrán de mejorar su administración., el informe aunque es escrito, debe presentarse apoyado en una exposición verbal.
 - Implementación y seguimiento: Algunos autores consideran esta fase como opcional, que no corresponde al auditor realizarla, sino a la empresa, se considera que el auditor debe participar, para que se interpreten correctamente sus recomendaciones y no haya lugar a desvíos en las mismas.

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.

6.4 Plan de contingencias informático

Un plan de contingencias de seguridad informática contiene los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema y por lo general, contar con reemplazos de dichos sistemas.

Las causas pueden ser variadas y pasan por un problema informático, una falla en la correcta circulación de la información o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones.

El hecho de preparar un plan de contingencia no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas con anterioridad y que pueden provocar importantes pérdidas, no sólo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

A medida que las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de ésta, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. En caso de un desastre, la interrupción prolongada de los servicios de computación puede llevar a pérdidas financieras significativas, sobre todo si está implicada la responsabilidad de la gerencia de informática. Lo más grave es que se puede perder la credibilidad del público o de los clientes y, como consecuencia, la empresa puede terminar en un fracaso total.

Diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables, sobre todo si se está partiendo de cero. Una solución comprende las siguientes actividades:

1. Debe ser diseñada y elaborada de acuerdo con las necesidades de la empresa.
2. Puede requerir la construcción o adaptación de un sitio para los equipos computacionales.
3. Requerirá del desarrollo y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes. Se hará participar a personal de

muchos departamentos diferentes, el cual debe trabajar en conjunto cuando se desarrolle e implemente la solución.

4. Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres cubiertos. .

Como con cualquier proyecto de diseño, un método estructurado ayuda a asegurar que se toman en cuenta todos estos factores y que se les trata adecuadamente.

A continuación se muestran las principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres.

1. Identificación de riesgos.
2. Evaluación de riesgos.
3. Asignación de prioridades a las aplicaciones.
4. Establecimiento de los requerimientos de recuperación.
5. Elaboración de la documentación.
6. Verificación e implementación del plan.
7. Distribución y mantenimiento del plan. (Ver figura 6.13)



Figura 6.13 Actividades principales de un plan de contingencia.

Un plan de contingencias se encuentra constituido por dos tipos de procedimientos:

- a) **Preventivos:** se llevan a cabo de manera periódica y se realiza para evitar posibles vulnerabilidades no detectadas al principio del proyecto o para evitar ataques futuros.

Se relaciona con actividades simples como actualizar antivirus, limpieza física del equipo, etcétera.

- b) **Correctivos:** se llevan a cabo después de un ataque para cerrar las puertas por donde éste se realizó o también se puede realizar la corrección una vez que se han detectado fallas en la seguridad del sistema o de la organización.

Otra clasificación de plan de contingencias se lista a continuación:

- a) **Planificados:** se sabe con antelación lo que debe hacerse, de modo que cuando la situación ocurre se dispone de personal, manuales y recursos para corregirla.
- b) **No planificados:** el correctivo de emergencia deberá actuar lo más rápidamente posible con el objetivo de evitar costos y daños mayores.

En un plan contra desastre que permite la continuación o el reinicio de las operaciones si presentan algún problema, se observan las siguientes ventajas:

- Reduce al mínimo los daños que cualquier eventualidad pueda producir.
- Permite alcanzar una normalización de las actividades normales de la organización en un menor tiempo.
- Implica menores pérdidas tanto económicas, materiales, personales así como de imagen para la empresa.
- Estimula la creación de una cultura de seguridad informática, así como fomentar la ética entre el personal de la empresa.

Asimismo contar con un plan de contingencia presenta la siguiente desventaja para una empresa u organización:

- Implica la inversión de tiempo y dinero ya que es necesario definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese y de los activos que se quieren proteger. Por lo que será necesario asignar recursos para realizar dichas actividades.



DESARROLLO

CAPÍTULO 7

Sitio web educativo



“La página WEB es el soporte interactivo ideal para ofrecer un servicio, facilitar información, hacer negocio, etcétera. De un modo más completo y directo que cualquier otro”.

Vinton Cerf
(1934) Padre de Internet. (Fundador de Internet Society).

7.1 Conceptos básicos de web

a) WWW (World Wide Web – Red de Cobertura Mundial)

La World Wide Web es la red mundial formada por todas las páginas web. Se trata de un medio de comunicación de texto, gráficos y otros objetos multimedia a través de Internet. A continuación se muestra la historia de la www⁴⁸:

- 1945: Vannevar Bush describió un dispositivo personal, llamado *memex*, el cual permitiría a cada individuo almacenar su información en microfilmes, consultarlos rápidamente y crear vínculos entre unos documentos y otros.
- 1960: Douglas Engelbart propuso un entorno de trabajo por computadora, con un sistema para almacenar publicaciones con catálogos para facilitar la búsqueda y el acceso a los documentos referenciados.
- 1989: Tim Berners-Lee, informático del CERN (The European Organization for Nuclear Research - Organización Europea de Investigación Nuclear) inventa la World Wide Web. Se trataba de un sistema de hipertexto para compartir información basado en Internet, concebido originalmente para servir como herramienta de comunicación entre los científicos del CERN.
- 1990: Nace el primer proveedor comercial de acceso a Internet a través de discado, denominado “The World”.
- 1990: A finales de este año el primer buscador web ya tenía forma. También surgió la Web 1.0.
- 1991: Marc Andreessen, estudiante de la Universidad de Illinois, desarrolla MOSAIC, el primer browser.
- 1992: Se realizan las primeras transmisiones de voz y vídeo sobre Internet.
- 1993: A principios de este año ya había alrededor de cincuenta servidores. Asimismo en Febrero de este mismo año se lanzó la primera versión alfa del navegador Mosaic for X, desarrollado por la NCSA (National Center for Supercomputing Applications - Centro Nacional de Aplicaciones de Supercomputación).

⁴⁸ Ford. M., Lew. K., Spanier. S. y Stevenson. T. (1998). La world wide web. *Tecnologías de interconectividad de redes*, (p. 681-692) México: Prentice Hall.

- 1993: Para el mes de abril el tráfico de la www era el 0.1% del total de Internet, por lo que, el CERN declara la www como tecnología de acceso gratuito.
- 1993: El mes de septiembre de este año se marca como el comienzo del crecimiento explosivo de la web. El tráfico alcanzaba el 1% de todo el tráfico de Internet y había más de 500 servidores.
- 1994: Se creó el World Wide Web Consortium (W3C) organismo formado por empresas y universidades de todo el mundo, con el objetivo de trabajar en beneficio de la estandarización de sistemas aplicados a la web.
- 1997: Para este año los servidores ya eran más de 650000.
- 2003: La web ya es vista como algo cotidiano para la gran parte de los más de 600 millones de usuarios de Internet.
- 2006: El buscador Google anuncia que hace su búsqueda rastreando exactamente 8620000000 páginas web.
- 2011: Las redes sociales adquieren gran popularidad en Internet, de las más sobresalientes se tienen Facebook con 600 millones de usuarios repartidos por el todo el mundo y Twitter con 190 millones.

b) *Página web*

Una página Web es un documento o información adaptada para la World Wide Web y accesible mediante un navegador de Internet. Su principal característica son los enlaces a otras páginas. Puede ser escrita en el lenguaje HTML y estar integrada por texto, imágenes, videos, animaciones y sonidos. Para que cada página sea ubicada en el servidor, cuenta con una dirección única llamada URL (Uniform Resource Locator – Localizador Uniforme de Recursos). Una URL está formada como se muestra a continuación (Figura 7.1):

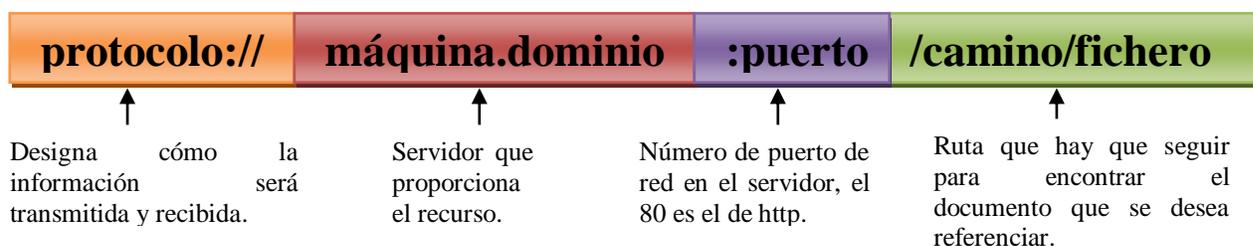


Figura 7.1 Estructura general de una dirección URL.

Por ejemplo, en la dirección <http://www.dgoserver.unam.mx/portaldgose/bolsa-trabajo/htmls/index.html> se tiene que:

- **http://** es la abreviatura de HyperText Transfer Protocol (Protocolo de transferencia de Hipertexto) indica el servicio utilizado para transmitir los datos.
- **www:** se trata de una página electrónica.
- **dgoserver.unam:** indica el nombre del servidor dentro de la organización.
- **.mx:** se refiere al nombre de dominio.
- **/portaldgose/bolsa-trabajo/htmls/index.html:** trayectoria por la que hay que ir para llegar a la carpeta donde está almacenada la información. En este ejemplo la página está en una carpeta llamada portaldgose que a su vez se encuentra en bolsa de trabajo y está en htmls, y el archivo que contiene la página se llama index.html

Características de las páginas web:

Las páginas web deben ser almacenadas en servidores web situados en cualquier parte del mundo. Estos servidores pueden restringir las páginas a una red privada, por ejemplo, una intranet, o pueden publicar las páginas en la www.

Al introducir en un explorador web la URL o bien al darle click a un enlace, se envía una petición al servidor que aloja dicha página para que posteriormente éste envíe la página web al equipo de cómputo y el explorador web utilizado se encargue de visualizarla en pantalla. A continuación se listan las principales formas para navegar en la red con páginas web:

- Hacer click en un hiperenlace de texto.
- Hacer click en un hiperenlace de un gráfico o imagen, por ejemplo, un botón o un dibujo.
- Escribir la URL de la página web en el cuadro de direcciones del explorador web.

c) Sitio web

Se trata del conjunto de una o más páginas web dedicadas a algún tema particular. Tienen una página de inicio que presenta todo el contenido del sitio, a partir de esta página de inicio se puede recorrer la información existente en el sitio.

El número de páginas que puede contener cada sitio varía de acuerdo con el tipo de empresa y del material que se quiera presentar en la red.

7.2 Desarrollo del sitio web

7.2.1 Requerimientos

El sistema recopilará información de alumnos y profesores sólo de la materia administración de redes y se contará con una base de datos para almacenar la información necesaria.

En principio, los alumnos deberán ingresar a la página para registrarse y poder acceder, en el tiempo estimado y permitido a la realización de cada examen; así también, se contará con un módulo de administración que permitirá registrar y hacer modificaciones a la información, ya sea de alumnos o profesores. El responsable de ingresar la información de los profesores la realizará el administrador del sistema.

Los resúmenes por capítulo, estarán disponibles en todo momento para el libre acceso de alumnos y profesores, así como para cualquiera que ingrese a la página. No así los exámenes, el tratamiento de éstos se explica posteriormente.

El sistema estará integrado por 4 módulos principales, que después se convertirán en las interfaces del sistema. A continuación se especifican las funciones que se podrán llevar a cabo en cada uno de ellos, así como sus particularidades:

1. Módulo de inicio de sesión

Este módulo consiste en un solo formulario, con dos campos, en el que se introducirá el id del usuario (éste depende del tipo de usuario) y la contraseña correctos. Pudiendo iniciar sesión ya sea alumnos, profesores y administrador de manera concurrente.

2. Módulo de registro

Este módulo se encontrará en la página principal, será indispensable que los alumnos realicen su registro antes de la realización del primer examen y que el administrador realice el registro de grupos y profesores. Ya que con este registro se les permitirá ingresar a la información correspondiente y sucesiva.

Para el registro de alumnos se solicitará la siguiente información:

1. Nombre
2. Apellido paterno
3. Apellido materno
4. Número Cuenta
5. Número Grupo
6. Usuario (el alumno deberá sugerir un identificador y el sistema lo validará).
7. Contraseña

Para el registro de los profesores se solicitará la siguiente información:

1. Nombre
2. Apellido paterno
3. Apellido materno
4. Registro Federal de Causantes (RFC)
5. Usuario (deberá sugerir un identificador y el sistema lo validará)
6. Contraseña

Una vez realizado el registro, el único que podrá editar la información será el administrador del sistema, por lo cual si se llegara a cometer un error se deberá consultar a dicho administrador.

3. Módulo alumnos

Para ingresar a este módulo será necesario que se haya hecho el registro con anterioridad, y sólo se podrá acceder a él cuando el administrador del sistema habilite el acceso (en el apartado del módulo del administrador se especifica el modo en que se habilitará).

El alumno sólo podrá tener acceso al sistema cuando el administrador haya habilitado el inicio de sesión. Inmediatamente después de iniciar sesión se le presentarán las instrucciones comunes a todos los exámenes, y la opción de comenzar a contestar el examen, a través de un botón de comienzo.

El orden de las preguntas de los exámenes será generado aleatoriamente, disminuyendo así, la posibilidad de copiar entre los alumnos.

El tiempo de duración del examen estará controlado, iniciando el conteo desde que el alumno dé clic en el botón comenzar examen.

El tiempo transcurrido será indicado en la pantalla.

Si el tiempo asignado para realizar el examen no se ha agotado, al finalizar el examen el alumno deberá dar clic en el botón finalizar examen y la calificación será correspondiente a la suma de los puntos que se hayan obtenido de las respuestas correctas entre el número total de preguntas; si el tiempo se agota y el alumno no concluye sus respuestas, la calificación será correspondiente al promedio que haya obtenido de las preguntas que contestó satisfactoriamente. En ambos casos, al finalizar el examen se presentará una pantalla donde se indique la calificación obtenida y una gráfica que muestre los subtemas evaluados.

4. Módulo profesores

Para ingresar a este módulo será necesario que se haya hecho el registro con anterioridad y el acceso estará disponible en cualquier momento.

Después de iniciada la sesión el profesor podrá acceder a la información de sus grupos. Sólo la podrá ver, no modificar. Podrá ver información detallada de cada examen realizado por sus alumnos, las respuestas correctas, etcétera. De los alumnos podrá visualizar la calificación de cada examen realizado de manera individual.

5. Módulo Administrador

Este módulo contará con un único superusuario que tendrá permisos para modificar, actualizar e insertar información a todas las tablas de la base de datos del sistema.

Para que el superusuario inicie sesión basta con que introduzca el id de superusuario y contraseña correctos y el sistema detectará que se trata del administrador, éste no necesita registrarse.

Este superusuario se encargará de habilitar la disponibilidad de acceso al sistema a los alumnos cuando sea la fecha estimada de la realización de cada parcial. Será un examen por tema; en la tesis se presentan 6 temas, por lo tanto serán 6 exámenes.

Sólo se podrá habilitar un número de examen a la vez.

Es importante recalcar la diferencia entre el tiempo de sesión del alumno, y el tiempo en que el examen estará disponible, por ejemplo, el examen estará disponible para la realización en el rango de tiempo que se indique por cada profesor, sin embargo, el tiempo que el alumno tendrá para contestarlo será de 30 min. Una vez iniciado el

examen, el tiempo empezará a transcurrir hasta agotarse, una vez agotado la sesión se deshabilitará y sólo podrán verse los resultados. Sin embargo, el examen seguirá habilitado para que pueda ser contestado por otros alumnos que no hayan iniciado sesión, el examen estará disponible hasta que se agote el tiempo de disponibilidad indicado por el administrador.

7.2.2 Especificaciones

Software:

- Apache Web Server Versión 2.2.4
- PHP Script Language Versión 5.2.3
- MySQL Database Versión 5.0.45
- phpMyAdmin Database Manager Versión 2.10.2

Usuarios:

Alumno:

- Contar con conocimientos básicos en computación.
- Computadora con acceso a internet.
- Para una correcta visualización se recomienda usar el navegador Mozilla Firefox (cualquier versión).
- Permitir ventanas emergentes.
- Previo registro al sistema.
- Usuario y Contraseña para acceso al sistema.

Profesor:

- Contar con conocimientos básicos en computación.
- Computadora con acceso a internet.
- Para una correcta visualización se recomienda usar el navegador Mozilla Firefox (cualquier versión).
- Permitir ventanas emergentes.
- Usuario y Contraseña para acceso al sistema.

Administrador:

- Computadora con acceso a internet.
- Usuario y Contraseña con privilegios de super-usuario.
- Contar con conocimientos básicos de BD.

Previa capacitación de administración del sistema. (Anexo manual de usuario).

7.2.3 Diseño

a) Casos de uso

Anteriormente, en la definición de requerimientos, se presentaron a los actores que interactuarán con el sistema y se observó que son tres, a continuación describiremos la función de cada uno de ellos.

Alumno: Cualquier alumno de la facultad de Ingeniería que se encuentre inscrito a algún grupo de Administración de Redes.

Profesor: Cualquier profesor que tenga a su cargo grupos de Administración de Redes. Para usar el sistema debe mantener comunicación con el administrador del sistema ya que éste efectuará su registro en el sistema.

Administrador: Este actor no puede ser cualquier persona, debe tener conocimiento sobre el manejo del sistema, y contar con conocimientos básicos de BD. Su función es la de mantener las condiciones idóneas para el buen funcionamiento del sistema. Se le otorgará privilegios de super-usuario (usuario root).

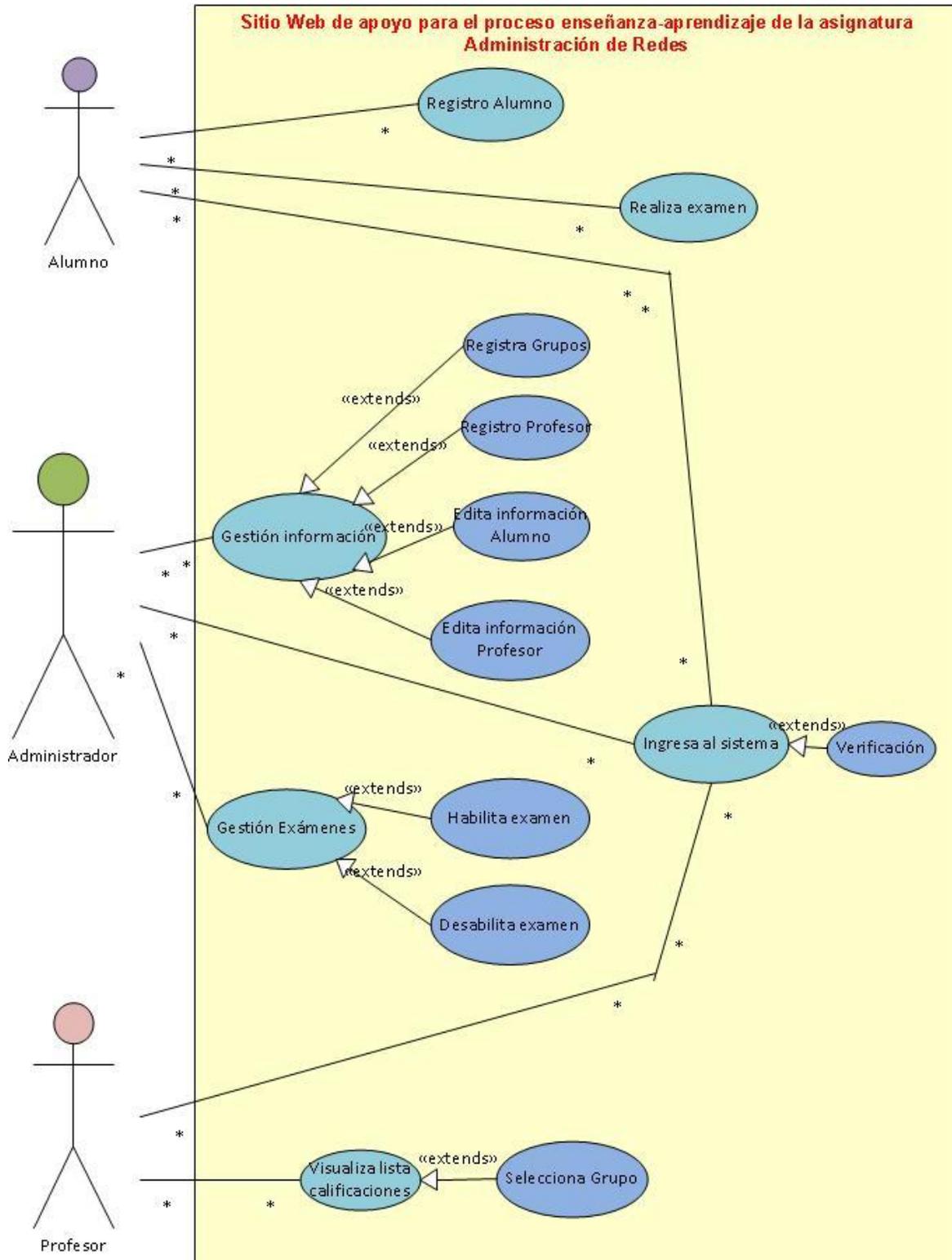


Figura7.2 Diagrama de casos de uso del sitio web de apoyo para el proceso enseñanza-aprendizaje de la asignatura *Administración de Redes*.

Otra parte importante del sistema son los casos de uso y en la figura 7.2, se puede observar que tenemos casos de uso, los cuales son los siguientes:

Registro Alumno: este caso de uso es especial para el alumno, ya que antes de ingresar al sistema para realizar algún examen debe realizar su previo registro; el alumno tendrá libertad para proponer su usuario y contraseña. (Ver tabla 7.1)

Tabla 7.1 Descripción caso de uso registros alumno.

Caso de uso: registro alumno	
Actor: alumno	
Curso normal	Alternativas
1) El alumno entra a URL del sistema.	
2) El sistema despliega opciones de registro alumno, inicio sesión.	
3) El alumno elige opción de registro alumno	
4) El sistema pide datos registro alumno: nombres, apellido paterno, apellido materno, número de cuenta, número de grupo, correo, usuario y contraseña.	
5) El alumno ingresa datos solicitados.	
6) El sistema verifica que los datos sean correctos.	7.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 3)
8) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Gestión de la información: se encarga de la administración de los grupos, alumnos, profesores, exámenes registrados en el sistema; aquí se pueden hacer altas y modificaciones, este caso de uso es propio del administrador (Ver tablas 7.2, 7.3, 7.4, 7.5 y 7.6).

Tabla 7.2: Descripción Caso de uso Alta grupo

Caso de uso: alta grupo	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se loggea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).

3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige opción de alta grupo	
5) El sistema pide datos alta grupo: número de grupo, profesor, hora de inicio y fin.	
6) El administrador ingresa datos solicitados.	
7) El sistema verifica que los datos sean correctos.	7.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 3)
8) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Tabla 7.3 Descripción caso de uso alta profesor.

Caso de uso: alta profesor	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se logea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de logeo (paso 1).
3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige opción de alta profesor.	
5) El sistema pide datos alta grupo: nombres, apellido paterno, apellido materno, RFC, correo, usuario y contraseña.	
6) El administrador ingresa datos solicitados.	
7) El sistema verifica que los datos sean correctos.	7.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 5)
8) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Tabla 7.4 Descripción caso de uso edita grupo.

Caso de uso: edita grupo	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se loggea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).
3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige opción de edita grupo.	
5) El sistema pide selección de número de grupo	
6) El administrador elige grupo	
7) El sistema muestra datos editables de grupo: profesos asignado, hora. de inicio y fin	
8) El administrador edita datos	
9) El sistema verifica que los datos editados sean correctos.	8.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 5)
10) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Tabla 7.5 Descripción caso de uso edita profesor.

Caso de uso: edita profesor	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se loggea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).
3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige opción de edita profesor.	

5) El sistema pide selección de profesor.	
6) El administrador elige profesor	
7) El sistema muestra datos editables de profesor: nombres, apellido paterno, apellido materno, RFC, correo, usuario y contraseña.	
8) El administrador edita datos	
9) El sistema verifica que los datos editados sean correctos.	9.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 7)
10) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Tabla 7.6 Descripción caso de uso edita alumno.

Caso de uso: edita alumno	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se logea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).
3) El sistema despliega opciones alta grupo, Alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige opción de edita alumno.	
5) El sistema pide selección de alumno.	
6) El administrador elige alumno	
7) El sistema muestra datos editables de alumno: nombres, apellido paterno, apellido materno, número de cuenta, número de grupo, correo, usuario y contraseña.	
8) El administrador edita datos	
9) El sistema verifica que los datos editados sean correctos.	9.1) Si los datos son incorrectos, el sistema lanza mensaje de error en pantalla y regresa al paso 7)
10) El sistema lanza mensaje de registro exitoso en pantalla. Regresa al paso 3)	

Gestión de exámenes: se encarga de habilitar y deshabilitar los exámenes que estarán disponibles para su realización, este caso de uso es propio del administrador, sin embargo estará sujeto previo acuerdo con los profesores.

Tabla 7.7 Descripción caso de uso habilita examen.

Caso de uso: habilita examen	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se logea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de logeo (paso 1).
3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige exámenes.	
5) El sistema muestra lista de exámenes.	
6) El administrador selecciona grupo habilitar.	
7) El sistema habilita examen.	

Tabla 7.8 Descripción caso de uso deshabilita examen.

Caso de uso: deshabilita examen	
Actor: administrador	
Curso normal	Alternativas
1) El administrador se logea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de logeo (paso 1).
3) El sistema despliega opciones alta grupo, alta profesor, edita grupo, edita profesor, edita alumno, exámenes.	
4) El administrador elige exámenes.	
5) El sistema muestra lista de exámenes.	
6) El administrador selecciona grupo deshabilitar.	
7) El sistema deshabilita examen.	

Ingresar al sistema: este caso de uso es general para los tres actores principales: alumno, profesor y administrador. Tienen que tener previo registro para ingresar al sistema.

Verificación: este caso de uso es obligatorio para los tres actores, se deberá ejecutar cada vez que ingresen al sistema.

Realiza examen: este caso de uso es propio del alumno, se debe seleccionar las respuestas de 15 preguntas aleatorias. (Ver tabla 7.9)

Tabla 7.9 Descripción caso de uso realiza examen.

Caso de uso: realiza examen	
Actor: alumno	
Curso normal	Alternativas
1) El alumno se loggea.	
2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).
3) El sistema despliega opciones realiza examen	
4) El alumno elige realizar examen.	
5) El sistema despliega preguntas examen habilitado.	
5) El sistema inicia conteo tiempo	
6) El alumno selecciona una respuesta por pregunta.	6.1) Si el contador de tiempo llega a 30 min. el sistema muestra calificación, y regresa a paso 1)
7) El alumno selecciona enviar	
8) El sistema califica y registra calificación en BD	
9) El sistema regresa a inicio.	

Visualiza lista de calificaciones: este caso es propio del profesor, y se encarga de desplegar una lista de calificaciones a partir de la previa selección de grupo. (Ver tabla 7.10)

Tabla 7.10 Descripción caso de uso visualiza lista calificaciones.

Caso de uso: visualiza lista calificaciones	
Actor: profesor	
Curso normal	Alternativas
1) El profesor se loggea.	

2) El sistema verifica que el usuario y contraseña sean correctos	2.1) Si no ingresa usuario y/o contraseña correcto el sistema lanza un mensaje de error y regresa a la ventana de loggeo (paso 1).
3) El sistema despliega lista de grupos	
4) El profesor elige grupo.	
5) El sistema despliega lista calificaciones	

b) Estructura del sitio web

La estructura de las páginas web es un aspecto de suma importancia que se debe tomar en cuenta al momento de su elaboración. Una buena estructura facilitará al usuario la navegación en las distintas páginas, manteniéndose así su atención para seguir conociendo más acerca de los temas expuestos. Si la estructura no es clara, es muy probable que el usuario abandone el sitio. Por ello es necesario organizar la información que se presentará.

Una vez realizado lo anterior, es necesario definir el tipo de estructura a utilizar, las cuales se describen a continuación:

- **Estructura de árbol o jerárquica:** a partir de una página de inicio (raíz) se pueden abrir otras secciones (ramas) que a su vez contienen otras páginas web (hojas). (Ver figura 7.3)

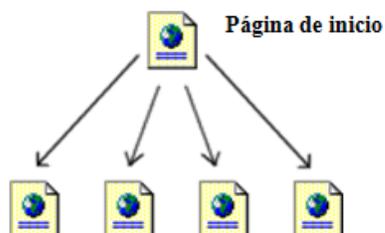


Figura 7.3 Estructura de árbol o jerárquica.

- **Estructura lineal:** contiene una página de inicio, y a partir de ésta se suceden las siguientes páginas una tras otra como si se tratara de un libro. (Ver figura 7.4)

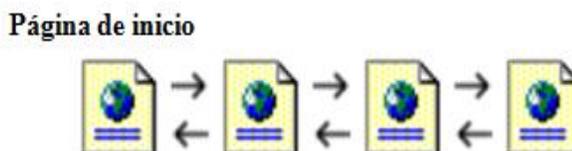


Figura 7.4 Estructura lineal.

- **Estructura en red:** las páginas que forman el sitio web se enlazan unas con otras según sus contenidos en una especie de red en la que no se aprecia ningún tipo de jerarquía. (Ver figura 7.5)

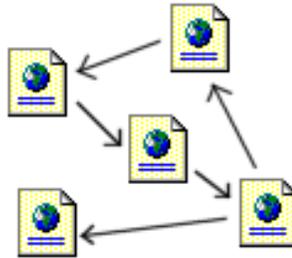


Figura 7.5 Estructura en red.

La estructura utilizada para el sitio en cuestión fue la de red. A continuación en la figura 7.6 se muestra un esquema global del contenido del sitio web.



Figura 7.6 Esquema global del sitio web.

El resultado final de la unión de páginas es el siguiente (ver figura 7.7):



Figura 7.7 Estructura en red del sitio web.

Para ilustrar la explicación anterior, se detalla en la figura 7.8 el mapa del sitio:

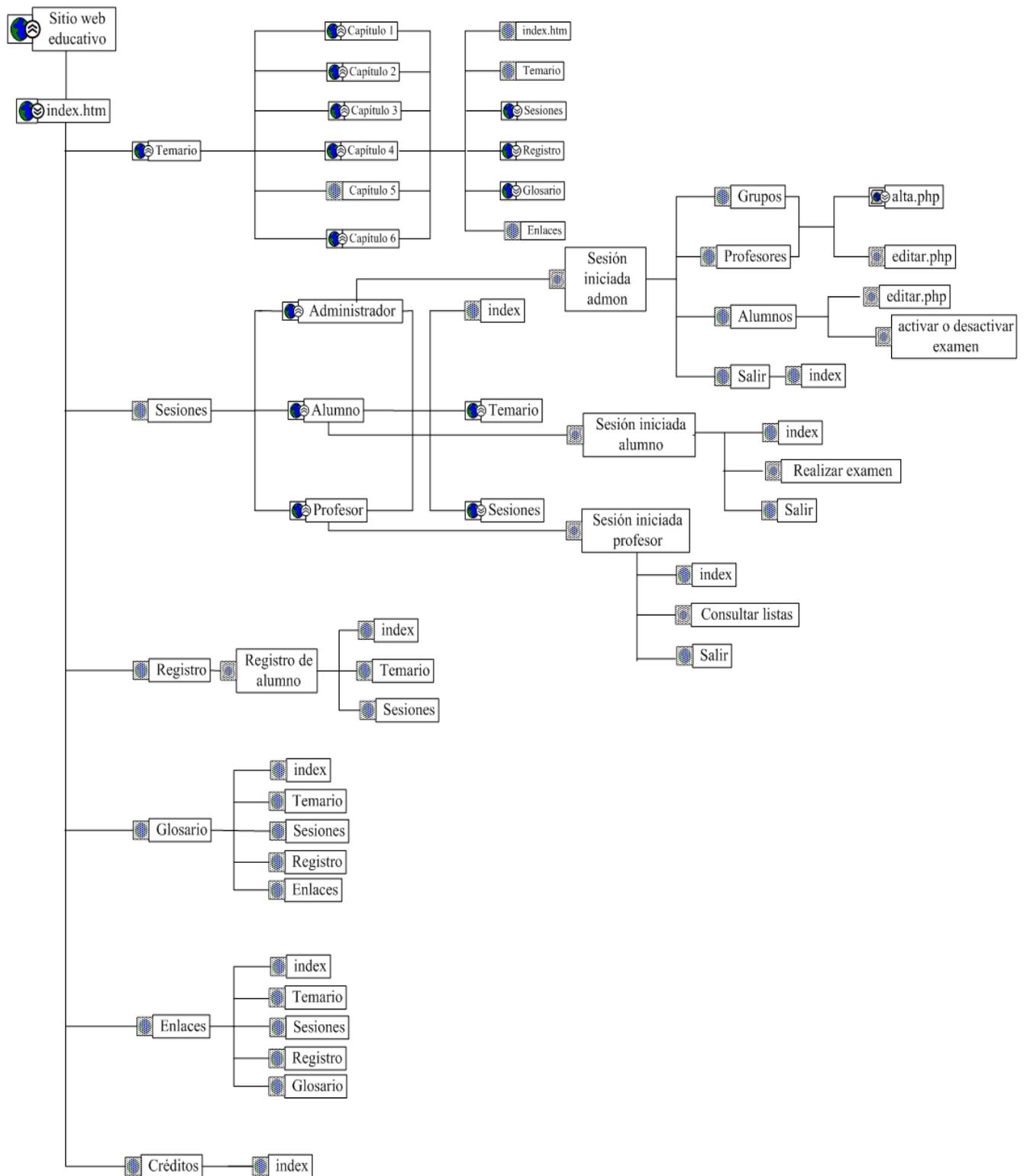


Figura 7.8 Estructura Sitio web

c) *Diseño web*

Para el proceso de diseño de páginas web se deben tomar en cuenta los siguientes aspectos principales:

- **Objetivos:** establecer para qué tipo de usuarios será el sitio web, asimismo, tener claro el mensaje que se desea transmitir.

En este caso, el sitio está dirigido principalmente a los alumnos y profesores de la facultad de Ingeniería, a los cuales se les pretende brindar una herramienta dinámica, eficiente, y eficaz como apoyo en su trayecto aprendizaje-enseñanza en materia de la administración de redes de datos.

- **Diseño visual:** es necesario distribuir el texto, los gráficos, y los vínculos a otros documentos. Es de suma importancia realizar un bosquejo, lo cual facilitará tener un orden claro sobre el diseño.

En particular se realizó un análisis y diversos bocetos que pretendían construir un performance que visualmente fuera amigable y atractivo para el usuario. Finalmente se eligió el boceto que más se ajusta a dichas características, de éste se habla a lo largo del presente capítulo.

- **Desarrollo:** una vez realizados los pasos anteriores es posible escribir cada página web que incluirá el sitio.

Lo más importante al momento del diseño es la comunicación, es por eso que un sitio web cuya información tenga una buena presentación, pero que su diseño no sea del todo agradable, hará que la navegación sea difícil para el usuario. De manera contraria, si el diseño es muy bueno, pero el contenido es inaccesible, los usuarios perderán el interés en el sitio web. Así, queda explícito que el buen diseño y funcionalidad de cualquier sitio web van de la mano. Por lo que se siguieron las siguientes recomendaciones:

- El tiempo de carga del sitio no debe ser excesivo para que el usuario no pierda el interés y salga del sitio web.
- Si existe un cambio entre la página principal y las secundarias del sitio web, debe persistir el mismo estilo en todo el sitio, para que el usuario se dé cuenta que aún se encuentra en él.
- El menú de navegación principal debe ser claro y visible en la página y cada link debe tener un título descriptivo.

Elección de colores

El filósofo Aristóteles fue el primero en afirmar que los colores se conforman con la mezcla de cuatro colores, denominados por él, como básicos, los cuales eran los de tierra, fuego, agua y cielo.

Siglos más tarde, Leonardo Da Vinci definió el color como algo propio de la materia, a su vez, definió la siguiente escala de colores: en primer lugar el blanco, como color principal, en seguida el amarillo para la tierra, verde para el agua, azul para el cielo, rojo para el fuego y negro para la oscuridad, observando que con la mezcla de estos colores obtenía todos los demás.

En 1665 Isaac Newton descubrió que la luz del sol al pasar a través de un prisma, se dividía en varios colores conformando un espectro (ver Figura 7.9). Por lo que estableció que la luz es color, principio que hoy en día sigue siendo aceptado.

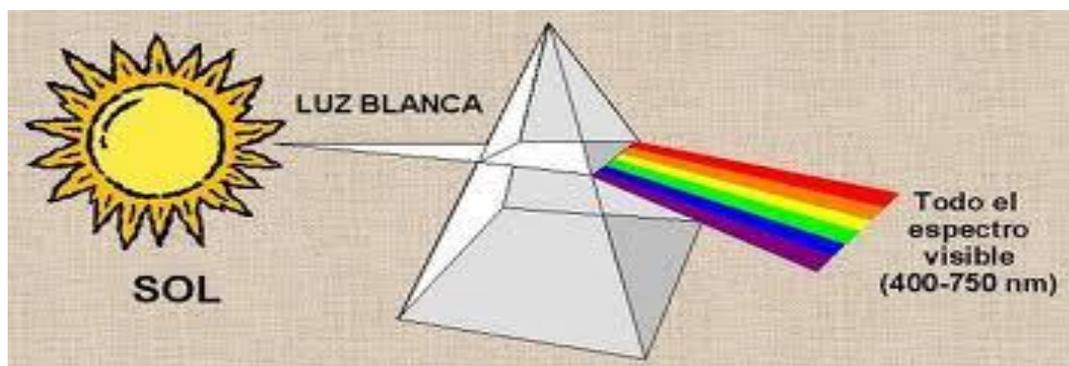


Figura 7.9 Prisma de colores.

Como se muestra en la figura 7.9, Newton logró la descomposición de la luz en siete colores del espectro, este fenómeno ocurre cuando la luz se refracta en el borde de un cristal.

Por otro lado, Johan Goethe estudió y probó las modificaciones físicas y psicológicas que el ser humano sufre ante la exposición a los diferentes colores.

Propiedades del color

El color presenta las siguientes propiedades: el tono, saturación y brillo (ver Figura 7.10).

- Tono (hue): es la cualidad por la cual se diferencia y se le asigna su nombre a determinado color.

- Saturación (saturation): es el atributo utilizado para describir cuan claro u oscuro parece un color y se determina por la cantidad de luz que contiene un color.
- Brillo (brightness): a través de este elemento se representa la viveza o palidez de un color. Dicho de otra forma es la cantidad de luz emitida por una fuente lumínica.



Figura 7.10 Propiedades del color.

Psicología del color

Con los colores se pueden tener diferentes respuestas emocionales en las personas tales como: la calma, plenitud, opresión, violencia, alegría, etcétera. La psicología de los colores fue ampliamente estudiada por el poeta y científico alemán Johann Wolfgang von Goethe, quien propuso que el color depende de la percepción, en la que se halla involucrado el cerebro y los mecanismos de la vista.

Cada color transmite diferentes emociones, a continuación se explica lo que cada uno transmite:

- Color blanco: es la suma de todos los colores y expresa paz, pureza e inocencia.
- Color gris: Es considerado el color de la neutralidad, ya que se encuentra entre la transición entre el blanco y el negro. Simboliza la indecisión y la ausencia de energía, expresa duda y melancolía.
- Color amarillo: es el más luminoso, cálido, ardiente y expansivo. Representa el color del sol, de la luz y del oro, y como tal es violento, intenso y agudo. Suelen interpretarse como animados, joviales, excitantes, afectivos e impulsivos.

- Color naranja: Posee fuerza activa, radiante y expansiva. Tiene un carácter acogedor, cálido, estimulante y una cualidad dinámica muy positiva y energética. Aumenta el optimismo, la seguridad, la confianza y el equilibrio.
- Color rojo: simboliza vitalidad, pasión, sangre, fuerza bruta y fuego, por otro lado expresa la sensualidad, la virilidad, la energía y en ocasiones resulta agresivo. El rojo estimula la adrenalina y la presión arterial. Además evoca la guerra y el mal.

Por ser el color más sobresaliente, habrá que controlar su extensión e intensidad, ya que por su potencia de excitación en grandes áreas cansa rápidamente.

- Color azul: provoca una sensación de placidez, expresa armonía, amistad, fidelidad y serenidad. Se encuentra asociado con el cielo, el mar y el aire. Se dice que es el color del infinito, de los sueños y de lo maravilloso.
- Color verde: se trata del color más tranquilo y sedante. Evoca la vegetación, el frescor y la naturaleza. Es el color de la calma y es considerado un color frío.
- Color violeta: es el color de la templanza, de la lucidez y de la reflexión. Es místico, melancólico y podría representar también la introversión.

Temperatura del color

La temperatura es un atributo que existe en los colores y está dividido en dos categorías (ver figura 7.11):

- Colores cálidos: van del rojo al amarillo y dan la sensación de actividad, alegría, dinamismo, confianza y amistad. Estos colores ardientes se proyectan hacia fuera y atraen la atención, son fuertes y agresivos. El poder de los colores ardientes afecta a la gente de muchas maneras, tales como el aumento de la presión sanguínea y la estimulación del sistema nervioso.
- Colores fríos: van del azul al verde e incluyen algunos tonos de violeta. Los colores fríos aminoran el metabolismo y aumentan la sensación de calma. Con estos colores se da un aspecto de seriedad y formalidad.

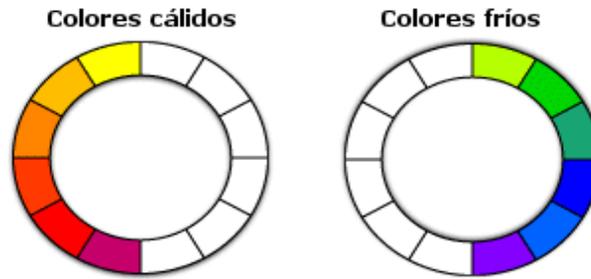


Figura 7.11 Temperatura del color.

Estudiar la teoría del color resulta de suma importancia ya que es una parte esencial para el diseño de un sitio web, esto es debido a todos los efectos que tienen los colores ante el ser humano. A continuación se listan algunos puntos por los cuales es importante conocer toda esta teoría de los colores para el buen diseño del sitio:

- Tiene un gran poder de atracción o rechazo dependiendo del uso que se le dé.
- Los colores también dan sensación de movimiento.
- Las emociones, sensaciones, y en definitiva todo lo que los colores pueden llegar a expresar y hacer sentir al espectador forma parte fundamental de la base de un buen diseño.
- El color, como elemento claramente evidenciado del diseño, puede ser la clave del éxito. Tanto si se piensa como si no, si se da cuenta o no de ello, se está cargando de significados cuando se elige un color.

Con base en lo anterior, se optó por elegir colores fríos en su mayoría, ya que cumplen con las características para establecer un entorno adecuado para el proceso de aprendizaje; y colores cálidos para captar la atención en ciertos puntos, como por ejemplo ligas y marcos.

Creación del fondo

Una vez elegidos los colores para el sitio web, se deben tomar en cuenta los tipos de formatos de imágenes aceptados en la web. Existe una amplia gama de formatos de imágenes, sin embargo los navegadores web comprenden sólo tres:

- **GIF (Graphics Interchange Format – Formato de Intercambio de Gráficos):** es ampliamente utilizado en la web, tanto para imágenes como para animaciones. Es un formato sin pérdida de calidad para imágenes con hasta 256 colores. Un punto a su favor es que posee transparencia.

- **JPEG (Joint Photographic Experts Group – Grupo de Expertos en Fotografía):** es el formato de imagen más utilizado para fotografías, imágenes de gran tamaño y variedad de colores en la web.
- **PNG (Portable Network Graphics – Gráficos de Red Portátiles):** es un formato de 48 bits de color y 16 bits para la escala de grises, motivo por el cual posee alta compresión sin pérdida de calidad. Al igual que GIF posee transparencia.

En la realización del fondo se utilizaron los colores azul y blanco, haciendo uso de un degradado.

Respecto a las imágenes se utilizó el formato JPEG, excepto para las que requerían transparencia para las cuales se utilizó el formato GIF.

Un grado es la transición entre dos colores, es decir, es la composición de dos o más tonalidades de color, de tal forma que siempre hay una transición gradual de una a otra tonalidad. Existen dos tipos de degradado, los cuales se describen a continuación:

- Degradado lineal: los colores se ordenan de izquierda a derecha, y recibe el nombre de degradado lineal ya que la transición de color se produce a lo largo de una línea.
- Degradado radial: los colores se organizan de adentro hacia afuera; es llamado radial porque la transición de color se produce a partir de un punto.

Se utilizó un degradado lineal únicamente en la parte del encabezado y los extremos de la página ya que el resto quedará de color blanco con el objetivo de que las imágenes y diagramas se puedan visualizar de manera correcta y cómoda para los usuarios. (Ver figura 7.12)



Figura 7.12 Degradado del sitio Web.

Una vez que se creó el fondo del sitio web, fue necesaria la realización de los siguientes componentes para tener el diseño completo del sitio:

Creación de menú

Para la elaboración del menú se optó por elegir un menú desplegable, de esta manera la navegación por el sitio se torna sencilla y amigable para el usuario (ver figura 7.13).



Figura 7.13 Menú desplegable para navegar por el sitio web.

Por otra parte, la sección de los resúmenes incluye un sub-menú por cada capítulo que se ubicó a un costado de la interfaz, esto para facilitarle al usuario la búsqueda de cada subtema (ver figura 7.14)

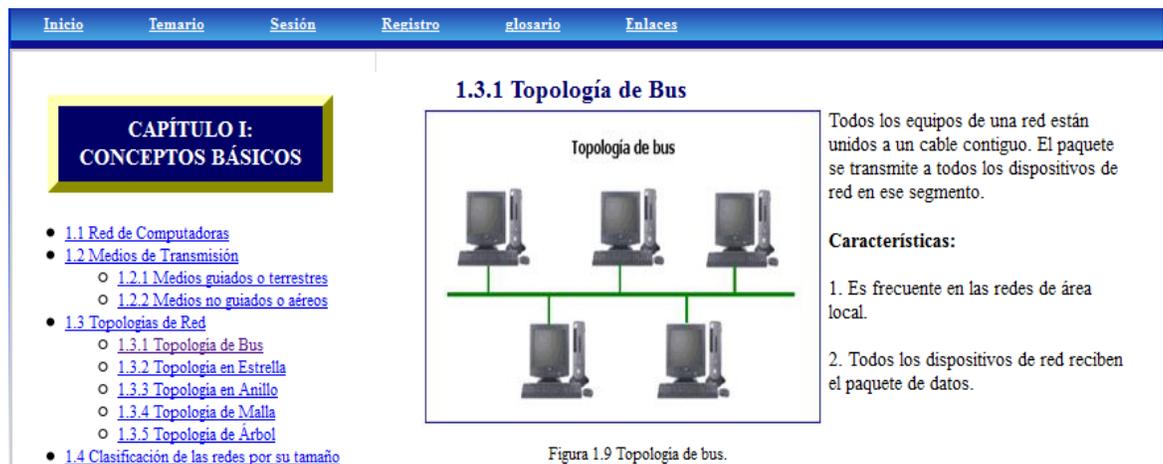


Figura 7.14 Menú del temario.

Creación de animaciones

Una animación es un proceso utilizado para dar la sensación de movimiento a imágenes que son utilizados para distintos fines, en este caso para hacer más atractivo el sitio web.

Pueden ser sencillas o complicadas agregando código action script o también pueden ser gifs animados.

Siendo los conceptos más utilizados para la creación de las animaciones los siguientes:

- Capas de máscara: se trata de un elemento que permite ocultar partes de una imagen, pero sin borrar esas partes, con lo que se pueden añadir varios efectos. Ejemplo de ello se muestra en la imagen 7.15:

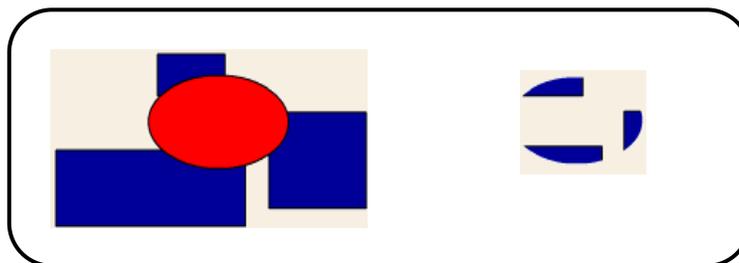


Figura 7.15 Animación con capas de máscara.

- Interpolación de movimiento: esta acción permite desplazar símbolos, grupos y bloques de texto. Es posible la interpolación de movimiento con las capas con guía de movimiento, con lo cual el objeto no sólo estará interpolado, sino que también va a seguir la forma de la línea. Ejemplo de una animación usando este concepto es la que se muestra en la figura 7.16:



Figura 7.16 Animación con interpolación de movimiento.

- Guías de movimiento: pueden formarse por otras formas que no sean líneas, dependiendo de la forma del trazado de la línea será el efecto que se esté tratando conseguir. Ejemplo de animación utilizando este concepto se muestra en la figura 7.17:

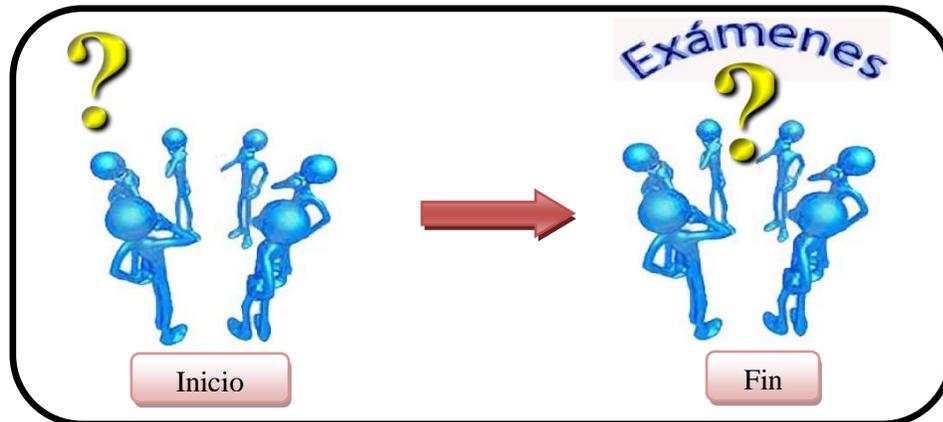


Figura 7.17 Animación con interpolación y guías de movimientos.

Elaboración del logo

Un logo es un elemento gráfico que identifica a una persona, empresa, institución o producto. Puede estar formado de letras, imágenes o ambas.

Para la elaboración del logo se tomó en cuenta que combinara con el fondo (ver figura 7.18):



Figura 7.18: Logo del sitio Web.

Lo que se pretende dar a entender con este logo es que en todo trabajo existe la intervención del humano, elemento que simboliza la mano, quien será el responsable de la administración de la red. El mundo hace referencia a que las redes de datos son globales cuya comunicación se establece a través de medios ya sean terrestres o aéreos, la diversidad de dichos elementos la representa el cable UTP. Las piezas de rompecabezas indican que para lograr una buena administración es necesario implementar varias piezas las cuales se complementan entre sí, donde cada una de éstas juega un papel fundamental para cumplir con los objetivos de la administración de las redes.

Software de apoyo y lenguajes de programación web

Para la elaboración del sitio web se utilizaron las siguientes herramientas de desarrollo y lenguajes de programación:

1. Adobe PhotoShop

PhotoShop es un programa que está destinado para la edición, retoque fotográfico y pintura. Debido a su capacidad de retoque y modificación de fotografías se ha convertido en el programa más famoso del mundo dentro de este ámbito. Sus principales características son las siguientes:

- Cuenta con una gran variedad de herramientas para la manipulación, tratamiento y retoque de imágenes.
- Posibilita la transformación de fotografías digitales, desde su optimización hasta la impresión y escaneado.

El formato propio de PhotoShop es .PSD, aunque también soporta otros formatos como: EPS, BMP, GIF, JPEG, PNG, entre otros.

Cabe mencionar que para el desarrollo del sitio web se utilizó la versión CS5 de PhotoShop, lanzada el 12 de abril de 2011 por Adobe Systems (ver figura 7.19)

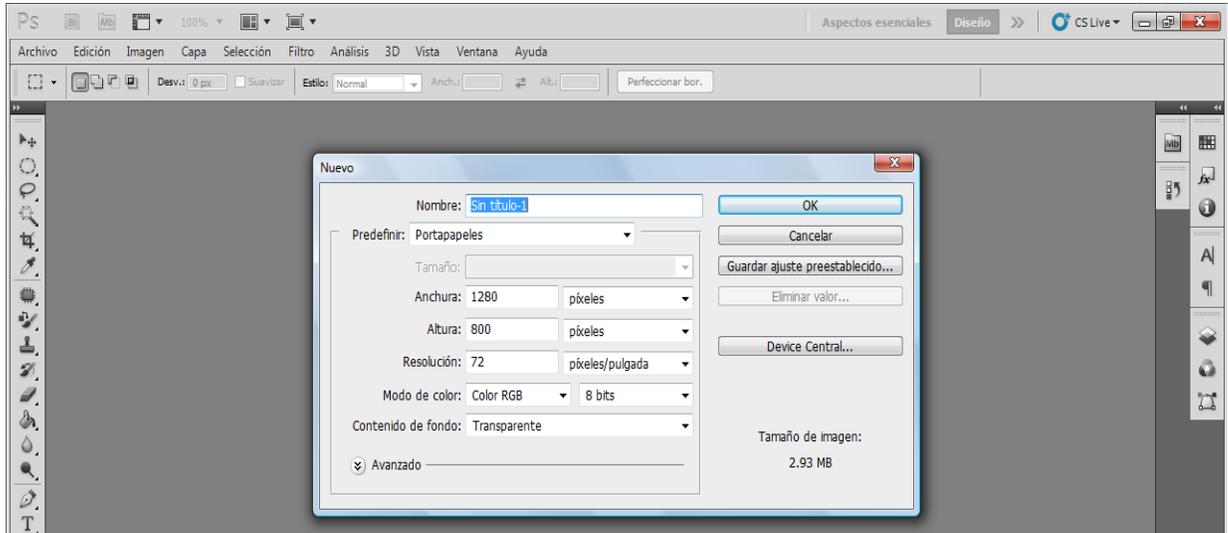


Figura 7.19 Interfaz de PhotoShop CS5.

En cuanto a las animaciones, se utilizó el programa Adobe Flash, del cual, se hablará a continuación.

2. *Adobe Flash*

En sus inicios era propiedad de una empresa llamada FutureWave Software y su nombre original era Future Splash Animator. Fue hasta diciembre de 1996 que Macromedia adquiere esta empresa y con ello este software que pasa a ser conocido como Flash 1.0. Y para el año 2005 Adobe compra Macromedia y junto con ella sus productos, entre ellos Flash, que pasa a llamarse Adobe Flash.

Adobe Flash es un programa de animación que permite dibujar en dos dimensiones y animar los dibujos incorporándoles sonido, video y la posibilidad de que el usuario interactúe con los contenidos. Permite al usuario importar sonidos en varios formatos como el MP3, así como la importación de gráficos con extensiones como PSD, JPEG, GIF, PNG, entre otras. A continuación se muestra el entorno de trabajo de Flash (ver figura 7. 20):

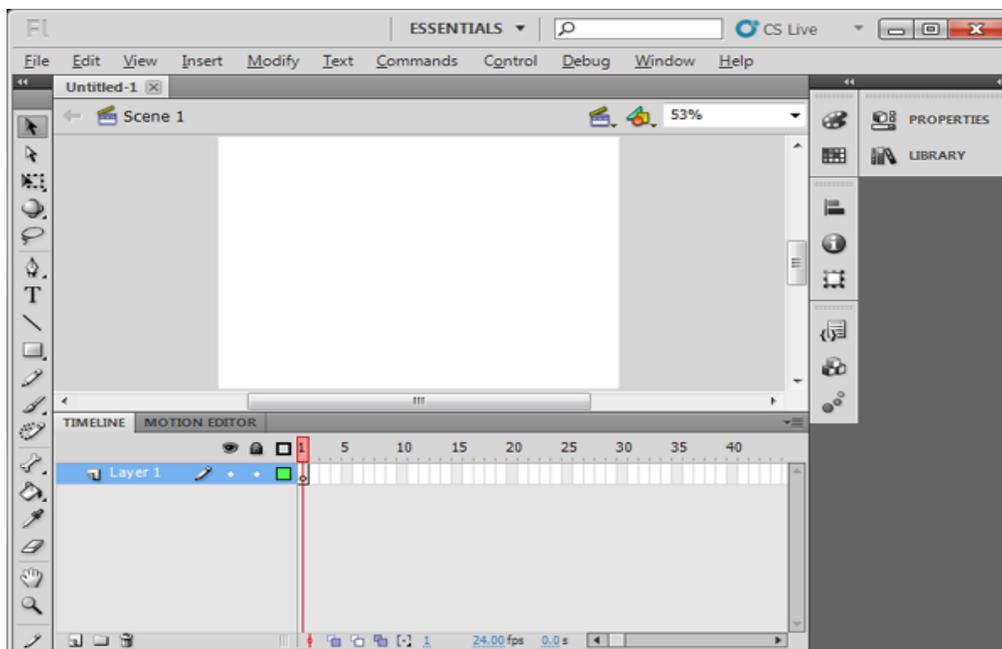


Figura 7.20 Entorno de trabajo de Flash CS5.

Flash utiliza dos tipos distintos de archivos uno para crear y otro para distribuir el contenido: el archivo de creación posee una extensión .fla y la extensión correspondiente al archivo de distribución de contenido se conoce como película flash y lleva la extensión .swf.

Algunas de las aplicaciones más comunes de Flash se listan a continuación:

- Animaciones: una animación es la composición de una o varias imágenes que presentan cambios, en un lapso determinado de tiempo.
- Presentaciones multimedia: se trata de aplicaciones con sonido y video, y pueden contener o no animaciones. También se pueden utilizar las presentaciones multimedia en la creación de CD multimedia.
- Sitios Web: Flash es usado para realizar sitios web enteros o bien parte de ellos. Los sitios desarrollados con Flash son visualmente muy atractivos.
- Juegos: a través del lenguaje de programación ActionScript, Flash proporciona una alternativa más sencilla para realizar juegos, esto siempre y cuando el usuario tenga conocimientos sobre el lenguaje de programación ActionScript.

3. HTML

Fue creado por el físico Tim Berners-Lee quien sentó las bases de la web tal y como se conoce hoy día. Lo que hace posible HTML es presentar información en Internet a través del explorador, es decir lo que se muestra en pantalla es la interpretación que hace el navegador del código HTML.

HTML es la abreviatura de HyperText Mark-up Language (Lenguaje de marcado hipertextual o de hipertexto). HTML no tiene ningún compilador, por lo tanto algún error de sintaxis que tenga éste no lo detectará y se visualizará en la forma como él lo entienda.

Para la creación de documentos en HTML son necesarias dos herramientas:

- Procesador de textos: es utilizado para escribir y editar el código HTML, pudiendo ser el bloc de notas. Aunque también existen programas de edición y creación de páginas web con los que se puede auxiliar, tales como: Microsoft Front Page o Dreamweaver. (Ver figura 7.21)



Figura 7.21 Programas para crear páginas web.

- Explorador web: se utiliza para navegar en la red y se encarga de interpretar el código HTML de la página web. Existen varios exploradores, sin embargo, los más populares son: Firefox Mozilla, Microsoft Internet Explorer, Google Chrome, Opera y Safari. (Ver figura 7.22)



Figura 7.22 Exploradores web.

Para poder crear las páginas web son utilizadas las etiquetas. En HTML una etiqueta representa líneas de código que le indican al navegador como interpretar un documento HTML (ver figura 7.23). Dentro de las reglas de formato de las etiquetas de HTML se tienen las siguientes:

- Las etiquetas pueden ser escritas con minúsculas o mayúsculas.
- El espacio en blanco es ignorado.
- Las etiquetas se abren y se cierran con paréntesis triangular (< >), las etiquetas de cierre son iguales a las de apertura, aunque también llevan una diagonal normal (/), como por ejemplo: letra en negrita
- El espacio en blanco se escribe con la siguiente instrucción:

Usando las distintas etiquetas que contiene la gamma de HTML se pueden realizar las siguientes acciones en un documento HTML:

- Definir la estructura del documento HTML.
- Editar y crear tablas.
- Insertar imágenes.
- Editar el texto del documento.



Figura 7.23 Representación de las etiquetas HTML.

Una página web como la que se observa en la figura 7.23 es una página muy básica, la cual se compone de las siguientes etiquetas, las cuales representan la estructura básica de una página web:

<HTML> Indica el inicio del documento

<HEAD> Indica el inicio de la cabecera <TITLE> Inicio del título del documento

</TITLE> Final del título del documento

</HEAD> Final de la cabecera

<BODY> Inicio del cuerpo del documento

Instrucciones HTML

</BODY> Final del cuerpo del documento

</HTML> Final del documento

4. PHP

Historia

Inició como una modificación a Perl creada por Rasmus Lerdorf a finales de 1994 conocida como Personal Home Pages – Herramientas Personales de Trabajo. Más tarde Rasmus tuvo la necesidad de crear páginas dinámicas que trabajasen con formularios por lo que creó una serie de etiquetas a las que denominó “Form Interpreters”, y lo publicó con el nombre de PHP/F1 en 1995.

Para el año 1997 Zeev Suraski y Andi Gutmans agregaron nuevas funcionalidades y el soporte a la gran mayoría de bases de datos comerciales, como MySQL y Oracle, así como un módulo para Apache. Así fue cómo surgió PHP3 siendo el sucesor de PHP/F1.

Como PHP3 carecía del uso de sesiones, algo muy común en las páginas web de cierta complejidad. Para el año 2000 se creó la versión PHP4.

La última versión es PHP5 que presenta mejoras significativas y un entorno de programación orientado a objetos mucho más completo.

Definición

PHP es el acrónimo de Hipertext Preprocessor. Es un lenguaje de programación que funciona del lado del servidor, es decir, se ejecuta en el servidor web justo antes de que se envíe la página a través de Internet al cliente. Las páginas que se ejecutan en el servidor pueden realizar accesos a bases de datos, conexiones en red y otras tareas para crear la página final que verá el cliente. Así el cliente solamente recibe una página con código HTML. (Ver figura 7.24)

Además con PHP se puede hacer lo siguiente:

- Procesar información de formularios.
- Generar páginas con contenidos dinámicos.
- Mandar y recibir cookies.

PHP se escribe dentro del código HTML y la forma de incluir código PHP a los documentos HTML es usando las etiquetas `<?php` o simplemente `<?`, cerrando la etiqueta así `>`

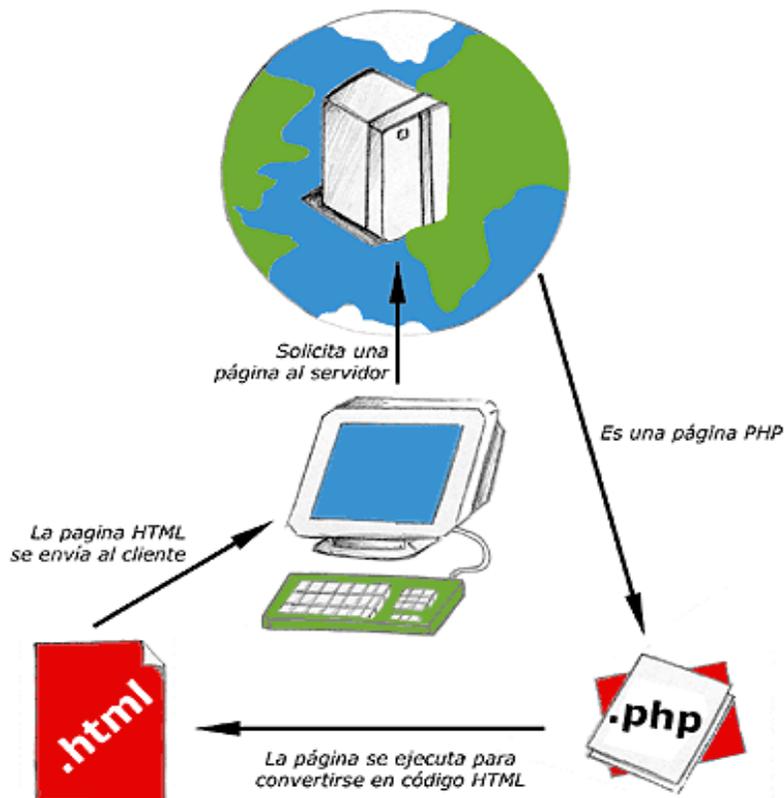


Figura 7.24 Funcionamiento de PHP.

PHP ha cobrado fuerte popularidad en cuanto al desarrollo de páginas dinámicas esto debido a las siguientes características:

- Es un software de libre distribución, es decir, no tiene costo alguno, y puede ser descargado de la página <http://www.php.net/downloads.php>.
- Es multiplataforma, esto es, existen versiones de PHP para Windows, Linux, Mac OS X, Unix, etcétera.
- Una de las características más importantes es su sencillez de uso comparado con otros lenguajes.
- Cuenta con un gran soporte para una gran cantidad de bases de datos.
- Permite la programación orientada a objetos.

5. Dreamweaver

Es un creador y editor de páginas web que sirve para diseño y programación web, básicamente para hacer o modificar páginas. Fue creado inicialmente por Macromedia y es actualmente producido por Adobe Systems. Es el programa más utilizado en el sector del diseño y la programación web debido a sus múltiples herramientas y utilidades.

Con Dreamweaver se pueden diseñar páginas con aspecto profesional, y soportan gran cantidad de tecnologías además de ser muy fáciles de usar, como: hojas de estilo y capas, JavaScript para crear efectos e interactividades, inserción de archivos multimedia, etcétera.

Las funciones de edición visual de Dreamweaver permiten agregar rápidamente diseño y funcionalidad a las páginas, sin la necesidad de programar manualmente el código HTML.

Dentro de otras funciones destacan: la conexión a un servidor FTP, a base de datos, así como el soporte para la programación de HTML, ASP, PHP, etcétera.

d) Diseño de Base de datos

Importancia de las bases de datos para las organizaciones

La función básica de una base de datos es permitir el almacenamiento y la recuperación de la información necesaria, para que las personas de las organizaciones puedan tomar decisiones. Es así que las Bases de Datos se tornan esenciales para la supervivencia de

cualquier organización; pues los datos estructurados constituyen un recurso básico para todas las organizaciones. (Figura 7.25)



Figura 7.25 Importancia de las BD para las organizaciones.

Las soluciones utilizadas por las empresas para almacenar los datos son diversas. Antes de la aparición de la informática se almacenaban en ficheros con cajones y carpetas y fichas. Tras la aparición de la informática estos datos se almacenan en archivos digitales dentro de las unidades de almacenamiento del ordenador.

Además las empresas requieren utilizar aplicaciones informáticas para realizar tareas propias de la empresa a fin de mecanizar a las mismas. Estas aplicaciones requieren manejar los datos de la empresa.

En los inicios de la era informática, cada programa almacenaba y utilizaba sus propios datos de forma un tanto caótica. La ventaja de este sistema, es que los procesos eran independientes por lo que la modificación de uno no afectaba al resto. Pero tiene grandes inconvenientes:

- Costo de almacenamiento elevado.
- Datos redundantes (se repiten continuamente).
- Probabilidad alta de inconsistencia en los datos.
- Difícil modificación en los datos y facilidad de problemas de inconsistencia al realizar esas modificaciones.

Lógicamente la solución a este problema es hacer que todas las aplicaciones utilicen los mismos datos. Esto provoca que los datos deban estar mucho más protegidos y controlados. Además los datos forman una estructura física y funcional que es lo que se conoce como base de datos.

Así, una base de datos (BD) es un conjunto de datos interrelacionados almacenados en conjunto, sin redundancias innecesarias, de forma independiente de los programas que acceden a ellos. (Ver figura 7.26)

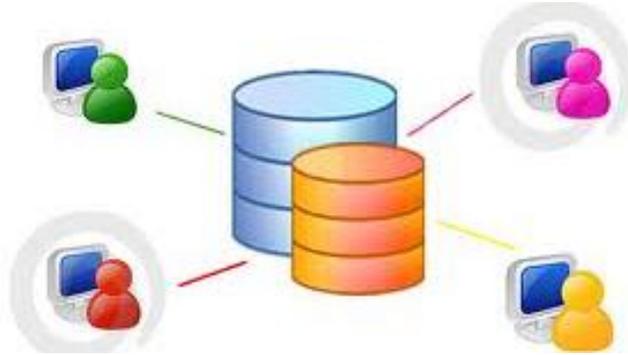


Figura 7.26 Base de datos.

Ventajas de las bases de datos

- Independencia de los datos y los programas y proceso. Esto permite modificar los datos sin modificar el código de las aplicaciones.
- Menor redundancia. No hace falta tanta repetición de datos. Aunque, sólo los buenos diseños de datos tienen poca redundancia.
- Integridad de los datos. Mayor dificultad de perder los datos o de realizar incoherencias con ellos.
- Mayor seguridad en los datos. Al limitar el acceso a ciertos usuarios.
- Datos más documentados. Gracias a los metadatos que permiten describir la información de las bases de datos.
- Acceso a los datos más eficiente. La organización de los datos produce un resultado más óptimo en rendimiento.
- Menor espacio de almacenamiento. Gracias a una mejor estructuración de los datos.

Desventajas de las bases de datos

- Instalación costosa. El control y administración de bases de datos requiere de un software y hardware poderoso.

- Requiere personal calificado. Debido a la dificultad de manejo de este tipo de sistemas.
- Implantación larga y difícil. Debido a los puntos anteriores. La adaptación del personal es mucho más complicada y lleva bastante tiempo.
- Ausencia de estándares reales. Lo cual significa una excesiva dependencia hacia los sistemas comerciales del mercado. Aunque hay una buena parte de esta tecnología aceptada como estándar de hecho.

Pasos para crear Bases de Datos

El primer paso para definir una base de datos es realizar un esquema conceptual, que representa la información independiente a la tecnología que se va a utilizar para gestionarla. El modelo conceptual es el más cercano al usuario, el lógico es el encargado de establecer el paso entre el modelo conceptual y el modelo físico del sistema.

En 1976 y 1977 dos artículos de Peter P. Chen⁴⁹ presentan un modelo para realizar esquemas que posean una visión unificada de los datos. Este modelo es el modelo entidad/interrelación que actualmente se conoce más con el nombre de entidad/relación.

Modelo entidad – relación

Denominado por sus siglas como E-R, representa a la realidad a través de entidades, que son objetos que existen y que se distinguen de otros por sus características, por ejemplo: un alumno se distingue de otro por sus características particulares como lo es el nombre, o el número de cuenta asignado al entrar a una institución educativa. Las entidades pueden ser de dos tipos:

- Tangibles: son todos aquellos objetos físicos que se pueden ver, tocar o sentir.
- Intangibles: todos aquellos eventos u objetos conceptuales que no se pueden ver, aun sabiendo que existen, por ejemplo: la entidad materia, se sabe que existe, sin embargo, no se puede visualizar o tocar.

⁴⁹ Chen. P. (1976). *The entity-relationship model: Towards a unified view of data*, ACM Trans. Sistemas de bases de datos, p. 9-36.

Pasos del esquema ER al Modelo relacional

En el modelo relacional los datos se organizan en tablas cuyos datos se relacionan. Edgar Frank Codd definió las bases del modelo relacional a finales de los 60⁵⁰. Trabajaba para IBM, empresa que tardó un poco en implementar sus bases. Pocos años después el modelo se empezó a implementar cada vez más, hasta ser el modelo de bases de datos más popular. (Ver figura 7.27).

En las bases de Codd se definían los objetivos de este modelo:

- Independencia física. La forma de almacenar los datos, no debe influir en su manipulación lógica
- Independencia lógica. Las aplicaciones que utilizan la base de datos no deben ser modificadas por que se modifiquen elementos de la base de datos.
- Flexibilidad. La base de datos ofrece fácilmente distintas vistas en función de los usuarios y aplicaciones.
- Uniformidad. Las estructuras lógicas siempre tienen una única forma conceptual (las tablas).
- Sencillez.

Transformaciones de entidades.

En principio las entidades de modelos Entidad Relación son transformadas al modelo relacional siguiendo estas instrucciones:

- **Entidades.** Las entidades pasan a ser tablas.
- **Atributos.** Los atributos pasan a ser columnas.
- **Identificadores principales.** Pasan a ser claves primarias.
- **Identificadores candidatos.** Pasan a ser claves candidatas.

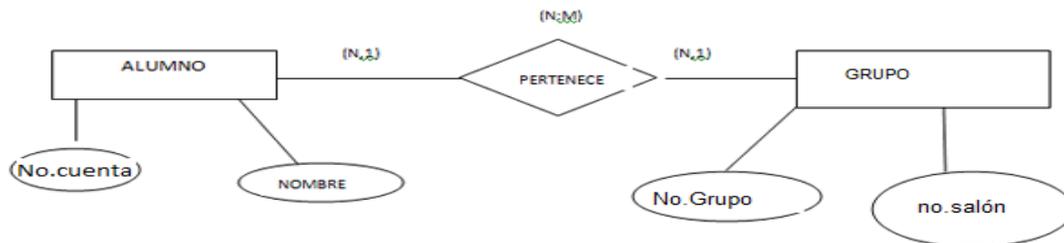


Figura 7.27 Ejemplo de modelo entidad relación.

⁵⁰ En 1970, Codd publicó en ACM el trabajo “Un modelo de datos relacional para grandes bancos de datos compartidos”. Extraído el 2 de junio de 2012 desde: <http://petra.euitio.uniovi.es/docencia/cursos/tercero/sis.ges.bas.dat/apuntes/12codd98.html>

Transformación de relaciones

La idea inicial es transformar a cada relación en una tabla en el modelo relacional. Pero hay que distinguir según el tipo de relación.

- **Relación varios a varios:** En las relaciones varios a varios, la relación se transforma en una tabla cuyos atributos son: los atributos de las relación y las claves de las entidades relacionadas (que pasarán a ser claves externas). La clave de la tabla la forman todas las claves externas.
- **Relaciones de orden n:** Las relaciones ternarias, cuaternarias y n-arias que unen más de dos relaciones se transforman en una tabla que contiene los atributos de la relación más los identificadores de las entidades relacionadas.
- **Relaciones uno a varios y uno a uno:** Las relaciones binarias de tipo uno a varios no requieren ser transformadas en una tabla en el modelo relacional. En su lugar la tabla de lado varios (tabla relacionada) incluye como la clave externa el identificador de la entidad del lado uno (tabla principal).

Una vez obtenido el esquema relacional resultante del modelo entidad relación que representaba la base de datos, normalmente se tiene una buena base de datos. Pero otras veces, debido a fallos en el diseño o a problemas indetectables en la fase del diseño, se cuenta con un esquema que puede producir una base de datos que incorpore estos problemas:

- **Redundancia:** Se llama así a los datos que se repiten continua e innecesariamente por las tablas de la base de datos.
- **Ambigüedades:** Datos que no clarifican suficientemente el registro al que representan.
- **Pérdida de restricciones de integridad.**
- **Anomalías en operaciones de modificación de datos.** El hecho de que al insertar un solo elemento haya que repetir tuplas en una tabla para variar unos pocos datos, o que eliminen un elemento suponga eliminar varias tuplas.

La solución a estos problemas suele ser dividir la tabla con problema en otras tablas más adecuadas.

Formas normales

Las formas normales se corresponden a una teoría de normalización iniciada por Codd. Codd definió en 1970 la primera forma normal, desde ese momento aparecieron la segunda, tercera, la Boyce-Codd, la cuarta y la quinta forma normal.

La teoría de formas normales es una teoría absolutamente matemática, pero en el presente trabajo, se describen de forma intuitiva:

- **Primera forma normal (1FN):** una tabla se encuentra en 1FN si impide que un atributo de una tupla pueda tomar más de un valor.
- **Segunda Forma Normal (2FN):** ocurre si una tabla está en primera forma normal y además cada atributo que no sea clave, depende de forma funcional completa respecto de cualquiera de las claves. Toda la clave principal debe hacer dependientes al resto de atributos, si hay atributos que depende sólo de parte de la clave, entonces esa parte de la clave y esos atributos formarán otra tabla.
- **Tercera Forma Normal (3FN):** ocurre cuando una tabla está en 2FN y además ningún atributo que no sea clave depende transitivamente de las claves de la tabla. Es decir, no ocurre cuando algún atributo depende funcionalmente de atributos que no son clave.
- **Forma Normal de Boyce-Codd (FNBC o BCFN):** ocurre si una tabla está en tercera forma normal y además todo determinante es una clave candidata.
- **Cuarta Forma Norma (4FN):** ocurre esta forma normal cuando una tabla está en forma normal de Boyce Cood y toda dependencia multi-valuada es una dependencia funcional.
- **Quinta Forma Normal (5FN):** es la más compleja y polémica de todas. Polémica porque no está claro en muchas ocasiones que sea una solución mejor que el no llegar a este nivel de normalización. Una tabla no está en quinta forma normal si hay una descomposición de esa tabla que muestre la misma información que la original.

Definición de Sistema de Gestión de Base de Datos

Los Sistemas de gestión de base de datos (SGBD) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la

utilizan. Los SGBD son un conjunto de programas encargados de definir, construir y manipular una base de datos, y mantener su integridad y redundancias. (Ver figura 7.28)

Las características de un Sistema Gestor de Base de Datos SGBD son:

- **Abstracción de la información.** Los SGBD ahorran a los usuarios detalles acerca del almacenamiento físico de los datos. Da lo mismo si una base de datos ocupa uno o cientos de archivos, este hecho se hace transparente al usuario. Así, se definen varios niveles de abstracción.
- **Independencia.** La independencia de los datos consiste en la capacidad de modificar el esquema (físico o lógico) de una base de datos sin tener que realizar cambios en las aplicaciones que se sirven de ella.
- **Redundancia mínima.** Un buen diseño de una base de datos logrará evitar la aparición de información repetida o redundante. De entrada, lo ideal es lograr una redundancia nula; no obstante, en algunos casos la complejidad de los cálculos hace necesaria la aparición de redundancias.
- **Consistencia.** En aquellos casos en los que no se ha logrado esta redundancia nula, será necesario vigilar que aquella información que aparece repetida se actualice de forma coherente, es decir, que todos los datos repetidos se actualicen de forma simultánea.
- **Seguridad.** La información almacenada en una base de datos puede llegar a tener un gran valor. Los SGBD deben garantizar que esta información se encuentra segura frente a usuarios malintencionados, que intenten leer información privilegiada; frente a ataques que deseen manipular o destruir la información; o simplemente ante las torpezas de algún usuario autorizado pero despistado. Normalmente, los SGBD disponen de un complejo sistema de permisos a usuarios y grupos de usuarios, que permiten otorgar diversas categorías de permisos.
- **Integridad.** Se trata de adoptar las medidas necesarias para garantizar la validez de los datos almacenados. Es decir, se trata de proteger los datos ante fallos de hardware, datos introducidos por usuarios descuidados, o cualquier otra circunstancia capaz de corromper la información almacenada.
- **Respaldo y recuperación.** Los SGBD deben proporcionar una forma eficiente de realizar copias de respaldo de la información almacenada en ellos, y de restaurar a partir de estas copias los datos que se hayan podido perder.

- **Control de la concurrencia.** En la mayoría de entornos, lo más habitual es que sean muchas las personas que acceden a una base de datos, bien para recuperar información, bien para almacenarla. Y es también frecuente que dichos accesos se realicen de forma simultánea. Así pues, un SGBD debe controlar este acceso concurrente a la información, que podría derivar en inconsistencias.

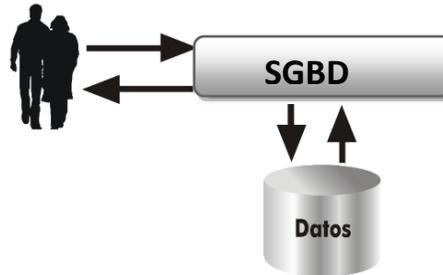


Figura 7.28 Esquema del funcionamiento y utilidad de un sistema gestor de base de datos.

Análisis y diseño de la base de datos asociada al sistema

Diseño Conceptual

Es el proceso de construcción de un modelo de los datos utilizados en una organización, independientemente de las consideraciones físicas. Es una descripción detallada de la estructura de la base de datos, y no importa cuál es el SGBD que se va a utilizar para manipular la base de datos. Un modelo conceptual es un lenguaje que se utiliza para describir esquemas conceptuales. El objetivo del diseño conceptual es describir el contenido de información de la base de datos y no las estructuras de almacenamiento que se necesitarán para manejar esta información.

El modelo conceptual de datos que se utilizó en el desarrollo de éste sitio web es el modelo Entidad-Relación (E-R). En el diagrama E - R que se muestra en la figura 7.29, están contenidas las siguientes entidades:

- **Administrador:** contiene información para acceso al administrador.
- **Alumno:** contiene datos personales de los estudiantes que se registran en el sistema.
- **Profesor:** contiene datos personales de los profesores que se registran en el sistema.
- **Grupos:** contiene el horario y número de grupos.
- **Quizz:** almacena las preguntas y las respuestas de cada examen.

- **Calificaciones:** Almacena las calificaciones de los alumnos por cada examen que realizan.

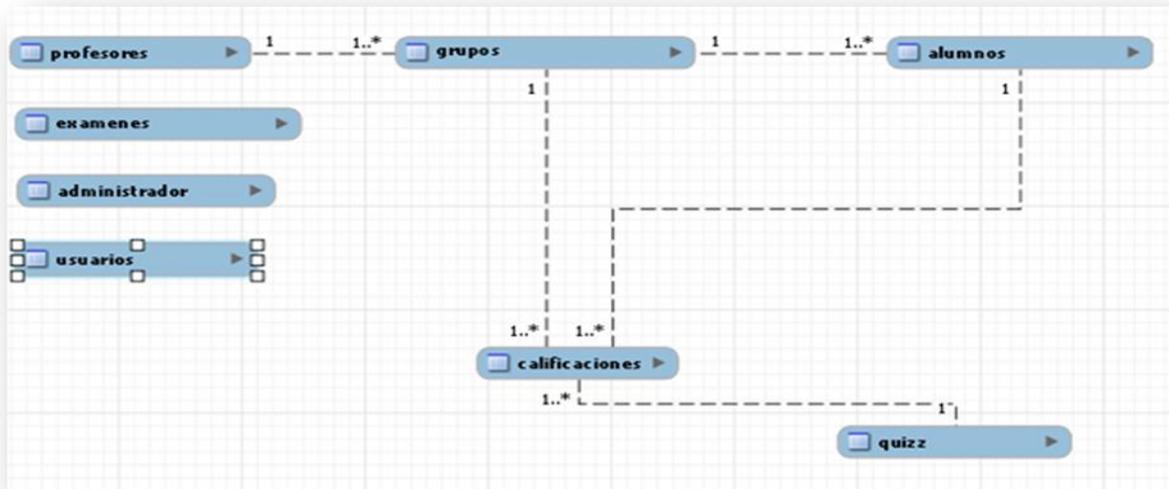


Figura 7.29 Modelo físico de BD general.

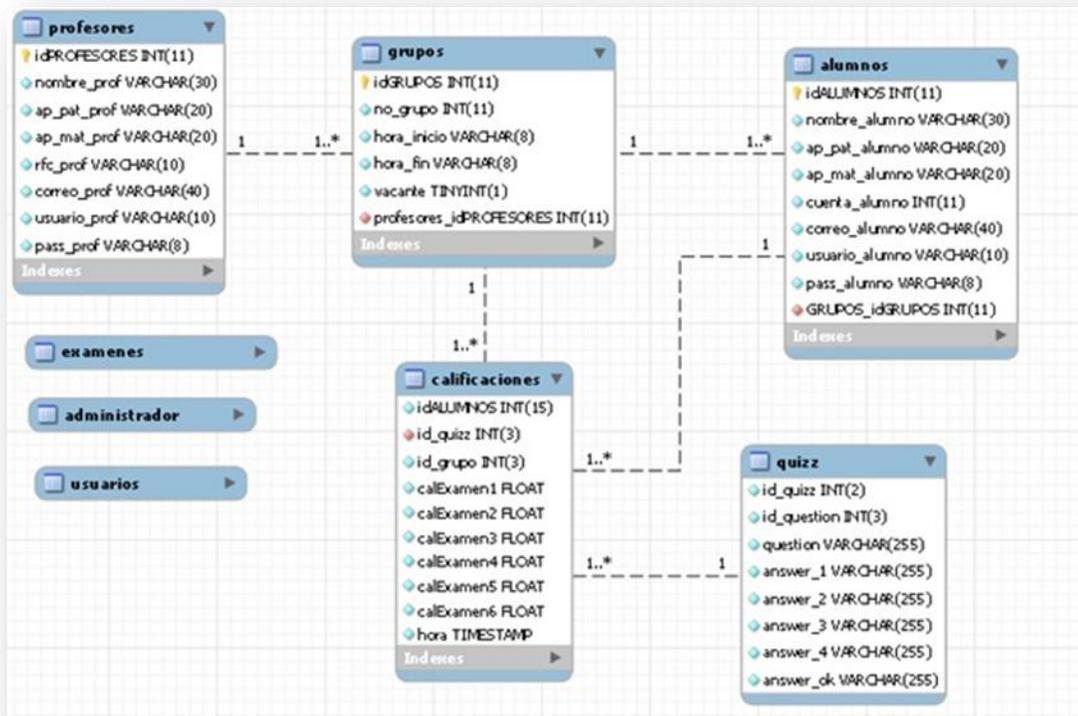


Figura 7.30 Modelo físico de BD detallado.

Para el manejo de la información de los exámenes se utilizan dos entidades más, las cuales son:

- **Exámenes:** Catalogo de títulos de exámenes por capítulo.
- **Usuarios:** Contiene los usuarios y contraseñas de los alumnos para poder acceder al sistema y realizar los exámenes.

7.2.4 Codificación

a) Para realizar la página de inicio, se utilizó el siguiente código en html:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>&deg;&deg;&deg;Administraci&ocaron de Redes;&deg;&deg;</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href=" ../Estilos/estilos.css" type="text/css" />
</head>
<!-- Comienza el cuerpo -->
<body>
<!-- Comienza cabecera -->
<div id="header">
<div class = "menu">
<ul>
<li><a href="index.htm">Inicio</a>
<li><a href="#">Temario</a>
<ul>
<li><a href="capitulo1.html">Capítulo I</a></li>
<li><a href="capitulo2.html">Capítulo II</a></li>
<li><a href="capitulo3.html">Capítulo III</a></li>
<li><a href="capitulo4.html">Capítulo IV</a></li>
<li><a href="capitulo5.html">Capítulo V</a></li>
<li><a href="capitulo6.html">Capítulo VI</a></li>
</ul>
<li><a href="#">Sesión</a></li>
<ul>
<li><a href="sesion-admon.html">Administrador</a></li>
<li><a href="sesion-profesor.html">Profesor</a></li>
```

```
<li><a href="sesion-alumno.html">Alumno</a></li>
</ul>

<li><a href="#">Registro</a></li>

<ul>
  <li><a href="registro-alumno.php">Alumno</a></li>
</ul>

<li><a href="glosario.html">Glosario</a></li>
<li><a href="enlaces.html">Enlaces</a></li>
<li><a href="creditos.html">Creditos</a></li>
</ul>

<div class= "menu p" />
</div>
</div>
</div>
<!-- end top navigation -->

<!-- Comienza la pagina -->
<div id="page">
<center><embed          src="../../Imagenes/prueba.swf"          quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"  type="application/x-
shockwave-flash" width="520" height="400" align="right">

<br><br><h1>Te damos la más cordial bienvenida a este portal educativo de apoyo
a la asignatura Administración de Redes.

<br><br>En este portal el usuario encontrará información confiable acerca de los
temas que se incluyen en el temario de la asignatura Administración de Redes,
asimismo habrá una sección de cuestionarios que podrá realizar una sola vez en un
tiempo de 30 minutos con ello podrá reafirmar conocimientos o bien identificar los
puntos a reforzar. También encontrará una sección de enlaces y bibliografía que
podrá consultar como apoyo para su aprendizaje.</h1>

<br><p><b>Para una correcta visualización se recomienda usar el navegador
Mozilla Firefox. Para descargar dar click en la imagen.</b>
<a href="http://www.mozilla.org/en-US/firefox/new/">
</a></b></p>
```

```

</embed>
</center>
</div>
<div class="page-end">
<a>&copy; Universidad Nacional Autónoma de México, Facultad de Ingeniería.
Todos los derechos reservados. </a>
</div>
</body>
</html>

```

Como se observa en el código anterior, la estructura del sitio se realizó a través de divisiones (div), y etiquetas de html. Así el resultado de la página principal es el siguiente (ver figura 7.31):



Figura 7.31 Página principal del sitio web educativo.

- b) Para realizar la conexión con la base de datos se utilizó el siguiente código de PHP:

```

<?php
function Conectar(){
    $db_host="localhost"; // Host al que conectar, habitualmente es el
    'localhost'
    $db_nombre="nombre_base"; // Nombre de la BD que se desea utilizar
    $db_user="nombre_usuario";//Nombre de usuario con permisos para
acceder

```

```
$db_pass="contraseña_usuario"; // Contraseña de dicho usuario

$con = mysql_connect($db_host, $db_user, $db_pass); // Realiza conexión
if (!$con){
    die('Could not connect: ' . mysql_error());
}
mysql_select_db($db_nombre , $con) or die("Error seleccionando la base de
datos.");
return $con;
}
?>
```

Lo primero que se hace es declarar cuatro variables donde se especifique el nombre del servidor en donde se encuentra la base de datos, el nombre de la base de datos, el nombre de usuario con el cual tratará de conectar y la contraseña de dicho usuario.

Una vez que se declaran las variables, se especifica el nombre del servidor en donde se encuentra la base de datos, enseguida se especifica el nombre de usuario con el cual tratará de conectar y por último se especifica la contraseña.

Después se especifica el nombre de la base de datos y en caso de que no exista la base de datos se manda un mensaje de error.

Los códigos desarrollados para la realización de la tesis en cuestión no se incluyen por razones de seguridad, debido a que al presentarlo generaría vulnerabilidades en el sistema.

Sin embargo se proporciona el enlace para poder visualizar el sitio web:

<http://redyseguridad.fi-p.unam.mx/proyectos/admonredes/PHP/index.htm#>

7.2.5 Pruebas de funcionalidad (basadas en requerimientos)

Las pruebas basadas en requerimientos son una aproximación sistemática al diseño de casos de prueba en donde el usuario considera cada requerimiento y deriva un conjunto de pruebas para cada uno de ellos. Las pruebas basadas en requerimientos son pruebas de validación en lugar de pruebas de defectos, el usuario intenta demostrar que el sistema ha implementado sus requerimientos de forma adecuada⁵¹.

⁵¹Sommerville, I. (2005). *Ingeniería de Software*. (7ª ed.) Madrid: Pearson Education. P. 502.

A continuación se detallan las pruebas realizadas al sitio web basadas en los requerimientos funcionales (ver tablas 7.11, 7.12 y 7.13):

Tabla 7.11 Pruebas de validación para usuario tipo alumno.

Los usuarios de tipo alumno estarán autorizados a realizar las siguientes funciones: registrarse y realizar exámenes	
Prueba realizada	Solución obtenida
Registro	Se ha generado un nuevo registro
Repite su registro con los mismos datos	No se generó el registro. El registro ya existe
Repite su registro con diferentes datos	Se ha generado un nuevo registro valido
Realizar un examen	Se ha actualizado la calificación del examen
Intenta repetir examen	No se permite. Sistema arrojó mensaje: "Ya haz realizado el examen".

Tabla 7.12 Pruebas de validación para usuario tipo administrador.

Los usuarios de tipo administrador estarán autorizados para realizar las siguientes funciones: alta de profesores y grupos, modificar información de grupos, profesores y alumnos, habilitar y deshabilitar exámenes	
Prueba realizada	Solución obtenida
Realiza alta profesor	Se ha generado registro de profesor
Intenta repetir registro de profesor con mismos datos	No se generó registro. El registro ya existe.
Repite el registro con diferentes datos	Se ha generado un nuevo registro valido
Realiza alta grupo	Se ha generado registro de grupo
Intenta repetir alta grupo con mismos datos	No se generó registro. El registro ya existe
Repite el registro con diferentes datos	Se ha generado un nuevo registro valido
Realiza edición de información de profesor	Se ha editado información de profesor
Realiza edición de información de grupo	Se ha editado información de grupo
Realiza edición de información de alumno	Se ha editado información de alumno
Se habilita un examen	Se ha habilita un examen
Se habilita el mismo examen	Se ha habilitado el mismo examen
Se deshabilita examen	Se ha deshabilitado examen
Se deshabilita mismo examen	Se ha deshabilitado mismo examen

Tabla 7.13 Pruebas de validación para usuario tipo profesor.

Los usuarios de tipo profesor estarán autorizados para realizar las siguientes funciones: Visualizar lista de calificaciones por grupo	
Prueba realizada	Solución obtenida
Visualiza lista calificaciones de grupo seleccionado	Se ha visualizado lista calificación por grupo

7.3 Actividades de evaluación

Para cubrir el objetivo de enseñanza-aprendizaje conjuntos, se estableció la sección de cuestionarios, el funcionamiento de dicha sección se describe a continuación:

Esta sección de cuestionarios está diseñada únicamente para aquellos alumnos que estén registrados en el sitio web, esto será controlado por el administrador del sistema el cual activará los exámenes en un día determinado, así al momento de que un alumno inicie sesión encontrará activo el examen correspondiente de acuerdo con el temario de la asignatura Administración de Redes. (Ver figuras 7.32, 7.33, 7.34 y 7.35)

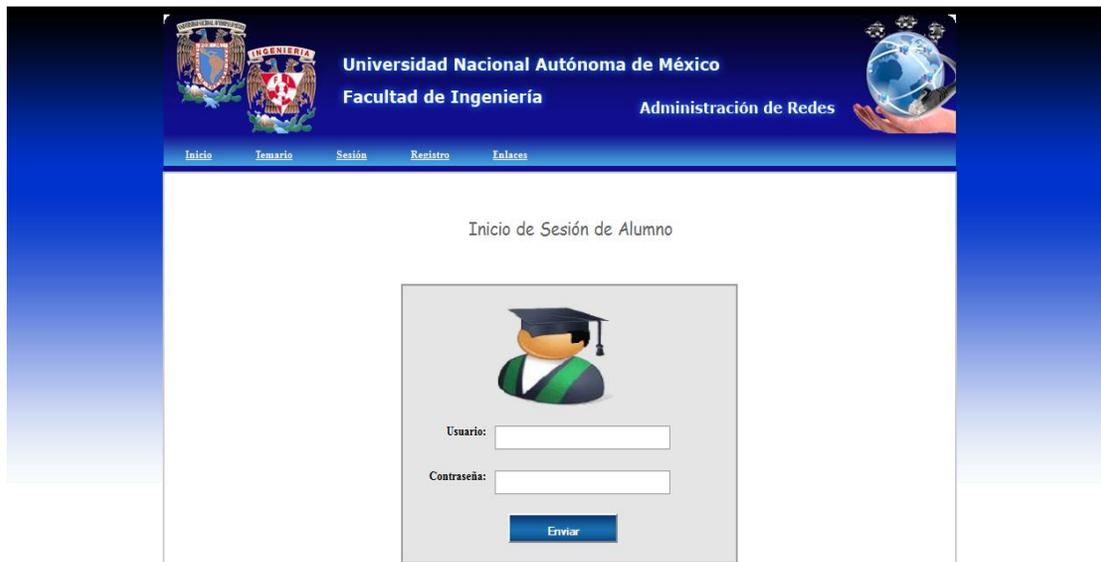


Figura 7.32 Página de inicio de sesión de alumnos.



Figura 7.33 Página de inicio de sección de exámenes.



Figura 7.34 Página para realizar examen.

Universidad Nacional Autónoma de México
Facultad de Ingeniería
Administración de Redes

Inicio Grupos Profesores Alumnos Base de Datos Salir

Examen activo			
Nombre del examen	Descripción	Estatus	Desactivar
Cápitulo 1	Conceptos básicos	Activo	Examen 1

Exámenes inactivos			
Nombre del examen	Descripción	Estatus	Activar
Cápitulo 2	Planeación	Inactivo	Examen 2
Cápitulo 3	Organización	Inactivo	Examen 3
Cápitulo 4	Integración	Inactivo	Examen 4
Cápitulo 5	Dirección	Inactivo	Examen 5
Cápitulo 6	Control	Inactivo	Examen 6

Figura 7.35 Página de administración para activar exámenes.

Para ello se desarrollaron seis cuestionarios que comprenden los 6 capítulos contenidos en el sitio web y en los cuales se abarcan cada uno de los temas vistos en la asignatura. Cada examen está conformado por 30 preguntas de las cuales aparecerán solamente 15 de manera aleatoria para que los exámenes no se repitan, evitando así que el usuario adivine o se aprenda las respuestas si éstas son estáticas.

En caso de que el alumno no termine de contestar el examen en 30 minutos el sistema automáticamente, muestra una pantalla indicando que el tiempo se agotó, inmediatamente después indica la calificación obtenida. (Ver figuras 7.36 y 7.37)

5. Se trata de los medios de transmisión que requieren un canal físico para transportar los datos en una red.

- Guiados o terrestres
- Cables UTP
- No guiados o aéreos
- Fibra óptica

6. ¿Qué categoría de cable UTP es la más usada en la implementación de redes?

- UTP categoría 5
- UTP categoría 6

Su tiempo se ha terminado

Aceptar

Figura 7.36 Mensaje indicador de terminación de tiempo para resolver examen.



Figura 7.37 Página que muestra la calificación obtenida.

Asimismo cada alumno tiene una sola oportunidad de realizar el cuestionario, la calificación queda asentada en la base de datos y puede ser consultada por los profesores. (Ver figura 7.38).



Grupo	Hora de inicio	Hora de término	Consultar
3	3:00 am	3:30 pm	Consultar
10	7:00 am	5:45 am	Consultar
230	2:00 am	4:45	Consultar

Figura 7.38 Listas de calificaciones por grupo.

RESULTADOS

Resultados:

Se realizó el sitio web educativo con el objeto de proporcionar a alumnos y profesores de la asignatura de Administración de Redes una herramienta para contribuir en su proceso de enseñanza-aprendizaje, esperando esta sea de utilidad en un futuro ya que cuenta con los elementos suficientes para lograr los resultados deseados. Por ello, se investigó a cerca de cada tema contenido en el temario de dicha asignatura y se realizaron resúmenes de éstos presentándolos mediante tablas, diagramas, imágenes y conceptos descritos con viñetas, con el fin de que el alumno experimente una lectura amena y entendible. Asimismo se incluyeron cuestionarios de evaluación con los que el alumno podrá poner en práctica los conocimientos obtenidos y el profesor tener un indicador de cómo van progresando los alumnos en cada capítulo.

Cabe destacar que las preguntas que contienen los cuestionarios en línea, también fueron supervisadas, de esa manera se trata de preguntas claves que tienen el objetivo de evaluar los conocimientos que adquieran los usuarios al accesar y leer el sitio web. Las preguntas presentadas se muestran de forma aleatoria, con lo cual siempre aparecen diferentes y se con ello se evitará que el usuario adivine la respuesta de la pregunta, con eso se forzará a que el usuario previamente haya leído a cerca de lo que se le está preguntando.

Se proporcionaron los elementos para brindar el apoyo en el proceso de enseñanza-aprendizaje, sin embargo depende de alumnos y profesores en qué magnitud lo puedan y quieran explotar.

Claro está que este sitio web es un panorama introductorio a cada tema, en donde, si el usuario desea saber más acerca de ellos, podrá hacer una investigación más a fondo, pero teniendo las bases necesarias.

CONCLUSIONES

“Lo maravilloso de aprender algo es que nadie puede arrebatárnoslo”.

B.B.King.

Conclusiones:

En la actualidad el uso de redes de datos se ha intensificado a tal grado que se está convirtiendo en una necesidad básica para la vida de muchas personas y organizaciones en general, por ello se torna imprescindible que las redes cumplan con sus objetivos principales: disponibilidad, confiabilidad, eficiencia y seguridad. Para cumplir con dichos objetivos es fundamental contar con conocimientos sólidos de administración de redes, que ayuden al profesional a prevenir fallos, ataques informáticos, dar mantenimiento, y obtener una mayor productividad. De ahí radica la importancia del desarrollo de la presente tesis: apoyar al aprendizaje de los alumnos que se convertirán en esos futuros profesionales capaces de enfrentar y solucionar tales problemáticas de manera eficaz y eficiente.

Lo anterior representa una de las motivaciones para realizar la presente tesis pero también, se centró en aportar algo a la Facultad de Ingeniería, que ayudará a los alumnos y profesores, pero en particular a los de la carrera de Ingeniería en Computación. Esto nos llevó a analizar e identificar lo que se nos había hecho más complicado a lo largo de la carrera, por ello, con base en nuestra experiencia y por comentarios de compañeros de nuestra generación, optamos por brindarle un apoyo a la asignatura de *Administración de Redes*, por lo siguiente:

La información que cubre el temario de la asignatura en cuestión es extensa, se encuentra dispersa en múltiples fuentes digitales e impresas y se cuenta con poco tiempo para ahondar en ella y abordarla en su totalidad. Entonces hace que el proceso de enseñanza-aprendizaje se torne tedioso y que no se esté logrando un aprendizaje efectivo sobre los temas. Por lo tanto, recopilando material, resumiéndolo, y presentándolo mediante el uso de imágenes, diagramas y ejemplos, los alumnos podrán comprender con mayor facilidad cada tema. Así también desarrollando cuestionarios de evaluación y poniéndolos a disposición de alumnos y profesores se logra brindar un apoyo para el proceso de enseñanza-aprendizaje.

Pero, ¿Cómo logramos proporcionar el apoyo tanto a profesores como alumnos? Se decidió elaborar un sitio web, lo cual se debió a la facilidad y comodidad que tendrán los usuarios para emplearlo en línea, por la simple razón de que puede ser consultado desde cualquier parte en donde exista una computadora con conexión a Internet haciendo uso del explorador Mozilla Firefox.

Así el resultado obtenido de la realización de esta tesis se resume en la construcción del sitio web, lo cual representa una herramienta de apoyo al proceso de enseñanza-aprendizaje para los profesores y alumnos respectivamente. Por supuesto, sería como un complemento y nunca con la intención de sustituir la relación profesor-alumno, sino como un refuerzo para el aprendizaje de la asignatura de *Administración de Redes*. Para establecer la relación de enseñanza-aprendizaje se conjuntaron dos elementos, los resúmenes con la información de la materia y la sección de exámenes.

Para la elaboración de los resúmenes tuvimos que consultar en distintas fuentes impresas y digitales y obtener la información adecuada para cubrir el objetivo de cada capítulo del temario de la asignatura. Esto no significa, que al tener de manera concentrada la información y con el simple hecho de que el usuario la lea se vuelva un experto en los temas, pero sí obtendrá las bases para ahondar en cualquiera de ellos.

En el proceso de búsqueda de información en fuentes impresas se tuvo dificultad, ya que, actualmente, en la Facultad de Ingeniería no se cuenta con material bibliográfico que abarque en su totalidad el contenido de los temas que se proponen en el temario de la asignatura, por lo que se consultaron diferentes fuentes, entre ellas algunas digitales, para obtener a partir de éstas cada resumen. Además algunos temas eran demasiados extensos, por lo que optamos por explicarlos a través de tablas, diagramas y descripciones mediante viñetas, para así, lograr que al usuario no se le haga tan pesado o tedioso leer los temas que son muy extensos. Por otro lado, temas como el de direccionamiento lógico, no sabíamos cómo abordarlo en un principio, ya que se trata de un tema teórico-práctico que consta de varios pasos y que para poder comprenderlo es imprescindible explicar cada uno de ellos, sin excepción. Esto lo pudimos solucionar diseñando un ejemplo donde se pudiera observar cada acción realizada de manera detallada hasta obtener el resultado tanto de direccionamiento lógico por subneteo como por VLSM.

Referente a la disponibilidad de la información, surgió la cuestión de dejarla restringida o no, sin embargo, pensamos que esta herramienta, como fuente de información fiable debe servir no sólo a los estudiantes que cursan la asignatura, sino a todo aquel usuario interesado en aprender acerca de la administración de las redes.

Aunado a lo anterior se realizó una serie de cuestionarios que, al realizar los alumnos, permiten medir su nivel de comprensión de cada capítulo y así, reforzar los temas que encuentren más complicados, colaborando así en su auto-aprendizaje. Además, el profesor puede utilizar dichas calificaciones como medida de avance en el aprendizaje de los

alumnos y de acuerdo con su criterio, incorporarla como parte de sus evaluaciones si así lo desea, o bien, reforzar algún tema que él crea necesario.

Al elaborar los cuestionarios pertenecientes a cada capítulo nos encontramos que los alumnos podrían memorizar las respuestas o copiarse entre sí, por tal motivo, pensamos que la mejor solución fue realizar un apartado de treinta preguntas por cada examen, de las cuales, mostrar únicamente quince en pantalla para que los alumnos las puedan resolver y que el orden de éstas sea de manera aleatoria; otra medida que decidimos incluir fue asignarles a los exámenes un tiempo máximo de solución de treinta minutos para que de esta forma los alumnos, usuarios del sistema, lean cada tema antes de resolver un examen y no en el momento de estar contestando los reactivos.

Cabe mencionar que la realización de cuestionarios también fue supervisada, con el fin de incluir los puntos clave de cada tema y poniendo especial énfasis en que esas preguntas se plantearán de forma clara para los alumnos.

En cuanto a la elaboración de esta herramienta se utilizó el diseño gráfico, para lograr que el sitio web se tornara atractivo a la vista de los usuarios, para que de esta manera, éstos permanezcan interesados en él. Esto fue algo que se nos dificultó ya que no teníamos ninguna experiencia en esta área, por ello, tuvimos que investigar temas referentes a ello, tales como: estructuras de sitios web, psicología de los colores y como realizar animaciones y logos. Por lo que tuvimos que aprender a usar las herramientas de Adobe Flash y Adobe Photoshop.

Así el diseño estético del sitio web, en un principio se pensó realizarlo únicamente con imágenes estáticas, sin embargo, se optó por agregar algunas animaciones para que la navegación no se tornara aburrida y tediosa para el usuario, sin caer en el exceso, ya que ello representa un factor que distrae al usuario del objetivo principal a cubrir.

Por otro lado, dentro de las sugerencias que podríamos plantear para futuras mejoras mencionamos las siguientes:

- Una vez puesto en marcha el sitio web, realizar encuestas dentro de la comunidad estudiantil para saber si la información y los exámenes incluidos les hayan servido de algo en su rendimiento académico de la asignatura de *Administración de Redes* y de esta manera incluir elementos que puedan ayudar a mejorarlo.

- Se podría retomar el proyecto para incluir una sección donde alumnos y profesores puedan subir archivos de interés y así difundir más conocimientos.
- Otra mejora que se podría implementar a futuro sería la de incluir actividades interactivas al final de cada tema para ir reforzando aún más cada uno de ellos.

Por último, cabe mencionar, que el desarrollo de esta tesis, nos deja la satisfacción de saber que las futuras generaciones contarán con información completa y concisa que los introduzca acerca de los temas de la asignatura de *Administración de Redes*, para su mejor desempeño como estudiantes y a su vez como profesionales, así como también para los profesores, para que les apoye en su labor de enseñanza. Aportando así a la Facultad de Ingeniería una herramienta informática dirigida a la asignatura de *Administración de Redes*.

Por lo tanto y basado en lo expuesto anteriormente, la hipótesis planteada se comprobó, ya que la herramienta, es decir, el sitio web educativo se elaboró con los elementos suficientes para apoyar al proceso de enseñanza-aprendizaje de la asignatura de *Administración de Redes*, dependiendo no de nosotras sino de alumnos y profesoras el uso y explotación de la misma.

GLOSARIO



- **2B1Q:** se trata de un tipo de codificación para transmitir datos, consiste en codificar 2 bits (2B) mediante un pulso que puede asumir 4 valores, -3, -1, 1 o 3 volts, llamado elemento o símbolo (1Q). Este código de línea permite mejorar la eficiencia en la transmisión a largas distancias de las señales digitales.
- **1FN (Primera forma normal):** es una forma normal usada en normalización de base de datos. Una tabla de base de datos se encuentra en 1FN si impide que un atributo de una tupla pueda tomar más de un valor.

A

- **ADSL (Asimetric Digital Subscriber Line – Línea de Abonado Digital Asimétrica):** es un sistema de transmisión de datos con elevado ancho de banda que se implementa sobre las líneas telefónicas convencionales, haciéndolo de un modo asimétrico, ya que la velocidad de recepción de datos es diferente a la de envío. Permite enviarlos desde 128 Kbps hasta 612 Kbps, y recibirlos desde 1,544 Mbps hasta 6 Mbps.
- **AI (Auditoría Informática):** proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
- **Amenaza:** es todo aquello que pretende o intenta destruir o dañar un bien. Se encuentra latente y representa sólo una posibilidad de poder manifestarse.
- **AMI (Alternate Mark Inversion- Inversión de marcas alternadas):** es un código en línea, el cual se usa para transmisiones de datos, en este caso, binarias. En este código, cuando se asigna un impulso positivo al primer "1", al siguiente "1" se le asigna un impulso negativo, y así sucesivamente.
- **ANSI (American National Standards Institute - Instituto Nacional Estadounidense de Estándares):** es una organización miembro de la ISO, sin ánimo de lucro que supervisa el desarrollo de estándares de productos, servicios, procesos y sistemas en los Estados Unidos, con el objetivo que los productos de dicho país puedan usarse en todo el mundo.
- **API (Application Programming Interface - Interfaz de Programación de Aplicaciones):** conjunto de rutinas, procedimientos, protocolos, funciones y herramientas que determinada biblioteca pone a disposición para que sean utilizados por

otro software como una capa de abstracción. En otras palabras, es una interfaz que permite la comunicación entre distintos componentes software.

- **Ataque:** se trata de la culminación de una amenaza, es decir, cuando una amenaza se aprovecha de una o varias vulnerabilidades, por lo que se presenta un daño ya sea en menor o mayor medida.
- **ATM (Asynchronous Transfer Mode - Modo de Transferencia Asíncrona):** es una tecnología de telecomunicación que transmite información en forma de cortos paquetes de longitud constante y que pueden ser enrutados individualmente mediante el uso de canales virtuales.
- **Autenticación:** es la acción de verificar la identidad del usuario o proceso que desea acceder al recurso o la información.

B

- **BD (Data Bases - Bases de datos):** es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso.
- **Bps (Bits por segundo – Bits per second):** se trata de una unidad del SI (Le Système International d'Unités -Sistema Internacional de Unidades) utilizada para expresar la velocidad de transmisión de datos, en otras palabras, se trata del número de impulsos elementales (1 o 0) transmitidos en cada segundo.
- **BSS (Basic Service Set - Conjunto de Servicios Básicos):** se trata del conjunto de dos elementos, BSC (Base Station Controller - Controlador de Estaciones base) y BTS (Base Transceiver Station - Estación de Transmisión-Recepción Base), que en conjunto forman estaciones inalámbricas, con lo que es posible conectarse a un centro de conmutación móvil para que se puedan establecer y cortar llamadas.

C

- **CAP (Carrierless Amplitude and Phase - Modulación de fase y amplitud sin portadora):** es un tipo de modulación que fue ampliamente utilizada en los comienzos de la ASDL pero nunca se estandarizó correctamente y en consecuencia, no existe interoperabilidad posible entre el hardware de los distintos fabricantes. Consiste en que una portadora es impuesta por la banda trasmisora formando un filtro a través del cual los símbolos fuera de los límites son filtrados.

CAP divide la señal modulada en segmentos que después almacena en memoria. La señal portadora se suprime, puesto que no aporta ninguna información ("carrierless"). La onda transmitida es la generada al pasar cada uno de estos segmentos por dos filtros. En recepción se reensamblan los segmentos y la portadora, volviendo a obtener la señal modulada.

- **CC (Criterios Comunes - Common Criteria):** norma internacional para evaluar la seguridad de los productos de tecnología, cuyo objetivo principal es proporcionar protección a la información como, no revelar secretos sin autorización, perder información por el uso y modificar la información.
- **CCITT (Consultative Committee for International Telegraphy and Telephony - Comité Consultivo Internacional de Telefonía y Telecomunicaciones):** es el antiguo nombre de la organización de normalización internacional de las telecomunicaciones, actualmente conocido como ITU.
- **CDMA (Code Division Multiple Access - Acceso Múltiple por División en Código):** Técnica usada para transmitir datos que hace una división asignando a cada usuario un código diferente, de esta manera es posible que varios usuarios puedan transmitir de manera simultánea sobre el mismo canal.
- **CERN (The European Organization for Nuclear Research – Organización Europea de Investigación Nuclear):** es el laboratorio más grande de investigación en física de partículas fundado en 1954 y ubicado entre la frontera de Francia y Suiza. Además se trata de uno de los centros de investigación más importantes del mundo.
- **CLNS (Connectionless Network Service - Servicio No Orientado a Conexión):** es un servicio de telecomunicaciones que establece la comunicación entre entidades sin necesidad de establecer una conexión entre ellas. Cuando una entidad tiene información para transmitir, sencillamente la envía.
- **CMIP (Common Management Information Protocol - Protocolo de administración de información común):** es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes.
- **CMIS (Common Management Information Services – Servicios Comunes de Información de Administración):** se refiere al conjunto de servicios proporcionados por la arquitectura de administración OSI los cuales definen su implementación en el protocolo CMIP y son invocados mediante un conjunto de instrucciones relacionadas

con uno o varios objetos de la MIB, por ejemplo, obtener un valor de un atributo (M – GET), modificar el valor de un atributo (M –SET), entre otros.

- **CMISE (Common Management Information Service Element - Elemento Común de Servicio de Información de Gestión):** es uno de los componentes de la arquitectura del protocolo CMIP, que se encarga de la generación de requerimientos (requests) estándares básicos y el procesamiento de mensajes de respuesta según lo definido por el CMIS.
- **Cookies:** son pequeños archivos que algunos sitios web guardan en la computadora. Por ejemplo, cuando un usuario introduce su nombre y contraseña en determinada página de Internet, se almacenan estos datos en una cookie para que no tenga que estar introduciéndolos para cada página del servidor. Cabe mencionar que ocupan espacio en disco por lo que se recomienda borrarlas periódicamente.
- **CORBA (Common Object Request Broker Architecture - Arquitectura Común de Intermediarios en Peticiones a Objetos):** se trata de una arquitectura de programación distribuida diseñada para soportar objetos independientemente de su ubicación dentro de una red o máquina, lo que permite la interoperabilidad entre diferentes aplicaciones escritas en diferentes lenguajes y ejecutadas en diferentes plataformas.
- **Cross-Connects (Conexiones Cruzadas):** esquema de conexión en el que el equipo activo se conecta a un panel de parcheo o bloque de terminación y éste a su vez a otro panel de parcheo mediante cables de parcheo.

D

- **DCF (Data Communication Function - Función de Comunicación de Datos):** es una función de TMN que se utiliza para transportar, de manera pasiva, la información de gestión intercambiada entre los demás bloques funcionales (OSF, NEF, WSF, MF y QAF) ya que es la encargada de proveer las funciones de las tres primeras capas del modelo de referencia OSI.
- **DMT (Discrete Multi-tone Modulation - Modulación por Multitono Discreto):** es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.
- **DQDB (Distributed Queue Dual Bus - Bus Dual de Cola Distribuida):** se trata de la implementación del estándar IEEE 802.6 definido para redes de área metropolitana. Consiste en dos buses unidireccionales, en los cuales todas las estaciones están

conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si ésta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo. Actualmente este protocolo se encuentra en desuso.

- **DWDM (Multiplexación por División en Longitud de Onda - Dense Wavelength Division Multiplexing):** se trata de un tipo de multiplexación que se realiza por división en longitud de onda, tiene su origen en la posibilidad de acoplar las salidas de diferentes fuentes emisoras de luz, cada una a una longitud de onda diferente sobre una misma fibra óptica.
- **DSSS (Direct Sequence Spread Spectrum - Espectro Ensanchado por Secuencia Directa):** el término espectro ensanchado es una técnica de transmisión en la cual un código pseudoaleatorio, independiente de los datos de información, es empleado como forma de onda modulante para “esparcir” la energía de la señal sobre un ancho de banda mucho mayor que el ancho de banda de información de la señal original. Los sistemas de secuencia directa (DS) son sistemas de espectro ensanchado en los cuales la portadora, es decir, la señal que contiene la información a transmitir, está modulada por un código de dispersión de alta velocidad y una corriente de datos de información. La secuencia del código de alta velocidad es el causante directo del ensanchamiento de la señal transmitida.

E

- **EAL (Evaluation Assurance Level - Niveles de evaluación de garantía):** están definidos en el ISO/IEC 15408-3 y van desde EAL1 a EAL7 definen el nivel de seguridad con que cuenta determinado sistema así como la garantía de la solución de fallas.
- **EIA (Electronic Industries Alliance – Alianza de Industrias Electrónicas):** es una organización comercial de fabricantes de electrónica y alta tecnología en EE.UU. cuya misión es promover el desarrollo del mercado y competitividad.
- **ER (Entity Relationship):** conocido también como Diagrama de Entidad Relación por sus siglas en español DER. Es una herramienta para el modelado de datos que permite representar las entidades de un sistema informático así como sus relaciones y propiedades.
- **Ethernet:** es un protocolo de acceso de red TCP/IP para redes de área local. Que define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

- **Ética:** la palabra ética proviene del latín *ethos*, cuyo significado es costumbre; actualmente se define como el conjunto de principios, valores, costumbres y normas de conducta, adquiridos, asimilados y practicados de un modo estrictamente racional o consciente. Corresponde al ejercicio libre y consciente de la razón para justificar nuestros actos desde el punto de vista del bien y del mal.
- **Etom (Enhanced Telecommunication Operations Map - Mapa de Operaciones de Telecomunicaciones Mejorado):** es un modelo que sirve como marco de referencia de procesos de negocio orientado al sector de las telecomunicaciones. Describe y analiza todos los procesos empresariales necesarios para el funcionamiento de una empresa.
- **E&M trunks (Puertos E & M):** es un tipo de señalización que fue desarrollado para permitir centrales (conjunto de varias líneas telefónicas) en diferentes ubicaciones geográficas para comunicarse a través de un circuito privado analógico. Es un tipo de señalización que utiliza corriente directa (DC), las señales en los cables por separado, llamados la iniciativa E y el cable M. Dependiendo de quién está hablando, E&M puede significar el “oído y la boca”, o desde otro punto de vista la tierra y el imán. La parte del “oído” representa la conexión eléctrica a tierra y la parte del imán o bien la “boca” representa el tono en el auricular del teléfono.

F

- **FDM (Frequency Division Multiplexing - Multiplexación por División de Frecuencia):** es un tipo de multiplexación usada para dividir el ancho de banda disponible en un medio físico en varios canales lógicos independientes más pequeños quedando cada canal con un ancho de banda más angosto, de manera que se puedan enviar continuamente señales provenientes de diferentes canales de baja velocidad sobre el canal de alta velocidad. Este proceso es utilizado generalmente en líneas telefónicas y en conexiones físicas de pares trenzados para incrementar la velocidad de los datos.
- **FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos):** se trata de un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Protocolo de Control de Transferencia), basado en la arquitectura cliente – servidor.

G

- **Gateway o puerta de enlace:** es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local conectadas a él de un acceso hacia una red exterior.

- **GPRS (Packet Radio Service - Servicio General de Paquetes Vía Radio):** es una extensión de GSM, para la transmisión de datos no conmutada o por paquetes. Se encarga de actualizar los servicios de datos GSM para hacerlos compatibles con redes de área local (LANs), redes de área extendida (WANs) e Internet.
- **GSM (Global System for Mobile Communications - Sistema Global para las comunicaciones Móviles):** es un estándar abierto de tecnología celular que pertenece a la segunda generación de tecnologías celulares. Permite realizar llamadas de voz y transferencia de datos.



- **HDB3 (High Density Bipolar-3 Zeros - Código de Alta Densidad Bipolar de 3 Ceros):** es un código de telecomunicaciones principalmente usado en Japón, Europa y Australia. Consiste en sustituir secuencias de bits que provocan niveles de tensión constantes por otras que garantizan la anulación de la componente continua y la sincronización del receptor. La longitud de la secuencia queda inalterada, por lo que la velocidad de transmisión de datos es la misma; además el receptor debe ser capaz de reconocer estas secuencias de datos especiales.
- **HDSL (High bit rate Digital Subscriber Line o Línea de abonado digital de alta velocidad binaria):** es un sistema de transmisión de datos simétrica, ya que provee el mismo ancho de banda en los dos sentidos, es de alta velocidad y utiliza dos pares de cables trenzados.
- **HLR (Home Location Register - Registro de Localización de Llamada):** es una base de datos utilizada por la tecnología GSM donde se almacena la posición del usuario dentro de la red, si se encuentra conectado o no, servicios que puede y no puede usar, tipo de terminal y toda la información administrativa referente al usuario. Es de carácter permanente, ya que, cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.



- **IDL (Interface Definition Language – Lenguaje de Descripción de Interfaz):** es un lenguaje de programación pensado exclusivamente para especificar las interfaces que usarán los clientes, usados en el modelo CORBA. La tarea de una IDL es poner de acuerdo con distintos lenguajes en el formato y tamaño de sus especificaciones.

- **IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos):** es la mayor asociación internacional sin fines de lucro formada por ingenieros eléctricos, en electrónica, en computación y en telecomunicaciones. Su trabajo es promover la creatividad, el desarrollo, la integración y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.
- **IMEI (International Mobile Equipment Identity - Identidad Internacional de Equipo Móvil):** es un código pre-grabado en los teléfonos móviles GSM. Este código identifica al aparato de forma única a nivel mundial, y es transmitido por el teléfono a la red al conectarse a ésta. Esto quiere decir que la operadora conoce, quién y desde dónde hace la llamada y desde qué terminal telefónica la hizo.
- **IP (Internet Protocol - Protocolo de Internet):** forma parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de paquetes de datos (datagramas), aunque sin garantizar su entrega. El protocolo IP determina el destinatario del mensaje.
- **IPv4 (Internet Protocol versión 4 - Protocolo de Internet versión 4):** es la cuarta versión del protocolo IP (Internet Protocol – Protocolo de Internet), y la primera en ser implementada a gran escala. IPv4 usa direcciones de 32 bits, limitándola a $2^{32} = 4.294.967.296$ direcciones únicas, muchas de las cuales están dedicadas a redes locales. Debido al enorme crecimiento que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), se ha visto que las direcciones IPv4 ya son muy escasas.
- **ITU (Unión Internacional de Telecomunicaciones - International telecommunications Union):** Organismo encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras de las mismas.
- **IOP (Internet Inter ORB Protocol - Interoperabilidad entre ORB):** CORBA especifica el GIOP (General Inter ORB Protocol - Protocolo Entre ORBs General) que define la comunicación entre ORBs diferentes. IOP es una instancia de GIOP que se usa en redes de tipo TCP/IP, gracias a esto, es posible que objetos que emplean ORBs de fabricantes distintos puedan interoperar en redes como Internet.
- **ISDN (Integrated Services Digital Network - Red Digital de Servicios Integrados):** es un protocolo de red de comunicaciones, que contempla tanto las comunicaciones de voz, como las de datos, transmitiendo ambas sobre la misma infraestructura en formato digital, y a distintas velocidades. Es totalmente digital y permite el transporte de voz y

de datos (textos, gráficas, videoconferencia, etcétera) todo transmitido desde una única interfaz de red.

- **ITSEC (Information Technology Security Evaluation Criteria – Criterio de Evaluación de la Seguridad de las Tecnologías de la Información):** mejor conocido como el libro blanco, surgió en 1991, proveía niveles de seguridad donde se definía la funcionalidad del producto desarrollado.

K

- **Kbps (Kilobites por segundo - Kilobits per second):** es una unidad de medida que se usa en telecomunicaciones para calcular la velocidad de transferencia de información a través de una red. Equivale a transmitir 1000 bits por segundo.

L

- **LAN (Local Area Network - Redes de Área Local):** son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Son redes pequeñas, habituales en oficinas, colegios y empresas pequeñas. Las velocidades de transmisión típicas de LAN van de 10 a 100 Mbps.
- **LOS (Line of Sight - Conexión con línea de vista):** es un término utilizado en comunicaciones por radiofrecuencia para describir un trayecto que debe tener visibilidad directa entre antenas para lograr una comunicación exitosa entre emisor y receptor.

M

- **Mbps (Megabit por segundo – Megabit per second):** es una unidad de medida que se usa en telecomunicaciones para calcular la velocidad de transferencia de información a través de una red. Equivale a transmitir 1000 kilobits por segundo o bien 1000000 bits por segundo.
- **Metadatos:** son datos que describen otros datos. Por ejemplo lo que se guarda en los sistemas de archivo, es decir, para cada archivo informático almacenado se guardan los siguientes metadatos: fecha y hora de creación, fecha y hora de modificación y última vez que fue accedido.

- **MF (Mediation Function - Bloque de Función de Mediación):** es un elemento de la arquitectura funcional de TMN que forma parte de las funciones fundamentales requeridas por TMN para cumplir su función general de gestión de red. Específicamente se encarga de que la información entre un bloque de función TMN-compatible y un bloque de función no-TMN-compatible será traducida por otro elemento funcional TMN llamado QAF (Q Adaptor Function - Bloque de función de adaptador Q).
- **Middleware:** es un software que conecta componentes de software o aplicaciones para que puedan intercambiar datos entre ellas. Es utilizado a menudo para soportar aplicaciones distribuidas. Esto incluye servidores web, servidores de aplicaciones, sistemas de gestión de contenido, entre otras. Este concepto surge como una solución al problema de cómo conectar nuevas aplicaciones con viejos sistemas, así como para facilitar el procesamiento distribuido: conexión de múltiples aplicaciones para crear una aplicación más grande, generalmente sobre una red.
- **MSC (Mobile Switching Center - Centro de Conmutación Móvil):** es el elemento principal de todo sistema GSM, se encarga de establecer, gestionar y despejar conexiones, así como de enrutar las llamadas a la celda correcta. Proporciona la interfaz con el sistema telefónico.
- **MTP (Message Transfer Parts - Parte de Transferencia de Mensaje):** se trata de un conjunto de recomendaciones que se dividen en tres niveles: capa física, la cual define las características físicas, eléctricas y funcionales del enlace de señalización digital, la capa de enlace de datos, que se encarga de proporcionar una transferencia fiable de mensajes de señalización entre dos puntos de señalización conectados directamente, y la capa de red, la cual proporciona la ruta y los aspectos de gestión de tráfico de MTP.
- **MySQL:** es un sistema de administración de bases de datos para bases de datos relacionales. Se caracteriza por ser de código abierto, portable (puede trabajar en distintos sistemas operativos) y multiproceso. Utiliza el lenguaje de programación SQL (Structured Query Language – Lenguaje de Consulta Estructurado) para realizar consultas a la base de datos.



- **NEF (Network Element Function - Bloque de Función de Elemento de Red):** elemento de la arquitectura funcional de TMN que forma parte de las funciones fundamentales requeridas por TMN para cumplir su función general de gestión de red.

Su función es posibilitar la conmutación de los datos entre los usuarios de la red de telecomunicaciones.

- **NLOS (Non Line of Sight - Conexión sin Línea de Vista):** es un término utilizado en comunicaciones por radiofrecuencia para describir un trayecto parcialmente obstruido entre la ubicación del transmisor de la señal y la ubicación del receptor de la señal. Los obstáculos que pueden obstaculizar la línea de vista incluyen árboles, edificios, montañas y otras estructuras y/o objetos construidos por el hombre u obra de la naturaleza.

O

- **OAM (Operations, Administration, and Management - Operación, Administración y Mantenimiento):** es un término generalmente utilizado para describir los procesos, actividades, instrumentos, normas, etcétera, relacionados con la explotación, administración, gestión y mantenimiento de cualquier sistema. Es más común en el contexto de las redes de ordenadores o quipos informáticos.
- **OFDM (Orthogonal Frequency Division Multiplexing - Multiplexación por División de Frecuencias Ortogonales):** es un tipo de multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.
- **OMG (Object Management Group - Grupo de Gestión de Objetos):** es una organización sin ánimo de lucro que promueve el uso de tecnología orientada a objetos mediante guías y especificaciones para las mismas, cuidando y estableciendo diversos estándares para el manejo de mencionadas tecnologías.
- **OSF (Operations System Function - Bloque de Función de Sistemas de Operaciones):** elemento de la arquitectura funcional de TMN que forma parte de las funciones fundamentales requeridas por TMN para cumplir su función general de gestión de red. Procesa información relacionada a la gestión de telecomunicaciones con el propósito de monitorear, coordinar y controlar funciones de telecomunicaciones incluyendo funciones de gestión. Inicia las operaciones de gestión y recibe las notificaciones de los agentes.
- **OSI (Open System Interconnection - Modelo de Interconexión de Sistemas Abiertos):** es un modelo de referencia que proporciona una descripción generalizada de las herramientas de interconectividad de redes, que se divide en siete capas donde cada una

de ellas realiza funciones diferentes: aplicación, presentación, sesión, transporte, red, enlace de datos y física.

- **ORB (Object Request Brokers - Intermediario de Petición de Objetos):** se trata del núcleo de cualquier implementación CORBA, transmiten los mensajes que se intercambian cliente y servidor, por lo que se ocupan de canalizar las comunicaciones entre los objetos locales y los remotos y localizar al objeto remoto a partir de una referencia.



- **PDH (Plesiochronous Digital Hierarchy - Jerarquía Digital Plesiócrona):** es una tecnología usada en telecomunicaciones usada para transportar grandes cantidades de información mediante equipos digitales de transmisión, tradicionalmente se utiliza para telefonía y permite enviar varios canales telefónicos sobre un mismo medio, cable coaxial, fibra óptica, radio o microondas.
- **PDU (Protocol Data Unit - Unidades de Datos de Protocolo):** se refiere a la forma que adopta una sección de datos en cualquier capa del modelo OSI. Una PDU tiene un nombre distinto para reflejar su nuevo aspecto, por ejemplo, se llama *segmento* en la capa de transporte, *paquete* en la capa de red, *trama* en la capa de enlace y *bits* en la capa física.
- **Perpetrador:** toda aquella persona que lleve a cabo conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.
- **PHP:** es el acrónimo de Hipertext Preprocessor. Es un lenguaje de programación que se ejecuta del lado del servidor web, lo cual permite que se realicen accesos a bases de datos, conexiones en red y otras tareas para crear la página final que verá el cliente. Así el cliente solamente recibe una página con código HTML.
- **POTS (Plain Old Telephone Service - Servicio telefónico Ordinario Antiguo):** es conocido también como Servicio Telefónico Tradicional o Telefonía Básica y se refiere al servicio telefónico estándar de voz analógico (no digital) que utiliza hilos de cobre.
- **PP (Protection Profile - Perfiles de Protección):** es un documento usado como parte del proceso de evaluación de los criterios comunes, el cual define un conjunto de objetivos y requisitos de seguridad, independientemente de la implementación, para una categoría de productos que cubre las necesidades de seguridad comunes a varios

usuarios. Permitiendo la elaboración de estándares funcionales y constituye una ayuda para la formulación del pliego de condiciones de un producto.

- **Propender:** acción de inclinarse por alguna cosa en especial o bien tendencia hacia algo específico.
- **PSTN (Public Switched Telephone Network - red telefónica pública conmutada):** son redes desarrolladas a lo largo de los años para transmitir las señales vocales. Se basa en el concepto de conmutación de circuitos, es decir, la realización de una comunicación requiere el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una.

R

- **RDSI (Integrated Service Digital Network - Red Digital de Servicios Integrados):** es un tipo de red que agrupa distintos servicios anteriormente distribuidos a través de soportes distintos, siempre que se utilice tecnología digital: telefonía digital, videoconferencia, mensajería electrónica, sonido, datos, imágenes, etcétera. Esto implica el uso de protocolos idénticos y redes físicas de banda ancha. Este tipo de redes no se ven afectadas por ruidos e interferencias y alcanza velocidades entre los 64 y 128 Kbps.
- **RDSL (Integrated Services Digital Network - Red Digital de Servicios Integrados):** es una red que procede por evolución de la Red Telefónica convencional, facilita conexiones digitales extremo a extremo entre los terminales conectados a ella, como teléfono, fax y ordenador para proporcionar una amplia gama de servicios, tanto de voz como de datos, a la que los usuarios acceden a través de un conjunto de interfaces normalizadas definidas por el ITU-T. Esta red coexiste con las redes convencionales de telefonía y datos, tendiendo a convertirse en una única y universal red de telecomunicaciones.
- **RFC (Request for Comments - Petición De Comentarios):** Son documentos cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. Sirven de referencia para la comunidad de Internet, ya que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

S

- **SCP (Service Control Point - Punto de Control de Servicio):** se trata de una de las tres clases de puntos de señalización en una red SS7. Se trata de una base de datos centralizada que determina cómo reenviar una llamada, un ejemplo de esto son los números 800 y 900. Un SCP responde con el número telefónico real, asociado con el número 800/900 marcado.
- **SDH (Jerarquía Digital Síncrona - Synchronous Digital Hierarchy):** es un protocolo de transporte que opera en la primera capa del modelo OSI. Se basa en la existencia de una referencia temporal común (Reloj primario), que multiplexa diferentes señales dentro de una jerarquía común flexible, y gestiona su transmisión de forma eficiente a través de fibra óptica, con mecanismos internos de protección.
- **SGBD (Sistema de Gestión de Base de Datos):** se trata de un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.
- **SGSN (Serving GPRS Support Node - Nodo de Soporte de Servicio GPRS):** es el elemento de la arquitectura GPRS responsable de la gestión de la conexión del terminal móvil a la red GPRS.
- **SIP (Session Initiation Protocol - Protocolo de Inicio de Sesiones):** es un protocolo de control, pensado para la creación, modificación y terminación de sesiones, con uno o más participantes. Esas sesiones pueden comprender conferencias multimedia, llamadas telefónicas sobre Internet (o cualquier otra red IP). Utiliza el modelo de Internet y lo convierte al mundo de las telecomunicaciones, utilizando protocolos de Internet existentes tales como HTTP y SMTP (Simple Mail Transfer Protocol). También usa una estructura de dirección URL. Usa estas direcciones de tipo correo electrónico para identificar a los usuarios en lugar de los dispositivos que los utilizan. De esta forma SIP no depende del dispositivo y no hace distinción alguna entre voz y datos, teléfono u ordenador.
- **SMAES (Systems Management Application Entity - Entidad de aplicación de gestión de sistemas):** es la entidad de nivel de aplicación del protocolo CMIP (Common Management Information Protocol - Protocolo de administración de información común) responsable del intercambio de información de gestión con SMAES de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red.

- **SMAP (Systems Management Application Process - Proceso de Aplicación del Sistema de Administración):** se define como el elemento del protocolo CMIP que proporciona la interfaz con la información compartida por la MIB (Base de Información de Administración). Los SMAPs dialogan con otros SMAPs a través de la red.
- **SNMP (Simple Network Management Protocol - Protocolo Simple de Administración de Red):** es un protocolo que pertenece a la capa de aplicación y facilita el intercambio de información de administración entre dispositivos de red, formando parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, así como planear su crecimiento.
- **SONET (Synchronous Optical Network - Red Óptica de Sincronía):** se trata de un conjunto de estándares para la transmisión o transporte de datos síncronos a través de redes de fibra óptica. Tanto SONET como SDH sirven para lo mismo, con la diferencia de que SONET es utilizada en Estados Unidos, Canadá, Corea, Taiwán y Hong Kong; mientras que SDH es utilizada en el resto del mundo. Los estándares de SONET están definidos por la ANSI (American National Standards Institute - Instituto Nacional Estadounidense de Estándares) y los de SDH por la ITU (International Telecommunications Union - Unión Internacional de Telecomunicaciones).
- **STM (Synchronous Transport Module - Módulo de transporte síncrono):** es la trama utilizada en la tecnología SDH que permite al operador incorporar o extraer sólo aquellas señales tributarias () que sean requeridas por el nodo, sin tener que multiplexar o demultiplexar totalmente la señal principal.
- **STP (Signal Transfer Point - Punto de Transferencia de Señal):** se trata de una de las tres clases de puntos de señalización en una red SS7. Se encarga de enrutar el tráfico de la red actuando como un concentrador debido a esto brinda un uso mejorado de la red SS7 al eliminar la necesidad de tener enlaces directos entre los diversos puntos de señalización. Además puede hacer las veces de un firewall para controlar los mensajes SS7 que se intercambian con otras redes.
- **SS7 (Sistema de Señalización de canal común número 7):** es un estándar global para las telecomunicaciones definidas por el sector de estandarización de las telecomunicaciones (ITU-T). Define el protocolo y los procedimientos mediante los cuales los elementos de la red de telefonía conmutada pública (PSTN, Public Switched Telephone Network) intercambian información sobre una red digital para efectuar el ruteo, establecimiento y control de llamadas. Satisface las necesidades tanto de voz como de datos, permitiendo una amplia gama de conexiones.

- **SSP (Service Switching Point. Punto de Intercambio de Servicio):** se trata de una de las tres clases de puntos de señalización en una red SS7. Son switches en los que se originan, terminan o se reenvían las llamadas. Un SSP envía mensajes de señalización a otros SSPs a fin de establecer, gestionar y liberar los circuitos de voz que se requieren para completar una llamada.

T

- **TCSEC (Trusted Computer Security Evaluation Criteria – Criterio de Evaluación de Seguridad de Cómputo Confiable):** conocido como, el libro naranja. Tiene su origen en 1980 y establece la aplicación de políticas de seguridad del departamento de defensa de Estados Unidos. Se preocupa fundamentalmente de la confidencialidad de la información clasificada a nivel nacional.
- **TDMA (Time Division Multiple Access - Acceso Múltiple de División de Tiempo):** se trata de una técnica de multiplexación que divide un único canal de frecuencia de radio en varias ranuras de tiempo. Así a cada persona que hace una llamada se le asigna una ranura de tiempo específica para la transmisión, lo que hace posible que varios usuarios utilicen un mismo canal simultáneamente sin interferir entre sí.
- **TDM (Time Division Multiplexing - multiplexación por división de tiempo):** es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de gran capacidad para transmitir a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión.
- **T1/E1:** E1 o Trama E1 es un formato de transmisión digital, el cual cuenta con un ancho de banda de 256 kilobytes transmitiendo a una velocidad de 2048 Mbps. T1 también es un formato de transmisión de datos y voz digitales, transmite a una velocidad de 1544 Mbps.
- **TCP/IP (Transmission Control Protocol/Internet Protocol - Protocolo de Control de Transmisión/Protocolo de Internet):** es el conjunto de protocolos de red en los que está basada Internet y que permite la transmisión de datos entre redes de computadoras. En concreto, TCP/IP hace referencia a los dos protocolos más importantes que forman al grupo: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP).
- **Terminal:** se refiere a un dispositivo de hardware que forma parte de una red de datos, el cual es utilizado para realizar una comunicación de paquetes de datos, es decir para enviar y recibir información.

- **TIA (Telecommunications Industry Association – Asociación de la Industria de Telecomunicaciones):** asociación industrial que junto con la EIA desarrollan y publican una serie de estándares sobre el cableado estructurado para voz y datos para las LAN.
- **TMN (Telecommunications Management Network - Red de Telecomunicaciones de gestión):** es un conjunto internacional de normas especificadas por la ITU (Unión Internacional de Telecomunicaciones - International telecommunications Union) para la gestión de redes de telecomunicaciones.
- **Token Ring:** es una implementación del estándar IEEE 802.5, que consiste en que un patrón de bits llamado token circula alrededor de una topología en anillo, pasando de máquina en máquina. Cuando una computadora desea transmitir una trama, debe tomar el token vacío (el tiempo que puede tener el token es de 10 mili segundos) y en ese momento enviar la información a la máquina que desea, una vez que la máquina destino recibió la información debe regresar el token a la computadora de origen con un mensaje de que recibió la información. Así se libera el token para que siga alrededor del anillo y otra máquina pueda usarlo para enviar información.

U

- **UDP (User Datagram Protocol – Protocolo de Datagrama de Usuario):** es un protocolo del nivel de transporte basado en el intercambio de datagramas (paquete con información totalmente independiente de otros). Es un protocolo no orientado a conexión y no detecta errores.
- **URL (Uniform Resource Locator – Localizador Uniforme de Recursos):** es una secuencia única de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones digitales, etc.
- **UTP (Unshielded Twisted Pair - Par Trenzado Sin Blindaje):** se trata de cables de pares trenzados y no dispone de protección contra las perturbaciones externas por lo que sólo es adecuado para entornos relativamente libres de perturbaciones.

V

- **VDSL (Very High Speed Digital Subscriber Line – Línea de Abonado Digital de muy Alto Índice de Datos):** es uno de los tipos de tecnología DSL que se refiere a una alternativa para alcanzar altas velocidades de transmisión de datos ya que es la

combinación de cables de fibra óptica que alimentan a las unidades ópticas de la red en los sectores residenciales y la conexión final a través de la red telefónica de cobre.

- **VLR (Visitor Location Register - Registro de Ubicación de Visitante):** es una base de datos utilizada en la tecnología GSM que contiene información administrativa seleccionada proveniente del HLR (Home Location Register - Registro de ubicación de origen), necesaria para el control de la llamada y provisión de servicios suscritos para cada móvil localizado en el área geográfica controlada por el VLR.

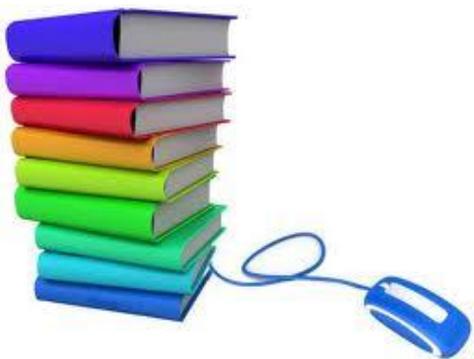


- **WiFi (Wireless Fidelity):** es una certificación de interoperabilidad de la industria que se basa en un subconjunto del estándar IEEE 802.11. Sin embargo, la palabra WiFi es conocida como Wireless Fidelity, que se refiere al estándar 802.11, en donde se definen las capas de enlace de datos y física del modelo OSI.
- **WSF (Workstation Function - Bloque de función de estación de trabajo):** se trata de uno de los bloques que componen el modelo TMN, el cual provee los medios para interpretar la información de TMN por parte del usuario y viceversa.
- **WWW (World Wide Web – Red Informática Mundial):** consiste en un medio de comunicación en donde se dispone de documentos de hipertexto (o sea se incluyen enlaces a otros sitios web) con texto, imágenes, videos o gráficos. Para acceder a estos documentos o páginas web, se requiere de un navegador, que no es más que un software capaz de interpretar de manera gráfica o visible la información que obtiene de Internet.



- **xDSL (Digital Subscriber Line - Línea de abonado digital):** es un grupo de tecnologías de comunicación que permiten transportar información multimedia a mayores velocidades que las que se obtienen actualmente vía modem, simplemente utilizando las líneas telefónicas convencionales.

REFERENCIAS



BIBLIOGRAFÍA

Black, U. (1997). *Redes de computadores. Protocolos, normas e interfaces*. (2ª ed.) México: Alfaomega.

Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 1: Aspectos básicos de networking*. México: Pearson Prentice Hall.

Cisco Networking Academy. (2011). *CCNA Exploration 4.0, Módulo 4: Acceso a la WAN*. México: Pearson Prentice Hall.

Ford, M., Lew, K., Spanier, S. y Stevenson, T. (1998). *Tecnologías de interconectividad de redes*. México: Prentice Hall.

Gido, J. y Clements, J. Traducción: Peralta, P. (2006). *Administración exitosa de proyectos*, (3ª ed.). México: Cengage Learning.

Hernández, R., Fernández, C. y Baptista, P. (1991). *Metodología de la investigación*. México: McGraw-Hill.

Kenneth, S. y Aubrey, A. (2009). *Diseño y soporte de redes de computadoras: guía de estudios CCNA Discovery*. México: Prentice Hall.

León, A. y Widjaja, I. (2002). *Redes de comunicaciones: conceptos fundamentales y arquitecturas básicas*. México: Mc-Graw Hill.

López, M.J. y Quezada, C (2006). *Fundamentos de seguridad informática*. Facultad de Ingeniería: UNAM.

Raya, J.L. (1997). *Redes locales y TCP/IP*. México: Alfaomega.

Silberschatz, A. (2002). *Fundamentos de Bases de Datos*. España: Mc-Graw Hill.

Sommerville, I. (2005). *Ingeniería del software*. (7ª ed.) Madrid: Pearson Education.

Tanenbaum, A.S. (1997). *Redes de computadoras*, México: Pearson Education.

MESOGRAFÍA

Todas las ligas fueron revisadas por última vez el 16 de abril de 2012.

ADSL

http://biblioteca.usac.edu.gt/tesis/08/08_0146_EO.pdf

Auditoría informática

<http://es.scribd.com/doc/32292825/Fases-de-Metodologia-de-Auditoria-Informatica>

Ataques informáticos

http://www.e-ghost.deusto.es/docs/articulo_seguridad.pdf

Bases de datos

<http://www.un.org/spanish/Depts/dpi/seminario/pdf/basesdedatos.pdf>

Bases de datos relacionales

<http://www.jorgesanchez.net/bd/bdrelacional.pdf>

Cable coaxial

http://www.quiminet.com/ar6/ar_vcdadddsahgsAztg-los-cables-coaxiales.htm

CDMA

<http://www.angelfire.com/al4/cdmaone/>

Clasificación de las redes por su tamaño

<http://ploise11.blogspot.com/2009/06/2-clasificacion-de-redes-segun-su.html>

<http://www.mitecnologico.com/Main/ClasificacionRedes>

Creación del fondo

<http://www.cristalab.com/blog/fundamentos-basicos-del-diseno-web-c9811/>

<http://www.proyectacolor.cl/teoria-de-los-colores/propiedades-de-los-colores.html>

<http://www.desenredate.com/articulos/teoria-psicologia-color.php>

Conflictos

<http://www.bibliojuridica.org/libros/1/139/15.pdf>

CORBA

<http://www.dspace.espol.edu.ec/bitstream/123456789/1499/1/2943.pdf>

Diseño de bases de datos

<http://alarcos.inf-cr.uclm.es/doc/bda/doc/teo/ant/BDa-t5.pdf>

Diseño de redes

http://www.aprendaredes.com/downloads/Como_Administrar_Netes.pdf

DWDM

http://www.ramonmillan.com/documentos/dwdm_redestelecom.pdf

Ethernet

<http://www.slideshare.net/edbamo/ethernet-4268800>

Ética informática

<http://www.abcpedia.com/diccionario/definicion-etica.html>

Estándar IEEE 802.11

<http://www.laserwifi.com/estander802.11.htm>

Estándar IEEE 802.16

<http://es.wikitel.info/wiki/WiMAX>

<http://dSPACE.ups.edu.ec/bitstream/123456789/214/3/Capitulo%202.pdf>

Estructura web

<http://www.joseacortes.com/recursosweb/8pasos/estructura.htm>

<http://www.monografias.com/trabajos5/laweb/laweb.shtml>

<http://www.un.org/spanish/Depts/dpi/seminario/pdf/principiosfireworks.pdf>

Gerencia y liderazgo

<http://liderazgoygerencia.blogspot.com>

GPRS

<http://www.jeuazarru.com/docs/GPRS.pdf>

GSM

<http://www.coopvvg.com.ar/alumnado-gomara/Files/gsm.pdf>

<http://www.dsi.fceia.unr.edu.ar/downloads/distribuidos/material/monografias/RedesGSM.pdf>

GSM y CDMA

<http://dspace.ups.edu.ec/bitstream/123456789/177/2/Capitulo%201.pdf>

Historia de la web

http://www.conectu.com/v4/es_articulos.php?a=99

http://www.hipertexto.info/documentos/h_www.htm

INTERNET2

<http://www.ati.es/novatica/1997/128/intdos-2.html>

Liderazgo

<http://www.ehu.es/SusanaTejada/asignat/organi/temas/Tema%202.%20Estilos%20de%20liderazgo.pdf>

Medios de transmisión

<http://www.alegsa.com.ar/Dic/medio%20de%20transmision%20de%20datos.php>

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/Comunicaciones/Presentaciones_Proyector/Medios.pdf

Metodología de la Auditoría Informática

<http://www.itchetumal.edu.mx/paginasvar/Maestros/mduran/Archivos/METODOLOGIA%20DE%20UNA%20AUDITORIA%20DE%20SISTEMAS.pdf>

Modelo eTOM

<http://es.scribd.com/doc/57149898/Modelo-eTom>

Modelo TNM

<http://www4.ujaen.es/~mdmolina/grr/Tema%205.pdf>

Normas APA

<http://www.cibem.org/paginas/img/apa6.pdf>

Objetivos del diseño de redes

http://www.taringa.net/posts/apuntes-y-monografias/5605080/1_2_2-Diseno-de-Objetivos-de-Red.html

Par trenzado

<http://www.slideshare.net/sgalsan/cable-par-trenzado>

PHP

<http://www.lawebera.es/de0/primerospasos.php>

Protocolos de administración de redes

<http://redyseguridad.fip.unam.mx/pp/maru/labpracticasyProtocolos%20Administracion%20Red.ed.pdf>

Protocolo SNMP

<http://velezconde.wordpress.com/herramientas-para-gestion-y-monitoreo/>

Seguridad Informática

<http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf>

Serie ISO 27000

<http://www.iso27000.es/sgsi.html>

http://www.kriptopolis.org/docs/ISO-27001_Los-controles.pdf

http://www.kriptopolis.org/docs/ISO-27001_Los-controles2.pdf

Subnetting (subneteo)

<http://hbeatriz.files.wordpress.com/2010/06/direccionamiento-ip-y-subredes-ejercicios-resueltos-1194346207489436-2.pdf>

TDMA

<http://www.alegsa.com.ar/Dic/tdma.php>

Topologías de red

<http://www.slideshare.net/guest7bb5a1/redes-topologia-de-red>

Trabajo en equipo

<http://www.youtube.com/watch?v=iACHd5iitGM>

VLSM

http://www.fsksm.utm.my/~homepage/scr2213/VLSM%20Workbook%20v1_0.pdf



ANEXOS

Anexo A. Manual del usuario

El siguiente describe las actividades que cada usuario del sitio web podrá realizar, por ello se divide en tres secciones:

1. Administrador

Para realizar las siguientes tareas será necesario entrar al sitio web e iniciar sesión como administrador, como se muestra en la figura 1.

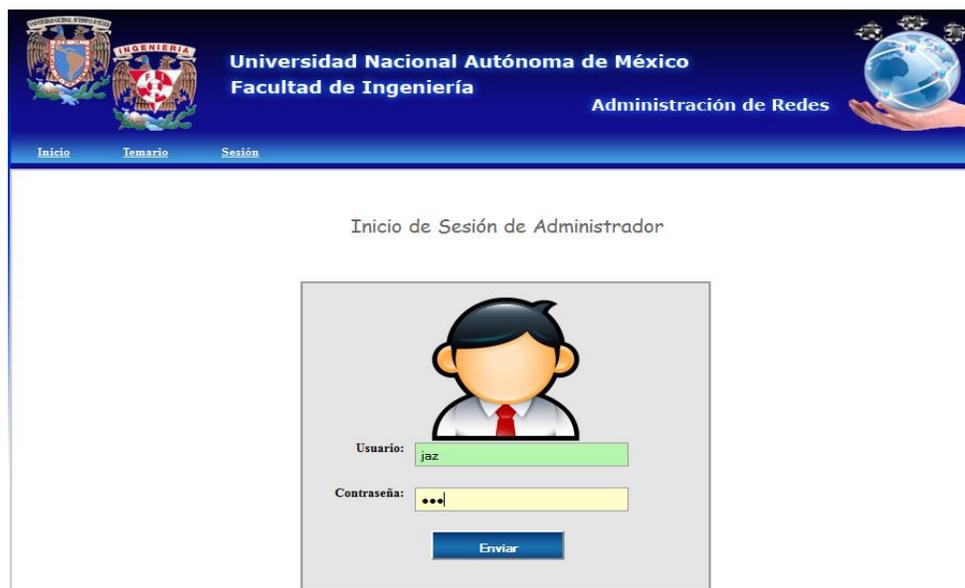


Figura 1 Inicio de sesión de administrador.

- a) **Registro de profesores:** una vez que se inicio sesión como administrador se deberá acceder a la sección de registros de profesor. (Ver figura 2).



Figura 2 pestaña para dar de alta profesores.

Se mostrará una pantalla como la que se muestra a continuación en la figura 3, dónde deberá ser debidamente llenado el formulario, este cuenta con validación de RFC y correo electrónico por lo que si cumplen con el formato no se podrá seguir con el registro.



Figura 3 Registro de profesores.

Al momento de dar clic en el botón de enviar se deberá mostrar una pantalla como la siguiente, dónde se indique que el registro fue exitoso. (Ver figura 4)



Registro Exitoso

Figura 4 Registro exitoso de profesor.

- b) Edición de profesores:** se deberá entrar a la sección de edición de profesores desde la barra de menú, como se muestra en la figura 2.

Al momento de dar clic en la pestaña de editar, se mostrará la siguiente pantalla, en la cual se podrá elegir el profesor para editar sus datos (figura 5):



Edición de Profesores

Seleccione un profesor para editar

Profesor:

- Seleccione un profesor
- \$nombre \$paterno \$materno
- Dulce1 Cruz Morales
- eli eli aa
- Dulce J a
- CINTIA QUEZADA REYES**
- anita santana delgadillo
- anita santanad delgadillo

Figura 5 Elegir profesor para editarlo.

Al momento de seleccionar el profesor y dar clic en el botón de enviar se mostrará la información del profesor seleccionado, como se muestra en la figura 6:

Registro de Profesores

Inserte los datos que se le piden a continuación

Nombre:

Ap. paterno:

Ap. materno:

RFC:

Correo:

Usuario:

Contraseña:

Figura 6 Datos de profesor para modificar.

Modificar los datos deseados y después dar clic en el botón de enviar para guardar los cambios. Para saber que el cambio se realizó se deberá observar una imagen como la siguiente (figura 7):



El registro fue editado exitosamente

Figura 7 Edición de profesor exitoso.

- c) **Registro de grupos:** se deberá realizar el registro de cada grupo perteneciente a la asignatura de Administración de Redes que quiera hacer uso del sitio web, para ello se deberán realizar las siguientes actividades:

Se muestra una pantalla como la siguiente (ver figura 8) donde se deberá seleccionar del menú la opción de grupos y seguido de esto la opción dar de alta y se mostrará una pantalla para llenar los datos del grupo a registrar. (Ver figura 9).



Figura 8 Sección de alta de grupos.



Alta de Grupos

Inserte el grupo con su respectivo horario

No. de grupo:	<input type="text" value="4"/>
Profesor:	<input type="text" value="anita santana delgadillo"/>
Hora inicio:	<input type="text" value="7:00 am"/>
Hora fin:	<input type="text" value="8:30 am"/>

Figura 9 Formulario para registrar grupos.

Una vez que se lleno el formulario con los datos del grupo a registrar se da clic en el botón de enviar y se debe de mostrar una imagen como la siguiente (ver figura 10) para saber que el grupo se registró correctamente:



Figura 10 Registro exitoso.

En caso de colocar un grupo existente mostrará el siguiente mensaje (figura 11):



Figura 11 Grupo existente.

- d) **Editar un grupo:** en esta sección se puede modificar el horario del grupo o el nombre del profesor que lo imparte; para ello es necesario entrar a la sección de edición de grupos, como se muestra en la figura 12:



Esta sección está diseñada para administrar el sistema de enseñanza-aprendizaje para la asignatura de Administración de Redes. Se podrán realizar las siguientes tareas: altas, bajas y cambios sobre la información relacionada con los grupos, alumnos y profesores; así también, el administrador será el responsable de habilitar los cuestionarios para que éstos puedan ser resueltos por los alumnos.



Figura 12 Sección de edición de grupos.

Una vez que se le dio clic a la pestaña de editar, se mostrará la siguiente pantalla (figura 13) para elegir el grupo que se requiere editar.



Edición de Grupo

Seleccione un grupo para editar

Grupo: 1

Seleccione un grupo

1
2
3
4
5
6
10
17
24
39
78
230

Figura 13 Elección de grupo a editar.

Ya que se seleccionó el grupo se muestra una pantalla (figura 14) donde se podrán seleccionar los datos que se requieren cambiar, ya sea el profesor asignado a ese grupo o bien el horario, seguido de realizar los cambios necesarios, dar clic en el botón de

enviar, y se deberá mostrar una imagen como la de la figura 15.



Edición de Grupos

Edite los datos que requiera

Profesor:

Hora inicio:

Hora fin:

Figura 14 Editar datos de grupo.

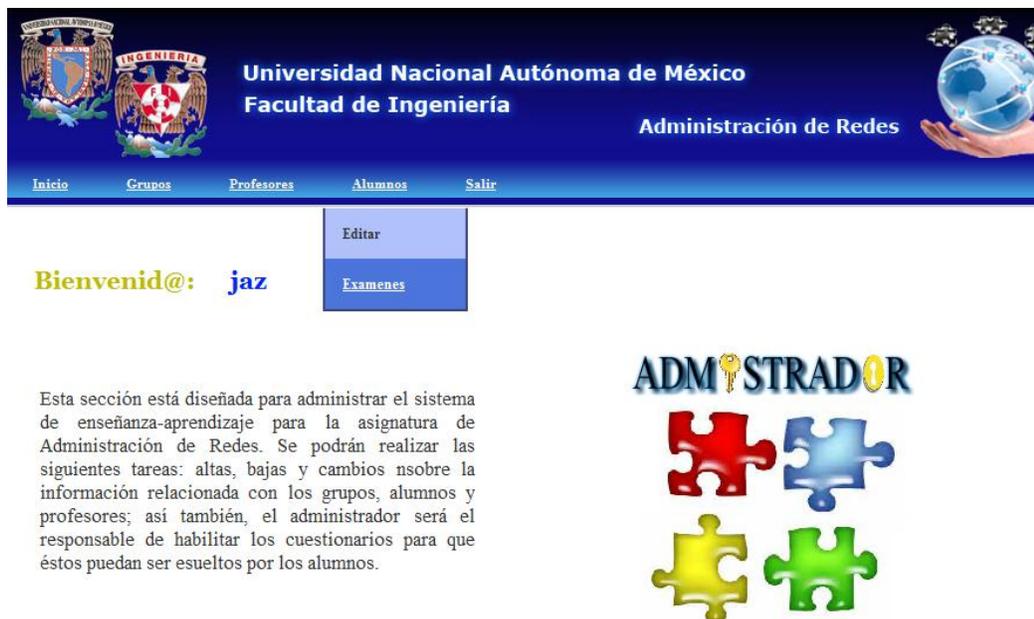


Edición Exitosa

Figura 15 Grupo editado exitosamente.

- e) **Editar alumno:** esta sección se diseñó con el propósito de editar los datos del alumno y poder modificarlos, esto, en caso de que a un alumno se le olvide su contraseña o por error haya registrado un dato incorrecto, así el administrador podrá asignarle una nueva contraseña o bien corregir cualquier dato.

Para realizar esta tarea, deberá entrar desde la barra del menú a alumno y después a editar, tal como se muestra en la figura 16:



Universidad Nacional Autónoma de México
Facultad de Ingeniería
Administración de Redes

Inicio Grupos Profesores Alumnos Salir

Bienvenid@: jaz

Editar
Exámenes

Esta sección está diseñada para administrar el sistema de enseñanza-aprendizaje para la asignatura de Administración de Redes. Se podrán realizar las siguientes tareas: altas, bajas y cambios nsobre la información relacionada con los grupos, alumnos y profesores; así también, el administrador será el responsable de habilitar los cuestionarios para que éstos puedan ser esueltos por los alumnos.

ADMINISTRADOR

Figura 16 Pestaña para entrar a editar alumno.

Una vez que se dé clic en editar se mostrará una pantalla para elegir el alumno que se desea editar (ver figura 17):



Universidad Nacional Autónoma de México
Facultad de Ingeniería
Administración de Redes

Inicio Grupos Profesores Alumnos Salir

Edición de Alumnos

Seleccione un alumno para editar

Alumno: ANGELICA CERVANTES AVALC

Enviar

Figura 17 Seleccionar alumno que se desea editar.

Al dar clic en el botón de enviar se mostrarán los datos del alumno seleccionado y es ahí donde se podrán editar cualquiera de los campos (figura 18), una vez que se realizaron los cambios deseados se envía la información y deberá aparecer una pantalla que nos indique que la edición fue exitosa (figura 19):



Universidad Nacional Autónoma de México
Facultad de Ingeniería
Administración de Redes

Inicio Grupos Profesores Alumnos Salir

Registro de Alumnos

Inserta los datos que se le piden a continuación

Nombre: ANGELICA

Ap. paterna: CERVANTES

Ap. materna: AVILOS

No. carnet: 304044348

Grupo: 1

Correo: engy_wax@hotmail.com

Usuario: engywas

Contraseña: *****

Enviar

Figura 18 Datos a editar del alumno.



Edición Exitosa

Figura 19 edición exitosa.

- f) **Activar y desactivar exámenes:** se podrá activar sólo un examen por lo que también se podrá desactivar únicamente dicho examen.

Para realizar estas actividades será necesario entrar a la sección de exámenes desde la barra de menú, como se muestra en la figura 20:



Bienvenid@: jaz

Editar

Exámenes

Esta sección está diseñada para administrar el sistema de enseñanza-aprendizaje para la asignatura de Administración de Redes. Se podrán realizar las siguientes tareas: altas, bajas y cambios sobre la información relacionada con los grupos, alumnos y profesores; así también, el administrador será el responsable de habilitar los cuestionarios para que éstos puedan ser esueltos por los alumnos.



Figura 20 Pestaña para entrar a activar o desactivar exámenes.

Al entrar a esta sección se mostrará la siguiente pantalla (figura 21), donde con sólo darle clic al examen deseado este se activará para poder ser resuelto por los alumnos, asimismo cuando se deseé desactivar bastará con darle clic al examen (ver figura 22):



<i>Examen activo</i>			
Nombre del examen	Descripción	Estatus	Desactivar
<i>Exámenes inactivos</i>			
Nombre del examen	Descripción	Estatus	Activar
Cápitulo 1	Conceptos básicos	Inactivo	Examen 1
Cápitulo 2	Planeación	Inactivo	Examen 2
Cápitulo 3	Organización	Inactivo	Examen 3
Cápitulo 4	Integración	Inactivo	Examen 4
Cápitulo 5	Dirección	Inactivo	Examen 5
Cápitulo 6	Control	Inactivo	Examen 6

Figura 21 Sección para activar y desactivar exámenes.



Examen activo			
Nombre del examen	Descripción	Estatus	Desactivar
Cápítulo 1	Conceptos básicos	Activo	Examen 1

Exámenes inactivos			
Nombre del examen	Descripción	Estatus	Activar
Cápítulo 2	Planeación	Inactivo	Examen 2
Cápítulo 3	Organización	Inactivo	Examen 3
Cápítulo 4	Integración	Inactivo	Examen 4
Cápítulo 5	Dirección	Inactivo	Examen 5
Cápítulo 6	Control	Inactivo	Examen 6

Figura 22 Examen 1 habilitado.

2. Alumnos

- a) **Registrar alumno:** en este apartado los alumnos podrán realizar su registro en el sistema. Para ello deberán entrar a registro de alumno, como se muestra en la figura 23.

Cabe mencionar que el registro de alumnos deberá ser realizado por los mismos, por lo cual esta sección no se encuentra restringida a ningún nivel.



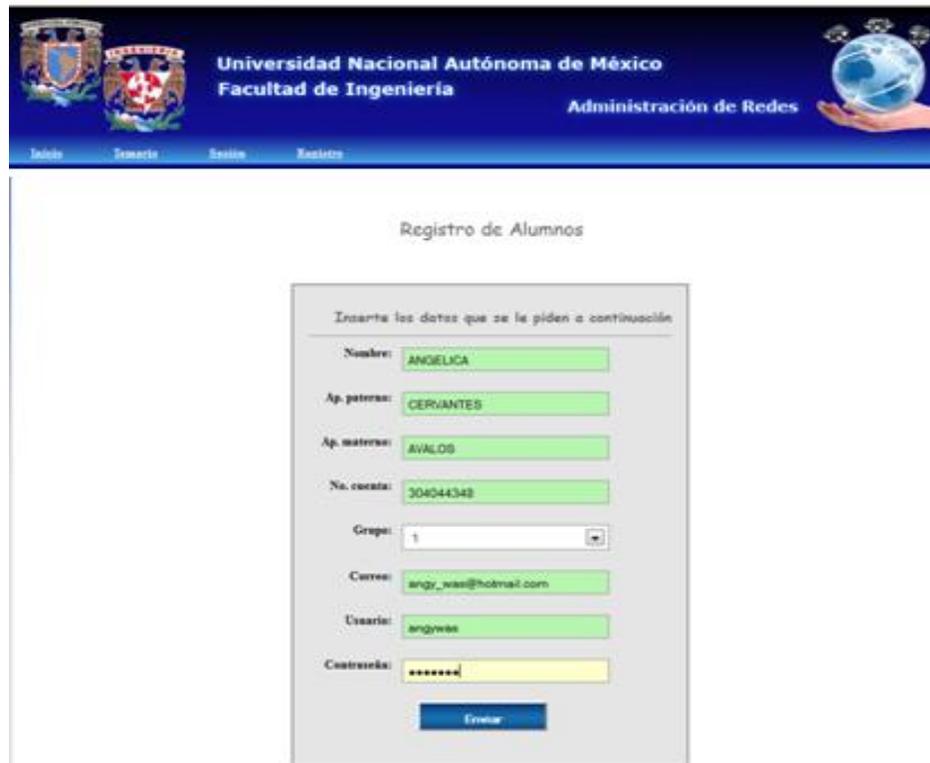
Te damos la más cordial bienvenida a este portal educativo de apoyo a la asignatura Administración de Redes.

En este portal el usuario encontrará información confiable acerca de los temas que se incluyen en el temario de la asignatura Administración de Redes, asimismo habrá una sección de cuestionarios que podrá realizar una sola vez en un tiempo de 30 minutos con ello podrá reafirmar conocimientos o bien identificar los puntos a reforzar. También encontrará una sección de enlaces y bibliografía que podrá consultar como apoyo para su aprendizaje.

BIENVENIDO

Figura 23 Pestaña para registrar alumno.

Una vez dentro se visualizará la pantalla con el formulario a llenar para poder realizar el registro (ver figura 24):



The screenshot shows the 'Registro de Alumnos' (Student Registration) form. At the top, there is a header for 'Universidad Nacional Autónoma de México Facultad de Ingeniería' and 'Administración de Redes'. The form itself is titled 'Registro de Alumnos' and contains the following fields:

- Nombre: ANGElica
- Ap. paterna: CERVANTES
- Ap. materna: AVALOS
- No. cuenta: 304044348
- Grupo: 1 (dropdown menu)
- Correo: angc_waa@hotmail.com
- Usuario: angcwa
- Contraseña: *****

At the bottom of the form is a blue 'Enviar' (Send) button.

Figura 24 Formulario para registrar alumno.



Figura 25 Registro exitoso de alumno.

Para realizar las siguientes tareas será necesario entrar al sitio web e iniciar sesión como alumno, como se muestra en la figura 26.



Inicio de Sesión de Alumno

Figura 26 Inicio de sesión de alumno.

- b) **Realizar examen:** en esta sección el alumno podrá realizar los exámenes, esto solamente en el caso de que uno de ellos se encuentre habilitado.

Una vez que inició sesión como alumno deberá dirigirse a la barra de menú y posicionarse en la pestaña de exámenes donde se desplegará la opción de realizar examen (figura 27).

En esta sección se podrán resolver los cuestionarios correspondientes a cada capítulo, los cuales van de acuerdo al temario de la asignatura Administración de Redes, éstos se encontrarán habilitados únicamente en la fecha indicada por el profesor. Es importante tener en cuenta que sólo tendrá una oportunidad para realizar la actividad por lo que es muy recomendable leer cada capítulo antes de comenzar el cuestionario ya que sólo contará con 30 minutos para su conclusión.

Figura 27 Pestaña para realizar examen.

En caso de que exista un examen habilitado, al dar clic en “realizar examen” se mostrará el examen a resolver, como se observa en la figura 28:



Universidad Nacional Autónoma de México
Facultad de Ingeniería
Administración de Redes

Usted tiene 30 minutos para realizar el examen: 00:02

Bienvenido: ANGELICA CERVANTES AVALOS
Examen: Capítulo 1
Descripción: Conceptos básicos

1. Es el modo de transmisión de infrarrojos donde la emisión es radial y se produce en casi todas las direcciones

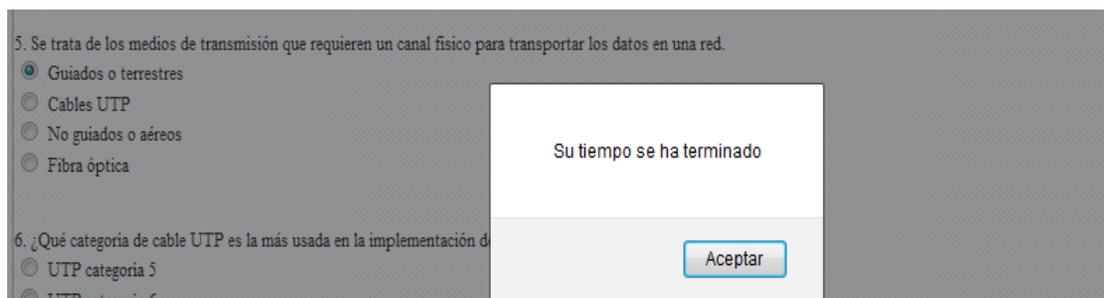
- Punto a punto
- Casi-Difuso
- Difuso
- Parcialmente difuso

2. Es la principal característica del medio inalámbrico de infrarrojos para que el transporte de datos entre dispositivos resulte exitoso

- Debe existir visibilidad directa entre los dispositivos que transmiten y reciben datos
- Atraviesa paredes de edificios y son omnidireccionales
- Transmiten a grandes velocidades y ancho de banda grande
- Conectan redes en áreas metropolitanas densamente pobladas

Figura 28 Interfaz para resolver examen.

Para la resolución del mismo se cuenta con 30 minutos, de modo que si en mencionado tiempo no se concluye el examen el sistema automáticamente lo dará por terminado (ver figura 29) y le mostrará una pantalla con la calificación obtenida (ver figura 30).



5. Se trata de los medios de transmisión que requieren un canal físico para transportar los datos en una red.

- Guiados o terrestres
- Cables UTP
- No guiados o aéreos
- Fibra óptica

6. ¿Qué categoría de cable UTP es la más usada en la implementación d

- UTP categoría 5
- UTP categoría 6

Su tiempo se ha terminado

Aceptar

Figura 29 Mensaje indicador de terminación de tiempo para resolver examen.



ANGELICA CERVANTES AVALOS, tu examen ha sido guardado con éxito
EXAMEN REALIZADO: Capítulo 1
DESCRIPCION: Conceptos básicos
CALIFICACION: 8

Figura 30 Página que muestra la calificación obtenida.

En caso de que el examen se concluya dentro de los 30 minutos establecidos, se podrá dar clic en el botón calificar para obtener la calificación obtenida (figura 31):

12. ¿Cuál de las siguientes opciones es una desventaja de la topología en anillo?

- Si el hub se cae, la red no tiene comunicación
- Las computadoras no regeneran la señal
- Si falla el canal entre dos nodos, toda la red se interrumpe
- Debido a sus rutas redundantes requiere una gran cantidad de cable

13. ¿Qué método de transmisión de señal utilizan las ondas de radio para transportar señales?

- Eléctrico
- Óptico
- Inalámbrico
- Acústico

14. Se trata de la topología de red que presenta distintas trayectorias alternativas en caso de que un nodo se encuentre averiado u ocupado

- Anillo
- Estrella
- Árbol
- Malla

15. ¿Qué categoría de UTP transmite datos de hasta 1 Gbps a una frecuencia superior a 250 MHz?

- Categoría 6
- Categoría 5e
- Categoría 5
- Categoría 4

Figura 31 Calificar examen.

Seguido de esta acción se mostrará una pantalla como la que se muestra en la figura 30 indicando cual fue la calificación obtenida.

Sí se intenta volver a realizar el examen el sistema enviará un mensaje donde indica que este ya ha sido resuelto, como se muestra en la figura 32:



Figura 32 Mensaje indicador de que el examen ya ha sido resuelto.

Finalmente, si el administrador no habilitó ningún examen se mostrará un mensaje de que no hay ningún examen disponible para ser resuelto, como se muestra en la figura 33:

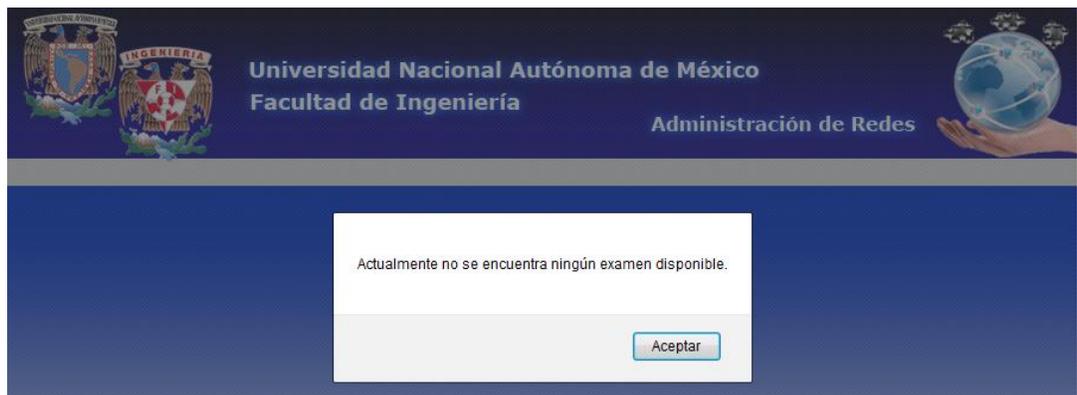


Figura 33 Mensaje indicador de que no hay exámenes habilitados.

3. Profesores

Para realizar las siguientes tareas será necesario entrar al sitio web e iniciar sesión como profesor, como se muestra en la figura 34.



Inicio de Sesión de Profesor

Figura 34 Inicio de sesión de profesor.

Una vez que inició sesión como profesor se mostrará una pantalla como la que se observa en la figura 35:



Bienvenid@: **cintia**

En esta sección se podrán visualizar las listas de los grupos impartidos, así como las calificaciones de los cuestionarios realizados por cada alumno. Dichas calificaciones las podrá tomar o no en cuenta para la evaluación de los alumnos de acuerdo a su criterio.

* Para que pueda hacer uso de esta herramienta será necesario pedir a sus alumnos que se registren en el sistema, así como indicarles la fecha en la que estará activo cada cuestionario.



Figura 35 Sesión de profesor.

En la barra del menú deberá seleccionar la opción de listas, la cual lo llevará a la siguiente pantalla (figura 36):

Grupo	Hora de inicio	Hora de término	Consultar
1	11:30 am	1:00 pm	Consultar

Figura 36 Listas de grupos asignados.

En este caso sólo se tiene asignado el grupo 1 y para ver la lista de alumnos se da clic en el botón de consultar, lo cual desplegará la lista de alumnos que se tienen registrados en dicho grupo, así como las calificación de cada examen que haya sido resuelto y el promedio de los seis exámenes. (Ver figura 37)

Grupo: 1										
Cuenta	Nombre	A. Paterno	A. Materno	Exm. 1	Exm. 2	Exm. 3	Exm. 4	Exm. 5	Exm. 6	Prom.
1234	D	J	K	2.67	0.00	0.00	0.00	0.00	0.00	0.45
304044348	ANGELICA	CERVANTES	AVALOS	8.00	0.00	0.00	0.00	0.00	0.00	1.33

Figura 37 Lista de calificaciones por alumno.