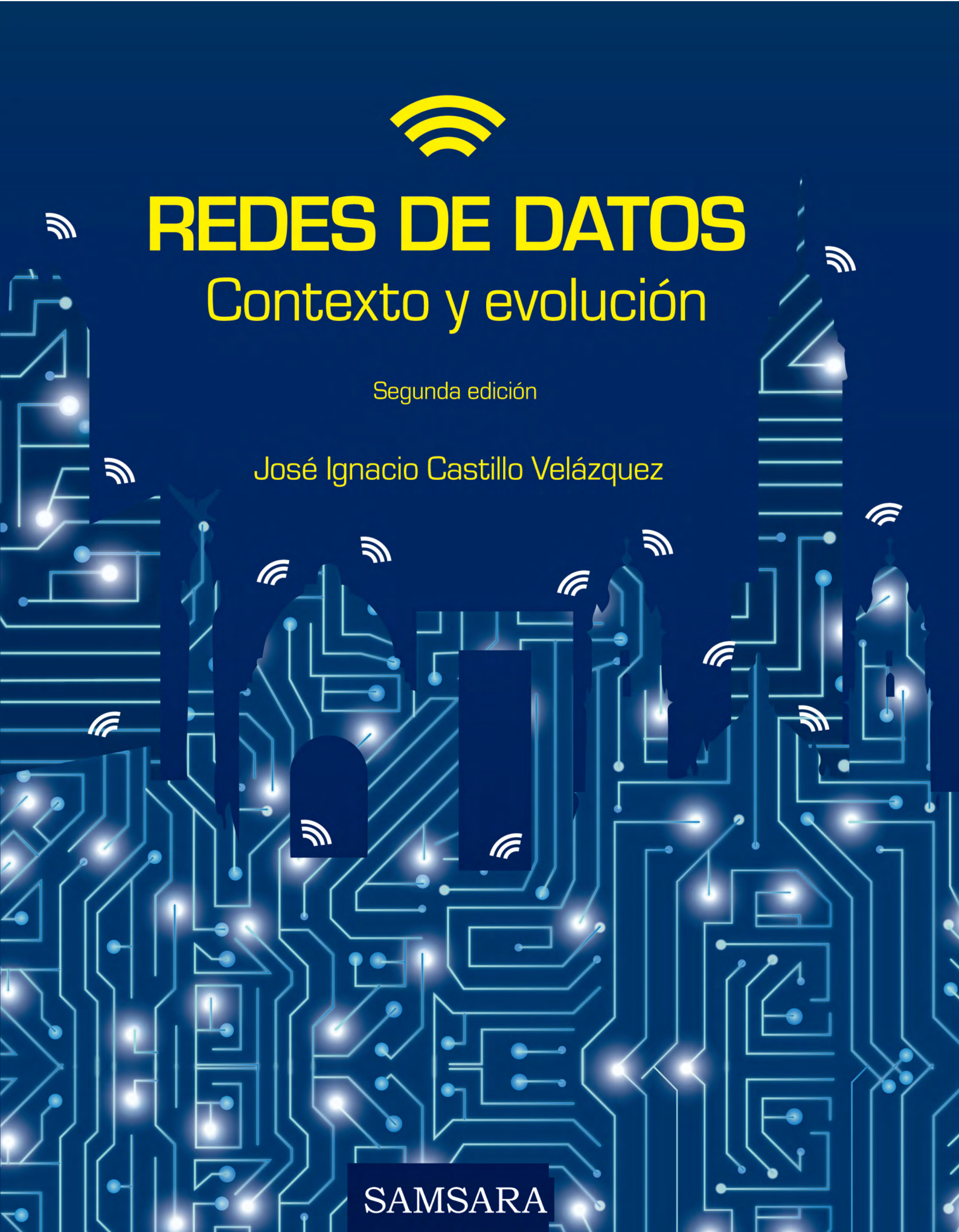
REDES DE DATOS

Contexto y evolución

Segunda edición

José Ignacio Castillo Velázquez



SAMSARA

Redes de datos: Contexto y evolución

Segunda Edición

José Ignacio Castillo Velázquez

Colegio de Ciencia y Tecnología

Universidad Autónoma de la Ciudad de México

SAMSARA
2016

Redes de datos:

Contexto y evolución

José Ignacio Castillo Velázquez

Segunda edición, enero de 2016

Primera edición septiembre de 2014. ISBN 978-970-94-2915-2

Registro INDAUTOR: 03-2016-012012315800-01

Editor: Sergio A. Santiago Madariaga

maquinahamlet@gmail.com

Diseño de portada: Iziar Nancy Eudave Salazar

ISBN 978-970-94-2968-8

Impreso en México

José Ignacio Castillo Velázquez. (2016). Redes de datos: Contexto y evolución. Ciudad de México: Samsara Editorial. 196 pp., 21 x 27 cms.

A Citlalli, mi dulce carabio

Contenido

PREFACIO

Para muchos, el origen y evolución de las tecnologías de la información y la comunicación (TIC) no son muy claros aunque su uso este muy difundido. Hoy existe una fuerte tendencia a conectarlo todo a internet, lo que conocemos como el Internet de las cosas (*Internet of Things* - IoT); incluyendo a las redes de energía eléctrica inteligentes (*Smart Grids*) y ciudades enteras, las ciudades inteligentes (*Smart Cities*). Toda la información generada constituye el gran cúmulo de datos *(Big Data*), la cual requerirá ser analizada (*Data Analytics*) para que la gente pueda tomar decisiones y esta sea útil en realidad. Después de los mainframes, llegó la arquitectura cliente servidor, de allí la virtualización para dar paso a la computación en la nube (*Cloud Computing*), la cual se soporta mediante los Centros de Datos (*Data Centers*); sin embargo, el gran riesgo en el espacio cibernético (Cyber Space) es la seguridad cibernética (Cyber Security). Todas estas tendencias tecnologías que han encontrado su desarrollo en este siglo, están gestando una cuarta revolución industrial, al combinar todas las áreas del conocimiento humano fusionándolas con las TIC de una manera totalmente multidisciplinar, relacionando datos para generar información e información para generar conocimiento y conocimiento para generar sabiduría. En todo caso, el patrón de evolución que siguen las tecnologías es similar, por lo que, los avances en los casi 186 años de las telecomunicaciones y 76 años de la computación digital nos permiten con base en lo que hoy se está gestando bosquejar aquello que madurará durante los próximos 10 años. Desde que la información se genera en un área de conocimiento y se hace útil en una determinada comunidad o país, hasta que llega a otra comunidad o país, puede pasar mucho tiempo, incluso dentro de una misma ciudad o país; ello sucedió durante la primera revolución industrial, la cual nació en el Reino Unido pero llegó al resto de Europa y los EEUU décadas después, y ni hablar de América Latina y África. Lo mismo sucedió con la segunda revolución industrial pero la adopción tecnológica duró periodos más cortos entre regiones geográficas, la tercera revolución, aquella de las TIC permite una tremenda reducción de tiempo de adopción entre que se generan, producen y distribuyen productos tecnológicos dentro del actual entorno globalizado. De modo que, ¿cómo podemos entender mejor esta vorágine en las TIC? Aquí es donde la contextualización puede ser útil en el aprendizaje relacionado con las TIC, ya que estas fundamentan su operación en las redes de computadoras.

Audiencia y enfoque del autor

Esta obra está dirigida a quienes desean introducirse en los principios de las comunicaciones de datos que dan forma a las actuales redes de computadoras. El valor de las referencias de corte académico es indudable, pero el corte de la experiencia agrega otro valor al texto, por ello, para que el lector tenga una idea mucho más amplia respecto de nuestra realidad en tecnología incluyo secciones que hacen referencia al estado que cada tecnología guardaba o guarda en México y, en algunos casos, en países de Latinoamérica. Adicionalmente la experiencia en la academia, industria y gobierno, así como en comités técnicos de organizaciones de estandarización, sin fines de lucro, como IEEE e ISO permite al autor abordar el texto con un enfoque amplio que combina teoría y práctica. El texto maneja en español los nombres de tecnologías, estándares y acrónimos asociados y siempre que es posible se incluye, en paréntesis, su nombre en inglés por ser el idioma estándar en el que se genera la literatura para la tecnología en esta época. Esta obra puede ser de utilidad para un público amplio al que recomendaría los capítulos I, II, III y VI. Sin embargo, para estudiantes de nivel universitario puede cubrirse en un curso introductorio de redes de datos, previo a tomar "switching and routing". También puede ser de consulta para técnicos y profesionales.

Organización del libro – Segunda edición

El libro se divide en tres partes: La primera parte "Las redes de telecomunicaciones antes de las redes de datos", abarcan los primeros 100 años de las telecomunicaciones y el nacimiento de las computadoras comerciales; integra a los capítulos I y II, mismos que permiten contextualizar a las redes de datos, establecer un marco de referencia común, un vocabulario para el resto de los capítulos, así como homogenizar conocimientos básicos para los lectores, fundamentalmente estudiantes de ciencia y tecnología. En el capítulo I "Las redes de telegrafía y telefonía", se hace una breve revisión acerca de las redes de telecomunicaciones previas a las redes de datos, introducidos en la medida de lo posible de manera cronológica; para lo cual se abordan brevemente las redes de telegrafía y telefonía antes de las redes de computadoras, se aborda el entorno global y el caso de México en términos históricos y se revisan datos recientes. En el capítulo II "Las computadoras antes de las redes de datos", se abordan las computadoras antes de las redes de computadoras; permite contextualizar a las actuales redes de datos al revisar a las computadoras desde aproximadamente 1940, cuando nacen las computadoras practicas hasta aquellas que se empleaban cuando se liberó internet comercial en 1995, el cual marcó la explosión de las redes de computadoras. Se incluye también una vista de lo que ocurrió en México y algunos países latinoamericanos en términos del desarrollo de la computación.

La segunda parte "Las redes de datos y sus estandarización", se conforma por los capítulos III, IV y V, los cuales son el corazón del texto. En el capítulo III "El nacimiento de las redes de datos", se hace una revisión global a las redes de datos, abarcando desde su nacimiento en la década de los años 1960, su evolución cronológica, hasta el nacimiento de internet comercial, en 1995, enmarcada dentro de una clasificación de las redes de datos propuesta por el autor. El capítulo IV "La estandarización en redes de datos" aborda el proceso evolutivo que permitió la interoperabilidad entre equipos de redes de distintos fabricantes, para lo cual se revisan Ethernet, el modelo ISO/OSI mapeando a IEEE 802.3 y TCP/IP; este capítulo incluye 4 prácticas de laboratorio apoyadas en el uso de un simulador con la finalidad de clarificar de la mejor manera posible los conceptos presentados. En el capítulo V "La arquitectura "cliente-servidor", se incluyen 4 prácticas de laboratorio, apoyadas en simulador, para permitir al lector obtener un conocimiento global de la conectividad, instalación y gestión básica de servidores vía CLI y GUI, en las que se aplican varios protocolos asociados a TCP/IP (mapeados desde ISO/OSI) sobre el cual se fundamenta la operación de internet.

La tercera parte, "La cuarta revolución industrial", la conforman el capítulo VI y VII. En el capítulo VI "TICS en el siglo XXI", se hace una revisión general de las tecnologías que están en pleno auge desarrollándose para gestar la próxima revolución industrial, se abordan brevemente las citadas *cloud computing, internet de las cosas, data centers, smartcities, smartgrid y cibersecurity*. Finalmente el capítulo VII "Contexto social y su impacto en las TICS", añade el contexto global de en qué momento histórico nacen las redes de datos y las TICS en general y algunas tendencias globales en las que nos encontramos para poder entender mejor el estado presente y futuro de las TICS sin olvidar, que uno de los factores más importantes para su desarrollo son las implicaciones sociales de la tecnología. Sin duda el mayor reto para cualquier texto en la actualidad relacionado con tecnología es que cuente con información actualizada dada la vorágine de los cambios y este texto es un fuerte intento por equilibrar las bases con lo moderno.

Notas en referencias y errores

A pesar de los esfuerzos de los revisores y editor, podrían encontrarse errores y es deseable corregirlos. Por tanto si el lector cree que ha encontrado un error, ya sea de referencia, de hechos o tipográfico, por favor contáctenos en *icastillo@computer.org*. Si se acepta su contribución, esta será mencionada en las futuras ediciones.

Diferencias entre la primera y segunda edición

La primera edición de 2014 cuenta con 5 capítulos; la segunda edición de 2016, con base en observaciones y sugerencias de los lectores estudiantes, profesores y profesionales, cuenta con 7 capítulos y las siguientes mejoras. El capítulo I de la primera edición, se dividió en lo que ahora son los capítulos I y II para hacer más claro el material presentado. También se dividió el libro en 3 partes para presentar una mejor estructura y se presentan introducciones a los capítulos clarificando el alcance de cada uno de ellos. También se mejoraron los gráficos existentes y se agregaron otros para hacer más didácticos y explícitos los temas. Se realizaron correcciones a errores encontrados, se reubicó y actualizó el contenido y se actualizaron las referencias, muchas de ellas se dirigen hacia fuentes originales. Además se incluyeron autoevaluaciones en cada capítulo. IEEE Computer Society permitió el uso de logos de proyectos de IEEE para hacer más atractivo el capítulo VI relacionado con "cloud computing", "cyber security", "big data" e "internet of things". La primera edición contó con 138 páginas y pese a que se buscó no hacer la segunda edición más voluminosa, esta cuenta con 196 páginas, pero permite seguir siendo digerible para un curso de 4 meses.

El autor

José Ignacio Castillo Velázquez Cuenta con 20 años de experiencia en TICs, tanto en empresas (Datacenter Dynamics, RedUno-Telmex, CEDAT-IFE y DICINET), como en universidades públicas y privadas (UACM, BUAP, UPAEP, UTM). Ha participado en más de 40 proyectos nacionales e internacionales como líder o miembro en las áreas técnicas y de gestión.

Como académico ha impartido más de 100 cursos de licenciatura y posgrado. Es árbitro en revistas (IEEE-LA Transactions, Springer-Health and Technology) y congresos nacionales e internacionales (IEEE II&TT, LASCCDCN, ICEDEG, COLCOM & ROPEC). Cuenta con más de 20 publicaciones en revistas y congresos; 2 reportes técnicos y un libro. Ha impartido más de 60 conferencias magistrales en congresos nacionales e internacionales. Desde 2008 es profesor de ingeniería en electrónica y telecomunicaciones en la Universidad Autónoma de la Ciudad de México. En 2015 fue profesor visitante en la Universidad de la Defensa y Fuerza Aérea de México (UDEFA).

Como profesional y consultor ha escrito 12 reportes técnicos en telecomunicaciones y colabora como consultor para Datacenter Dynamics. Es miembro de ICREA.

En IEEE es *Senior Member y* conferencista distinguido del programa "Distinguished Visitor Program" de IEEE Computer Society para el periodo 2015-2017. También es miembro de los comités técnicos de redes IEEE LAN/MAN y *cloud computing*. Fue miembro del consejo de administración de IEEE *Computer Society de 2011-2014*, donde Presidió del comité de auditoría; Recibió el reconocimiento *IEEE Computer Society Golden Core Member en 2011*. En IEEE Latinoamérica ocupó los cargos de Secretario Regional 2012-2013, Editor en Jefe de NoticIEEEro 2008-2011, Presidente del comité de comunidades virtuales 2007-2010 y miembro del comité de planeación estratégica 2009-2013.

J. I. Castillo obtuvo los grados de Licenciado en Ciencias de la Electrónica con mención honorífica por la Facultad de Ciencias de la Electrónica, y la Maestría en Ciencias en Dispositivos Electrónicos en el Centro de Investigación en Dispositivos Semiconductores, ambos por la Benemérita Universidad Autónoma de Puebla, México.

JICV

Bienvenidos comentarios y sugerencias a ignacio.castillo@uacm.edu.mx
Para mayor información consultar www.ignaciocastillo.org

Agradecimientos

Agradezco a la Universidad Autónoma de la Ciudad de México (UACM) por su gran apoyo para esta segunda edición, a *IEEE Computer Society* vía su Directora Ejecutiva Angela R. Burgess y su Director de Productos y Servicios Evan M. Butterfield en EEUU por permitirme usar los logos de las iniciativas en las que participa tal institución. Y por la lectura del texto, sus comentarios y observaciones a: Eduardo Rocha de *International Computer Room Experts Association* (ICREA), personal militar de la Universidad Del Ejercito y Fuerza Aérea (UDEFA) de la Secretaría de la Defensa Nacional (SEDENA), México. Y en especial a mi familia por su gran en invaluable apoyo. Finalmente gracias a mis estudiantes, asistentes a mis conferencias y amigos a quien se destina esta obra.

PARTE I: LAS REDES DE TELECOMUNICACIONES ANTES DE LAS REDES DE DATOS

Para el mundo de hoy, las redes de computadoras quedan inscritas en internet, es por ello fundamental dar un vistazo a su origen. Se revisan los primeros 100 años de las telecomunicaciones (1840-1940), así como desde el nacimiento de las computadoras comerciales y su evolución hasta el nacimiento de internet comercial (1940-1995).

CAPÍTULO I: LAS REDES DE TELEGRAFÍA Y TELEFONÍA

La red telegráfica de los EEUU fue una infraestructura estratégico-táctica que permitió a A. Lincoln ganar la guerra civil (1861-1865). Mientras que la red telegráfica de México en 1862 que sólo cubría la ruta Puerto de Veracruz, Puebla y Ciudad de México fue clave para la defensa y triunfo en la Batalla del 5 de Mayo.

En todo campo del conocimiento un paradigma se presenta como un continuo, pero en un ciclo; un paradigma entra en crisis, cuando deja de explicar fenómenos que siempre existieron pero sobre los cuales la humanidad en su proceso evolutivo apenas se estaba cuestionando. Para el paradigma mecanicista la crisis llegó aproximadamente a 200 años de su nacimiento (décadas 1690 Newton – 1890 Maxwell), pero también trajo su solución, el paradigma sistémico [física-relatividad (1905), ciencias de la vida-ADN (1928), etc.], de modo que el paradigma anterior sigue funcionando pero como un caso particular. Lo mismo sucede en todos los campos del conocimiento y dentro de estos periodos hay otros periodos de crisis que permiten ir avanzando.

Este capítulo permite al lector contextualizar a las actuales redes de datos tocando las telecomunicaciones en su primera centuria, desde aproximadamente 1840, el nacimiento del telégrafo comercial, hasta 1940 el nacimiento de la computadora digital comercial, considerando prácticamente al telégrafo y al teléfono alámbrico, e incluye una vista de lo que en la época ocurrió en México, país que lideraba en telecomunicaciones en América Latina en el periodo indicado.

I. Las telecomunicaciones antes de las redes de datos

Hablar de la tecnología es hablar de la propia humanidad, los avances tecnológicos de alrededor de 1750 permitieron acuñar el término primera revolución industrial y casi 100 años después apareció la segunda revolución industrial, alrededor de 1850. Durante el siglo XIX el modelo nación-estado se fundamentaba en acumular capital con base en la renta de la tierra, la agricultura, ganadería, minería y la industria petrolera; pero apareció la renta tecnológica y fue creciendo gradualmente. Para el siglo XX el mundo ya dejaba ver sus características globales, sus conexiones e interdependencias, lo cual quedó muy claro con la primera guerra mundial y con la crisis de la década de los 20, lo cual trajo la segunda guerra mundial como una prolongación de tal crisis. Ya para la segunda mitad del siglo XX el modelo nación-estado más avanzado, mostró un determinado equilibrio entre acumular capital con base en la renta de la tierra y en la renta tecnológica. Ya para finales del siglo XX y lo que va del XXI, sin duda el modelo "estado-nación más avanzado" muestra una transición hacia un modelo "estado transnacional", el cual acumula capital principalmente de la renta tecnológica, prácticamente sin importar la ubicación geográfica.

En 1904 nació la electrónica, término que se acuñó alrededor de 1930, pero es hasta la segunda guerra mundial que se gestan los grandes desarrollos tecnológicos a partir de la

electrónica, como la aparición de las computadoras digitales en 1941 y las bases de la telefonía móvil, las cuales se hicieron comerciales casi 10 años y 30 años después respectivamente.

En la década de los años 1950 maduraron las tecnologías que a la postre llevaron al nacimiento de la tercera revolución industrial, la cual podemos colocar en la década de 1980 con el desarrollo de las computadoras personales y la progresiva miniaturización y las redes de computadoras. A principios de 1990 la virtualización de los servidores era una realidad y con la llegada de la Internet comercial en 1995, se dejó de ver a las computadoras y a las telecomunicaciones como entes separados. A tal grado que el término "tecnologías de la información y la comunicación" (TIC) se hizo popular para describir toda tarea y área de estudio relacionada con la electrónica y computación.

Antes de abordar las redes de datos, es decir, las redes que interconectan computadoras, es necesario mostrar el contexto en el que se gestan estas redes, para ello se hace una breve revisión a las redes de telecomunicaciones previas a las redes de datos, es decir, las redes telegráficas y telefónicas, así como a la evolución de las computadoras. Con la finalidad de contextualizar los avances tecnológicos en telecomunicaciones de finales del siglo XIX, todo el siglo XX e inicios del siglo XXI, la figura I.1 muestra el comportamiento aproximado de la difusión mundial de las principales tecnologías relacionadas con la electricidad y la electrónica desde aproximadamente 1890 hasta el año 2010 [1].

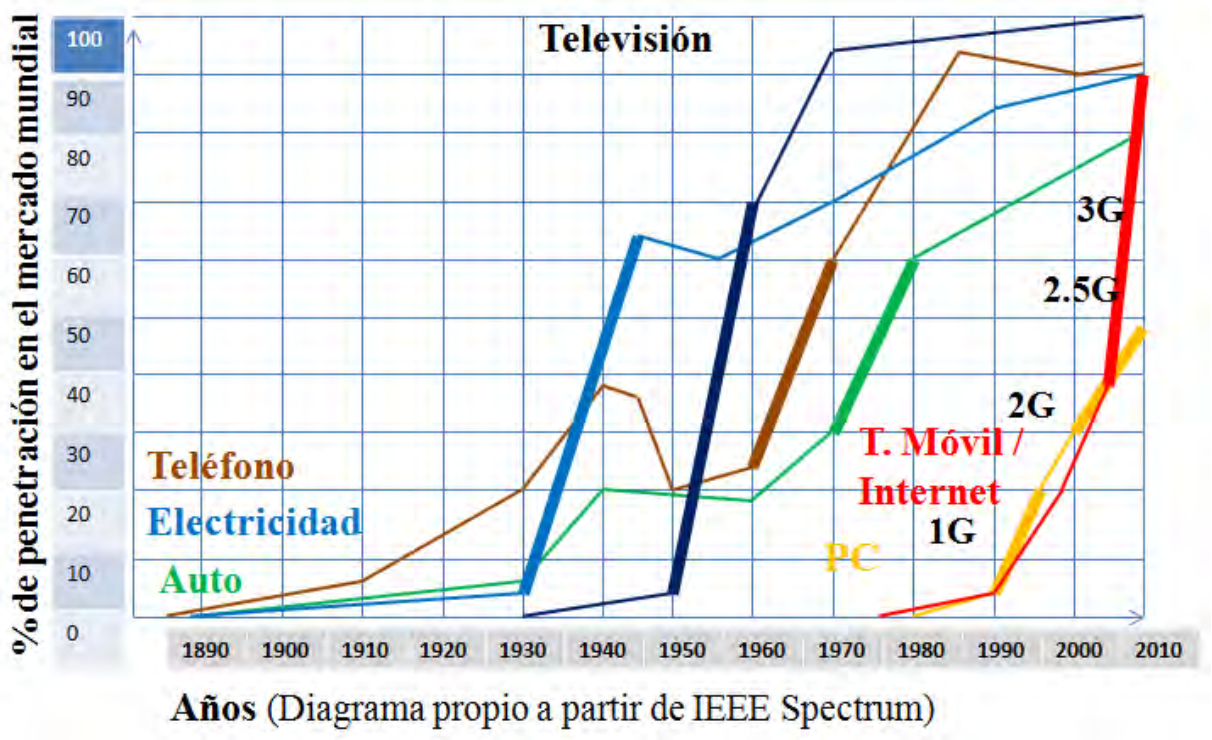


Fig. I.1. Difusión de las diferentes tecnologías en un periodo aproximado de 120 años.

En la gráfica observamos que durante la segunda guerra mundial se desaceleró la penetración de autos, la electricidad y el teléfono. La penetración de televisión fue mayor a la de la red eléctrica por los medios de energía portátiles y autogeneración eléctrica en lugares apartados de los centros de distribución. Incluso la televisión llegó a tener la mayor velocidad de penetración en la historia hasta antes de que se acelerara la penetración de la telefonía celular en los últimos 4 años. El gráfico para la radio es casi el mismo que para la televisión pero corrido aproximadamente 10 años antes, lo omito para no sobrecargar la gráfica. Desde 2010 la telefonía celular tuvo un crecimiento y para 2015 ya se habla de una penetración de aproximadamente el 99%. Cabe mencionar que otras áreas industriales, científicas y tecnológicas siguieron patrones similares a los mostrados en la figura.

En 2013 la Unión Internacional de Telecomunicaciones (UIT) estimó que cerca de 2.5 mil millones de personas en el mundo usaban internet vía banda ancha, el 25% de ellos pertenecen a países en vías de desarrollo, en contraste, en EEUU sólo el 6% de su población no accede a internet vía banda ancha. Por su parte la telefonía móvil es la más democrática, casi cada uno de los más de 7,000 millones de habitantes del planeta cuentan con uno, aunque claro está, no todos cuentan con las mismas funcionalidades y calidad de servicio; mientras que en términos de cantidad de información compartida, se estima que para finales de 2015 se comparten en internet cerca de 8 Zettabytes.

I.1 La primera red de telecomunicaciones: La telegrafía eléctrica

Si damos un paseo por la historia de la electricidad, iniciaríamos con los griegos hace más de 2,600 años, recordaríamos a Benjamin Franklin (1752), Alessandro Volta (1800), Michael Faraday (1791), etc. El gran salto se da con James Maxwell, quien agrupó a la electricidad y el magnetismo en la teoría electromagnética al reducir todo el conocimiento en electricidad y magnetismo en 20 ecuaciones diferenciales con 20 variables (On physical lines of force, 1861), expresadas para describir el comportamiento del campo potencial electromagnético modificando el concepto de líneas de fuerza de Faraday [2-4]. En 1881 Oliver Heaviside reemplazó el campo potencial electromagnético de Maxwell por "campos de fuerza" como la pieza central de la teoría electromagnética y redujo la complejidad de la teoría de Maxwell a cuatro ecuaciones diferenciales, conocidas como las ecuaciones de Maxwell. Las aplicaciones de la electricidad y magnetismo fueron un importantísimo motor para el desarrollo de la primera revolución industrial (1750-1850), al final de este periodo, la telegrafía se convirtió en la primera tecnología de telecomunicaciones, la cual tuvo un tremendo impacto económico, social y militar.

En 1832 Samuel Morse inventó el telégrafo eléctrico, y Gauss y Weber lo aplicaron tecnológicamente en 1833; pero el telégrafo eléctrico se convirtió en la primera tecnología de telecomunicaciones comercial en 1844, cuando se crea la primera red telegráfica de 64 Km en EEUU. Para 1846 se fundó la *Electric Telegraph Company*, la primera empresa de telecomunicaciones en el Reino Unido (RU) [5]. En 1851 se fundó *Western Union Telegraph Company,* en los EEUU, la cual inauguró los telegramas comerciales; ese año EEUU ya contaba con una red telegráfica de 32,000 Km, la cual interconectaba todo aquel país. Justo el 17 de mayo de 1865 se creó la ITU (International Telegraphic Union) y es durante la segunda mitad del siglo XIX cuando las telecomunicaciones se conciben como la comunicación a distancia mediante la propagación de ondas electromagnéticas (OEM). Hoy cada 17 de mayo, se celebra el día de las telecomunicaciones, el día de Internet, también el día de la sociedad de la información y el conocimiento. Entre 1844 y 1880, la telegrafía era la tecnología del momento, incluso Tomas A. Edison (1847-1931), quien contribuyó con las redes telegráficas, eléctricas y telefónicas, se hizo telegrafista en Boston en 1868, después trabajó para *Western Union*, la empresa de telegrafía más importante de EEUU en aquella época. Una vez que Europa se conectó con EEUU y Canadá se hicieron comunes los telegramas y los giros que dinamizaron la economía y el comercio vía las transferencias bancarias.

I.1.1 La telegrafía en México

México, después de independizarse de España, enfrentó una guerra contra EEUU entre 1846 y 1848, la cual dejó varios aprendizajes y es que la tecnología militar, las patentes y el entrenamiento fueron determinantes en aquella guerra; después de la cual habría que prepararse para futuras posibles invasiones. En 1849 Juan de la Granja, español radicado en México, cónsul general de México en EEUU y propietario minero, obtuvo la concesión para introducir desde EEUU el telégrafo en México.

En 1851 se inauguró la primera red de telégrafo de 180 Km entre la Ciudad de México y Nopalucan de la Granja en el Estado de Puebla, lugar donde se encuentra el Museo Nacional de Telecomunicaciones. En 1852 se terminó la red Ciudad de México-Puebla-Orizaba-Córdoba-Veracruz, una red de alrededor de 500 Km. Como toda tecnología disruptiva, es decir, aquella que provoca rápidamente un nuevo mercado al agregar valor, la telegrafía fue una tecnología de suma importancia durante las guerras, siendo esta una ventaja estratégico-táctica, por ejemplo, durante la guerra civil de EEUU entre 1861 y 1865, la cual dio ventajas al ejército de A. Lincoln.

En México la inversión en telecomunicaciones dio frutos durante la intervención francesa en México en 1862, ya que permitió tener comunicación entre Veracruz y la Ciudad de México, para que México preparara una defensa digna en Puebla; como se indica en el famoso mensaje: “Las armas nacionales se han cubierto de gloria” que el General Ignacio Zaragoza envió al entonces Presidente Benito Juárez vía telégrafo el 5 de mayo de 1862. Una vez terminado el segundo imperio mexicano en 1867, Juárez planeó la expansión de la red telegráfica hacia todo el país, pero al no haber dinero, se hizo efectiva en el periodo de Porfirio Díaz, con la participación de la iniciativa privada [6].

En 1881 la Ciudad de México ya contaba con un modesto servicio de alumbrado público y en 1885 México ya contaba con aproximadamente 15,570 Km de línea telegráfica. A modo de comparación, cabe resaltar que a México le llevó 30 años para contar con el 50% de la red telegráfica con la que contaba EEUU y la cual le llevó 7 años levantar. En 1910 México contaba con 15 estaciones de radiotelegrafía y para 1930 ya se comunicaba a la Ciudad de México con Madrid, España. Uno de los factores principales para la comercialización del telégrafo y otras tecnologías disponibles en la época, fue la demografía y él poder adquisitivo de la población, lo que indicó el mercado potencial. Se estima que en 1750 la población mundial era de 800 millones y para 1900 esta era de 1,650 millones. Alrededor de 1847 la población de México era de 6 millones y EEUU de

13 millones de habitantes aproximadamente; ya para 1900 México contaba con 13.5 millones, los estados de Guanajuato, Jalisco, Puebla y Veracruz estaban más poblados que el Distrito Federal; esta información nos da una idea del mercado potencial de la época en México [6,7]. Si ud. tiene la oportunidad le recomiendo visitar el museo de telecomunicaciones que se encuentra dentro del MUNAL, en el centro histórico de la Ciudad de México.

I.2 La segunda red de telecomunicaciones: La telefonía

En plena transición entre la primera y segunda revolución industrial, alrededor de 1850, el Reino Unido dejaría de ser la potencia hegemónica y surgiría como potencia EEUU. Durante la segunda revolución industrial la telefonía se convirtió en la segunda tecnología de las telecomunicaciones comercial. En 1876 Alexander Graham Bell patentó el teléfono eléctrico y ese mismo año se tendieron las primeras redes telefónicas con una distancia de 2 millas. En 1914 Alexandre Graham Bell recibió la *AIEE Edison Medal* por sus contribuciones a la telefonía [8, 9]. Para 1876 Edison diseñó y patentó un nuevo tipo de transmisor telefónico, mejorando el transmisor telefónico de Graham Bell. En 1879 Edison desarrolló el foco y para 1881 la planta eléctrica de su compañía ya tenía una red de energía eléctrica de más de 500 clientes, para los que proveía energía para iluminar más de 10,000 lámparas [10, 11]. También en 1881 Graham Bell inventó el par trenzado, el antecesor del cable UTP (*Unshielded Twisted Pair*) empleado actualmente en redes de computadoras. Para 1900 la red telefónica de EEUU ya contaba en todas sus líneas con par trenzado [12, 13].

La experiencia y la búsqueda de una solución a los problemas técnicos que se presentaban condujeron a perfeccionar el foco en 1883. En la época del auge de las redes eléctricas, telegráficas y telefónicas, Edison, Bell, Tesla y otros destacados ingenieros y científicos e inventores fundaron en 1884 el *American Institute of Electrical Engineers* (AIEE) en EEUU. Para 1904 John Fleming modificó el foco de Edison e inventó y patentó el diodo de tubo de vacío, dando las bases para el futuro nacimiento de la electrónica [14].

Es en 1906 cuando Lee de Forest inventó el tríodo (tubo de vacío controlado por rejilla), con el cual se desarrolló la radio. Con el diodo y el tríodo la tecnología eléctrica migró de los dispositivos electromagnéticos a la tecnología de tubos de vacío, razón por la que en 1946 Lee de Forest recibió la *AIEE Edison Medal*, por las profundas consecuencias técnicas y sociales que ha tenido el tríodo [15].

Dado el auge de las telecomunicaciones, en 1912 se creó el *Institute of Radio Engineers* (IRE) en EEUU, el cual era un organismo profesional para telecomunicaciones inspirado en el AIEE. Después de la primera guerra mundial el auge de las telecomunicaciones y otros desarrollos con base en el tríodo hicieron que se acuñara el término “electrónica” hasta el año 1930. Por su parte el ITU se fusionó en 1932 con la *International Radiotelegraphic Union* (IRU) para formar la *International Telecommunications Union* (ITU), la cual después de la segunda guerra mundial quedó bajo el mando de la ONU [12].

Las primeras redes de conmutación telefónicas fueron fijas, posteriormente la conmutación de circuitos se hizo con la intervención humana. Después de la Segunda Guerra Mundial, las redes eléctrica y telegráfica se siguieron desarrollando, pero en especial la telefónica, de modo tal que para 1951 en EEUU ya se contaba con conmutadores telefónicos de 5 dígitos, con una capacidad de 200,000 usuarios, cuyo costo era de casi 2 millones de dólares. Las compañías pioneras en redes telefónicas llenaron sus centrales telefónicas con tales conmutadores para ampliar su red telefónica pública conmutada" (*Public Switching Telephonic Network* - PSTN), como se le conoce a la red telefónica con tecnología por conmutación de circuitos (*Circuit-Switched Telephone Network*) [16-23].

Entre 1954 y 1960 *Bell Telephone* publicó cómo se enrutaban las llamadas telefónicas en las líneas troncales, es decir, entre las centrales telefónicas de larga distancia (incluyendo el sistema de señalización multitonos o multifrecuencia) y las frecuencias empleadas para los códigos de enrutamiento de las llamadas; lo que dejó claro el funcionamiento del sistema de señalización para controlar toda conmutación telefónica.

En 1963 con la finalidad de proveer mejores servicios de larga distancia, aprovechar las líneas instaladas y dar rutas a las señales al interconectar centrales de conmutación telefónica de larga distancia, *Bell Telephone* implementó el DTMF (Dual Tone Multi Frecuency). El DTMF es la señalización para el control del enrutamiento de las llamadas telefónicas, la cual iba en el mismo canal que se usa para la señal de audio.

La tecnología recibió el nombre de *In-Band Multiple-Frecuency Signaling* (Señalización por múltiples frecuencias en la misma banda o canal). Los protocolos de señalización eran conocidos como *Common Chanel Signal* – CCS (Señalización en un canal común). Uno de los protocolos de señalización populares fue el SS5, mismo que ITU-T estandarizó. Una consecuencia de que se conociera la metodología de señalización es que se crearon muchos "blue box" para burlar el cobro de llamadas de larga distancia.

Para 1974 la telefonía sufrió cambios radicales, se comercializó el conmutador o *switch* electrónico de marcación automática para quedarse en las centrales telefónicas, haciendo que para 1978 desapareciera en Catalina Island, California, la última central con tableros de conmutación manipulada por humanos en EEUU. Durante la década de los 70, se cambiaron los conmutadores telefónicos electromecánicos por conmutadores electrónicos que se encontraban en los *Electronic Private Automatic Branch eXchange* (EPABX), conocidos después sólo como conmutadores PBX, que engloba a los PABX, la versión analógica y a los PDBX, la versión digital [24].

En 1977 el SS6 sustituyó a la SS5 para la señalización del canal de comunicación y en 1980

el protocolo de señalización telefónica SS7 (Signal System #7) sustituyó al SS6. El protocolo SS7 fue mucho más seguro y estable dentro de las redes troncales de PSTN, lo cual desalentó el uso de los *blue box*.

El estándar SS7 define procedimientos, arquitectura de red, protocolos de control y enrutamiento por medio de los cuales los elementos de la red PSTN intercambian información sobre una red digital. La estandarización mejorada surge en 1988, en la que aparece el mapeo de la SS7 (Q.700), a partir del Modelo ISO (International Organization for Standardization) –OSI (Open Systems Interconnection), desarrollado para redes de computadoras. En 1993 se actualizó la Q.700 (Introduction to CCITT Signaling System No. 7) [25].

Por otra parte la llegada de la telefonía digital se da cuando maduran los métodos de conversión analógico a digital, principalmente con PCM (Pulse Code Modulation - Modulación por pulsos codificados) la cual hizo su aparición en 1937. PCM se definió como la representación digital de una señal analógica en la cual la magnitud de la señal se *muestrea* a intervalos uniformes, después se *cuantifica* y posteriormente se *codifica* asignando a cada nivel de cuantificación un código binario distinto para que dar como una señal digital. En el caso del teléfono, cuyo ancho de banda es de aproximadamente 4Khz, la señal analógica se muestrea a 8Khz, es decir cada 125 microsegundos; de este modo si se obtienen 8,000 muestras por 8 bits cada uno obtenemos 64Kbps, lo cual corresponde a un DS0 (Digital Signal 0), es decir, el ancho de banda que contrata para una línea telefónica un abonado con su proveedor PSTN. En el caso de los enlaces E1, se tienen 32 DS0, es decir 2,048Kbps o 2.048Mbps, es decir 31 canales telefónicos más. Una vez codificada PCM se pasa por último por un proceso de compresión que sigue o la ley u o la ley A, definidos por estándares ITU. PCM se emplea también en aplicaciones de audio digital además de sistemas de telefonía digital. Finalmente cabe recordar que en 1960 se inventó el laser, en 1970 la fibra óptica y los láseres de semiconductores en la misma década, pero estas tecnologías debían madurar hasta que en 1983 se hizo comercialmente viable implementar sistemas de fibra óptica para telefonía dentro de EEUU. También cabe recordar que una es la fecha en la que emergen las estandarizaciones y otra cuando las compañías de telecomunicaciones las implementan en sus sistemas, lo cual puede llevar de unos cuantos años a décadas.

I.2.1 La telefonía en México

En 1882 se instaló la primera compañía telefónica en México con el nombre *Mexicana Nacional Bell Telephone*, luego ese mismo año cambió de nombre a *Compañía Telefónica Mexicana* (CTE) y en 1904 apareció su competidor, *Teléfonos Ericsson*. En 1905 la CTE cambió su nombre a Compañía Telefónica y Telegráfica Mexicana (CTTM). Estas y otras compañías tuvieron altibajos durante la Revolución Mexicana, y las dos guerras mundiales. Finalmente Teléfonos de México (Telmex) nació en diciembre de 1947, una década después, los equipos telefónicos se comenzaron a fabricar en México.

La modernización tecnológica de México vino acompañada de eventos que dieron las condiciones para ello, fundamentalmente las políticas que permitieron la inversión extranjera y la importación de tecnología. En México los avances tecnológicos en electricidad y electrónica fueron acompañados del desarrollo de la industria petrolera, la más importante en la historia del mismo, la cual siguió patrones similares a los de las industrias de la telegrafía y la telefonía.

Cabe resaltar que la historia comercial del petróleo en México inició en 1863, pocos años después de que hubiesen iniciado los EEUU. Sin embargo, hasta 1876 con la llegada de Porfirio Díaz se inició el primer periodo de estabilidad de México y se dio continuidad a los planes de inversión extranjera iniciados con Benito Juárez. Las inversiones y tecnología llegaron de EEUU, Gran Bretaña y Holanda, las cuales dieron buenos frutos hasta 1910 y de allí se dio un espectacular crecimiento hasta 1921, año en el que México se colocó como el 2do productor mundial de crudo y de allí con la crisis de la década de los 20, inició la caída hasta 1928, punto más bajo de los precios internacionales del petróleo y punto máximo de la crisis de EEUU que se convirtió en crisis global. La inversión extranjera y la importación de tecnología siguieron patrones similares para todas las actividades de los sectores primario y secundario de la economía. Resalto estos aspectos del petróleo ya que para 2015 nos encontramos en una crisis económica mundial arrastrada desde 2008 en EEUU, así como la que se generó en 1929 en EEUU, en la que la historia para México parece repetirse, pero ahora tenemos un mucho mayor retraso científico y tecnológico que en la década de los 20 respecto de EEUU. Finalmente la presión social bajo la demanda de los beneficios de una revolución iniciada en México en 1910 y ya finalizada para 1927 condujo a un segundo periodo de estabilidad en México hasta la década de los 30; lo que a su vez condujo a varias expropiaciones, culminando con la expropiación petrolera del 38. Las expropiaciones a su vez condujeron a un bloqueo por parte de EEUU, el cual duró poco debido a la llegada de la segunda guerra mundial en

la que se retomaron acuerdos de colaboración estratégica entre ambos países. Políticas erróneas y la inexperiencia en el manejo de la industria petrolera llevaron a México a pedir a bancos de EEUU una fuerte deuda para modernizar lo que ya era Pemex. Pemex repuntó hasta 1958, pero paradójicamente volvió a pedir un fuerte préstamo para a bancos de EEUU. Pero también fue la década en la que se empezaron a fabricar teléfonos en el país. De 1959 al 1973 vino una época de baja en la producción, exportación, refinamiento de petróleo y sus derivados, por lo que en 1965 se creó el IMP (Instituto Mexicano del Petróleo) con la finalidad de generar desarrollos tecnológicos que permitieran con tecnología mexicana dejar de importar tecnología petrolera cara proveniente del extranjero. Desgraciadamente no se vio así a las empresas eléctrica ni electrónica ni de computación y hasta nuestros días padecemos de esa falta de visión de país y de futuro. Pese a todo, pero bajo la sombra del auge económico de los EEUU, en 1970 México se convirtió en la economía número 10 del mundo, su máximo histórico y para 1974 se superaba en el ámbito de petróleo la producción productividad y rentabilidad que se llegó a tener en 1921. La industria petrolera permitió al gobierno de México hacer inversiones en telefonía. En 1972 el gobierno de México adquirió el 51% de las acciones y Telmex se convirtió en una empresa paraestatal. Después del llamado milagro mexicano, una mala administración, tecnología obsoleta y las constantes crisis energéticas de los 70 y la caída de los precios del petróleo de los 80, el crudo mexicano toco fondo en 1986 (de modo que la caída de los precios del petróleo desde 2014 a niveles alarmantes 2015, parece recordarnos lo ya vivido). Lo anterior junto con la implementación global del modelo neoliberal al que muchos le echan la culpa, pero fundamentalmente debido a una mala administración llena de corrupción y despilfarro, se llegó a la caída de la industria petrolera y del país, lo cual condujo a nuevas privatizaciones y en 1989 se creó Pemex internacional, lo que condujo a su restructuración y la implementación de modelos de terciarización o “outsoursing” [26, 27]. Como una consecuencia, en diciembre de 1990 el control de Telmex, regresó a capital privado, un consorcio de tres empresas, 2 internacionales y una nacional. En 1997 las empresas de telecomunicaciones ofrecieron el servicio de larga distancia y se permitió la entrada de los competidores AT&T y Avantel, esta última fue comprada por Axtel. Con la liberación de internet comercial en 1995 y la implementación de internet 2 en México, Telmex y Avantel fueron de los principales proveedores de este tipo de servicio. Para el año 2000 el mercado de la telefonía fija fue rebasado por los abonados a teléfonos móviles, cuyo número creció exponencialmente, por lo que la competencia en telecomunicaciones por parte de los proveedores de servicios, se movió hacia esta última tecnología pero principalmente a los servicios de internet, de modo que los proveedores de servicios telefónicos se agregaron al grupo de los proveedores de internet [6].

Año	Población en México	Líneas Telefónicas	Abonados a teléfonos celulares	Abonados a internet de banda ancha fija
1960	38,676,979	338,450	No existían	No existían
1970	52,988,138	858,796	No existían	No existían
1980	70,353,013	2,699,732	1,500	No existían
1990	86,077,004	5,354,500	63,926	No existían en México
2000	103,873,607	12,301,676	14,077,880	15,000
2010	117,886,404	19,918,643	91,383,493	11,100,883
2013	122,332,399 (50,388,831 económicamente activos)	20,590,441	105,005,729	13,626,601

Tabla I.1. En la década de 2000 se dio el cambio desde teléfonos fijos hacia los teléfonos móviles, de allí los cambios en Telmex, entre otros. El punto de gran crecimiento fue 1999. Y para internet la década de 2000. En 2013 habían 50,388,831 habitantes como población económicamente activas en México [27].

Para el año 2008 se presentó una nueva crisis económica de alcance mundial como la de 1929, cuyo impacto se sintió en México de manera relativamente gradual, pero que en 2009 hizo que el PIB cayera a -6%. En México desde 2008, se dio un fuerte estancamiento en el número las líneas de telefonía fija, de las cuales Telmex tenía aproximadamente el 90%. Por su parte, las líneas de telefonía celular mostraron un fuerte incremento, pese a la crisis, y en general las telecomunicaciones no dejaron de crecer, prácticamente como si viviéramos en otro país. En 2014 la Comisión Federal de Electricidad (CFE) contaba con aproximadamente 30,000Km de fibra óptica que le dota de una capacidad para más de 400,000 enlaces de internet, situándose como el segundo lugar en su capacidad como proveedor de internet detrás de Telmex. Mientras que en términos de telecomunicaciones México tuvo una inversión de inversión de 3,483,100 MDD entre 2005 y 2013, Brasil invirtió en el mismo periodo, 10,209,900 MDD, de acuerdo con el banco mundial [27].

I.3 Autoevaluación para el capítulo I

1. Vea detenidamente la figura 1 y a partir de ella comente a qué cree que se deba el comportamiento del centro del gráfico.
2. Indique tres periodos entre 1840 y 1940 en el que pueda clasificar el desarrollo de las telecomunicaciones en México indicando su tipo, es decir, indicando si se trata de telegrafía o de telefonía.
3. Si analizáramos con profundidad la disponibilidad tecnológica en EEUU y México entre aproximadamente 1840 y 1940 veríamos que no existieron grandes diferencias en términos de disponibilidad tecnológica al menos entre quienes podrían comprarlas. ¿A qué atribuye tal hecho?
4. ¿En qué década aparecieron los conmutadores telefónicos de tipo electrónico PBX?
5. ¿A qué conocemos como PSTN?
6. ¿Cuál es el ancho de banda empleado en telefonía de una PSTN?
7. Indique cuál es la función de ISO, con qué fin fue creado y cuándo.
8. Indique al menos un estándar empleado en telefonía y en qué consiste.
9. Desde 1937 se empleó una técnica digital en telefonía llamada PCM, ¿en qué consiste?
10. Busque información relacionada con “blue box”.
11. Revise los videos históricos de las referencias 16 a 22.
12. ¿Cómo se define a las telecomunicaciones?
13. Liste a qué eventos relacionados con la celebración del “Día de las telecomunicaciones” o “Día de internet” ha asistido o planea asistir este año. ¿Participa activamente de alguna manera?, ¿Cómo?

Comparta sus reflexiones y la información que buscó con el resto de sus colegas.

CAPÍTULO II: LAS COMPUTADORAS ANTES DE LAS REDES DE DATOS

Una computadora hará lo que le digas, pero ello puede ser muy diferente de lo que tengas en mente.

Joseph Weizenbaum (1923-2008) Alemán

Inventor del lenguaje de programación SLIP (General Electric y MIT)

Este capítulo permite al lector contextualizar a las actuales redes de datos tocando las computadoras desde aproximadamente 1940 el nacimiento práctico de la computadora, hasta el despliegue de internet comercial de 1995, que marcó la explosión de las redes de computadoras e incluye una vista de lo que en la época ocurrió en México y otros países de América Latina que habían podido reducir la brecha con México.

II. Las computadoras antes de las redes de computadoras

Una vez que la primera y segunda revolución industrial se generalizaron en Europa, y EEUU, el nuevo orden económico mostraba a un nuevo jugador, Alemania, la cual se unió al grupo de países que generaba las tecnologías que resultaron en la implementación de las computadoras. Durante la segunda guerra mundial se gestó una revolución en la electrónica y se dio una carrera entre Alemania, Inglaterra y EEUU para diseñar y construir computadoras. Es en la década de los 70 cuando las redes de computadoras y tecnologías asociadas se convierten en la tercera tecnología de telecomunicaciones, las cuales se hicieron comerciales en los años 80. A continuación presento un breve resumen de evolución de las computadoras desde la generación cero hasta la cuarta. Es importante considerar que una es la fecha en la que el fabricante anuncia su producto, pero los equipos tardaban en construirse de 12 a 18 meses, por eso existen diferencias entre varios autores a la hora de clasificar las computadoras por generaciones.

II.1 La generación cero: mecánicas y electromecánicas

Con base en las ideas de Charles Babbage para el diseño de la máquina analítica en 1837 y Pascal se dieron avances que son la base de las computadoras actuales. Durante la primera guerra mundial hubieron muchos desarrollos, pero las necesidades en diversas industrias, principalmente la aviación requirieron hacer cálculos a gran velocidad y guardarlos en una memoria; de modo que para 1936 Konrad Zuse en Alemania, construyó la primera computadora electromecánica programable, la Z1, la cual contaba con 200 relés, 6 instrucciones y funcionaba con tarjetas perforadas. En 1938 Zuse creó su mejora, la Z2, la cual contaba con 800 relés; las Z1 y Z2 fueron

destruidas en 1940, durante la segunda guerra mundial. La tabla II.1 muestra algunas características de la Z1 [28]. El poder de la Z1 es mucho mayor que aquellos circuitos que se construyen en la actualidad en muchas universidades, después de varios cursos de electrónica digital, en su lugar se compran procesadores y microprocesadores, sin embargo, se debe enfatizar la importancia de comprender la arquitectura de las computadoras.

	Característica	Conjunto de instrucciones	Ciclos de reloj
Velocidad de reloj	1 Hz	1. Suma	3
Registros	2 de 22 bits	2. Resta	4-5
Memoria	64 palabras de 22 bits	3. Multiplicación	16
Unidad aritmética	+, -, *, /	4. División	18
Operaciones con	Decimales con punto flotante	5. Lectura de memoria	1
		6. Escritura en memoria	1

Tabla II.1. Características básicas de la Z1

En 1941 Konrad Zuse construyó la **Z3,** la cual fue la primera computadora programable del mundo, una "computadora electromagnética completamente automática" y binaria, ya que usaba álgebra booleana con base en 2,400 relés telefónicos a 5Hz; se programó automáticamente con tarjetas perforadas. La Z3 fue la cristalización de los conocimientos de tres autores: *Gottfried Leibniz*, quien inventó el sistema binario en 1690 con base en aritmética china del siglo XI; *George Boole* quien en 1854 inventó la lógica booleana y *Claude Shannon* quien en 1937 inventó la teoría de la comunicación con base en el algebra booleana. La Z3 fue destruida en 1944 durante un bombardeo aliado sobre Berlín. Un diagrama de su arquitectura básica se bosqueja en la figura II.1 [28]. La Z4 se construyó entre 1941-1944, contaba con 2,200 relés y era de tarjetas perforadas.

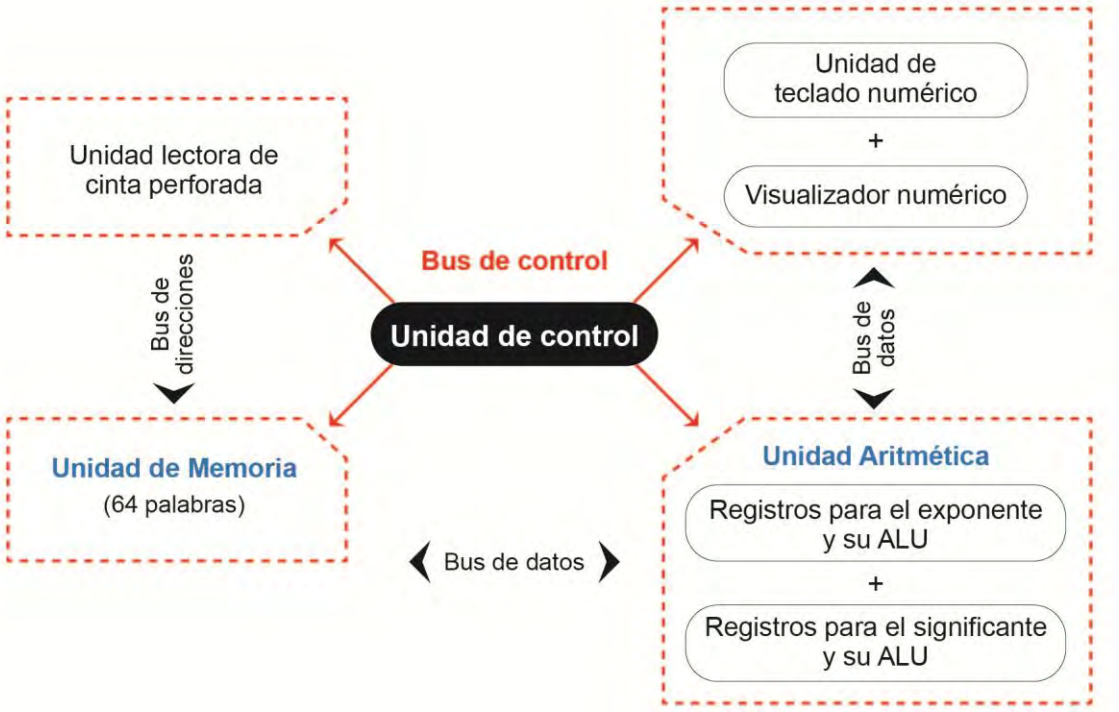


Fig. II.1. Diagrama a bloques del procesador Z3 (1941). Se incluyen los 3 tipos de bus.

.

Durante la segunda guerra mundial, el ejército alemán creó en 1939 la máquina de cifrado Lorenz SZ-40 y la SZ-42, pero los criptógrafos del ejército británico hicieron ingeniería inversa y dedujeron su funcionamiento en 1942 bajo el liderazgo de Alan Turing. Para lograrlo construyeron la *Heat Robinsons* y con base en ella Tommy Flowers en la Universidad de Londres, creó en 1943 la *Colossus Mark I*. Ésta fue la primera computadora electrónica digital programable que contaba con 1,500 bulbos, y se empleó para descifrar los códigos generados por las Lorenz; la versión II se produjo en 1944 con 2,400 bulbos.

Para 1944 se construyó la *Harvard Mark I* como un proyecto de la Universidad de Harvard y la IBM. Fue la primera computadora electromecánica de EEUU. En 1946 se construyó la ENIAC con 17,648 bulbos, 1500 relés, 6,000 interruptores, decimal y 72 toneladas, se programaba soldando cables, fue desarrollada en la Universidad de Pensilvania para el ejército de EEUU, y dejó de usarse en 1955. El mismo 1946 IBM compró las patentes de la Z3 a *Konrad Zuse*, quien creó su propia compañía en 1949, en 1950 vendió la primera computadora comercial en Suiza y su compañía fue comprada por *Siemens* en 1967. La Z3 fue reconstruida en Alemania en 1999, sin duda como parte de ese resurgimiento de orgullo alemán.

Entre 1947 y 1948 se construyó en el Reino Unido, la Manchester MARK I del tipo experimental. En este punto cabe recordar que durante 1935 y 1940 se desarrolló el radar en el Reino Unido, invento clave para detener a la Alemania nazi. Tal invento se compartió en 1940 con los EEUU para realizar desarrollos de radares hasta llegar al magnetrón, una de las tecnologías determinantes en aquella guerra, y claro luego vinieron los hornos de microondas comerciales en 1947. Pasaron muchos años para que otros países contaran con la transferencia tecnológica, este caso se repite por siempre y este patrón nos recuerda que la tecnología que podemos comprar hoy, cualquiera que ésta sea, fue desarrollada hace ya varios años [29].

II.2 La generación 1: 1950-1958, comercial con bulbos

En diciembre de 1947 John Bardeen, William Shockely y Walter Brattain inventaron el transistor (de germanio), en los laboratorios Bell (recibieron el premio Nobel de física en 1956), pero es la época en la que el transistor debió madurar, hasta llegarse a la producción masiva en 1951 [30]. En 1954 Texas Instruments produjo el primer transistor comercial de silicio, con lo que se abrieron las puertas para los circuitos con transistores y paulatinamente algunas partes de las computadoras de bulbos se fueron sustituyendo por circuitos con transistores [31]. También en 1954 se fabricaron las primeras computadoras no comerciales con transistores, IBM vendió su primera calculadora transistorizada. Mientras tanto las computadoras comerciales de la primera generación se harían solamente de bulbos o de bulbos y transistores durante casi toda la década de los años 50, ya que para 1958 se construyó la primera computadora comercial con transistores y se fabricarían incluso con tecnología híbrida hasta 1962.

Las primeras computadoras comerciales fueron las llamadas “mainframes”, cuya unidad de procesamiento central era construida con bulbos. Las mainframes eran computadoras grandes cuyo poder de computación estaba centralizado y atendía a varios usuarios que se conectaban vía terminales. La primera computadora comercial de propósito general fue la Alemana Z4 (modificada) vendida a Suiza en 1950 [28]. Evidentemente no muchos libros de historia de la computación de los EEUU hacen alusión a ella.

La segunda computadora comercial fue la Ferranti MARK I en Reino Unido, fue la 1ra computadora comercial para la Universidad de Manchester en 1951, generada a partir de la MARK I; contaba con 50 instrucciones y 4,500 bulbos [32]. También en 1951 se construyó la UNIVAC I de RAND Corp., primera computadora comercial en EEUU para la Oficina de Censos en 1951, con 5,000 bulbos, con capacidad para conectar hasta 24 unidades de entradas y salida y capacidad para manejar hasta 100,000 tarjetas perforadas; se produjeron 48 sistemas cuyo costo aproximado fue de un millón de dólares cada uno. Hasta 1951 EEUU y el Reino Unido habían producido aproximadamente 20 computadoras [33].

En 1953 se produjo la IBM 650 de primera generación, computadora de tamaño mediano; se fabricaron cerca de 2,000 sistemas y fue el modelo más popular en los años 50.

Después de las Z5 y Z11, la Zuse Z22 de 1955 fue completamente de bulbos con memoria de ferrita como RAM, tambor y tarjetas como memoria externa, a 3KHz, de 38 bits, usaba lenguaje ensamblador [28]. Por su parte las computadoras mainframes emblemáticas de IBM fueron las IBM Serie 700, desde la IBM 701 en 1952 hasta la IBM 709 en 1958, la cual realizaba 5,000 multiplicaciones o divisiones por segundo, para aplicaciones comerciales, científicas y problemas de ingeniería, para lo cual soportaba FORTRAN. La IBM 305 RAMAC, comercial desde 1956, que ya incluía disco para almacenamiento de datos para aproximadamente 5MB [34].

La Ferranti Mercury de 1956 de la compañía inglesa Ferranti, tenía 3,500 bulbos, era de punto flotante, como evolución de las anteriores MARK I y II, contaba con un arreglo de memoria de núcleo con capacidad para 1024 palabras de 10 dígitos, empleada para aplicaciones como diseño de aviones, cálculos para presas en ingeniería civil, y para meteorología y cálculo de impuestos principalmente. Las mainframes de tal generación tenían costos aproximados al millón de dólares [35]. La transición entre la primera y segunda generación de computadoras la marca la UNIVAC II en 1958, la cual contaba con 4 módulos, tenía 5,200 bulbos, 1200 transistores, costaba arriba de un millón de dólares en función de los accesorios y era compatible con la UNIVAC I. [36].

II.2.1 Las primeras mainframes en México y América Latina

En 1953 la UBA (Universidad Autónoma de Buenos Aires) en Argentina creó la licenciatura en "Computación Científica", con un corte altamente matemático y de influencia europea, se llegó a enseñar la arquitectura de la Mercury Ferranti, que les llegaría hasta 1960, pero también se analizaba la IBM1401, de segunda generación. En 1957 Colombia se convirtió en el primer país latinoamericano en contar con dos computadoras IBM 650 de primera generación, las cuales fueron adquiridas por empresas privadas; en el mismo año IBM de Venezuela adquirió una computadora del mismo modelo. En 1958 Cuba recibió la IBM RAMAC 305, de las cuales se fabricaron casi 1,000 desde 1956, pero por su revolución se instaló hasta 1962, cuando se fundaron los centros de computación y electrónica, sus posteriores adquisiciones fueron computadoras inglesas y francesas.

También en 1958, ya habiendo iniciando la época de la segunda generación de computadoras, en México, la UNAM (Universidad Nacional Autónoma de México) rentó su primera computadora, una IBM 650 de segunda mano, previamente usada en la UCLA (University of California - Los Angeles), para el CCE (Centro de Cómputo Electrónico). En 1959 Brasil se instaló una IBM RAMAC 305 para la compañía Anderson Clayton en Sao Paolo, en 1960 una IBM 650 la compró Volkswagen Brasil y el gobierno brasileño adquirió una IBM 305 RAMAC. En 1960 la UNAM compró su primera mini computadora, la Bendix G-15 computadora híbrida con casi 450 bulbos y 300 diodos de germanio. En 1961 el IPN (Instituto Politécnico Nacional) compró una IBM-709 para el Centro Nacional de Cálculo CENAC; ese mismo año la planta de IBM en Brasil inició la producción de la IBM 1401 [37, 38].

II.3 La generación 2: 1958-1965, comercial con transistores discretos.

En 1958 Jack Kilby inventó el circuito integrado (CI) en *Texas Instruments* y casi simultáneamente Robert Noyce en *Fairchild Semiconductors*, después se maduró hasta llegar al proceso planar en 1959. Posteriormente llegó la producción masiva para las SSI (*Small Scale Integration*) y MSI (*Medium Scale Integration*) y en 1960 ya se empleaba el término microelectrónica [39, 40]. En 1961 *Fairchild Semiconductor* ya usaba CIs de transistores planares para producir compuertas con lógica RTL y para 1963 publica su *Custom Microcircuit Design Handbook*, con lo que deja a cualquier fabricante listo el terreno para que sus mainframes usen CI monolíticos en sus diseños y para 1965 libera el amplificador operacional μA709. En el mismo 1963 inició la construcción de la primera computadora no comercial hecha completamente de CI, la AGC *(Apollo Guidance Computer*) para el programa espacial de EEUU [41]. Mientras tanto por un buen periodo, las computadoras comerciales de segunda generación se harían con base en circuitos con transistores discretos o con transistores y circuitos integrados SSI y MSI, estas computadoras con tecnología híbrida se fabricaron hasta 1969.

Al igual que las computadoras de primera generación, las de segunda generación, se caracterizaron por tener un equipo central conectado con una unidad lectora de tarjetas perforadas, la unidad de almacenamiento de discos, la impresora y varias terminales. Las compañías las ofrecían como sistemas completos, ya que todas las unidades indicadas eran compatibles solamente con sus mismos equipos. En Europa, en 1958, la compañía holandesa Electrológica fabricó la X1, computadora completamente transistorizada, de las cuales se vendieron 30 [42]. También en 1958 la *Stantec Zebra*, de STC Inglaterra, funcionaba con sólo tres módulos: uno para energía, otro para la computadora y almacenamiento, y un escritorio para la lectura y escritura con tarjetas [43]. Por su parte, la Zuse Z23 de 1961 fue la primera computadora transistorizada de Alemania [28].

En EEUU la primera computadora totalmente hecha con transistores fue la RCA 501 (*Electronic Data Processing System*) de 1958 [44]. Por parte de IBM, la IBM 7090 de 1959 fue la versión de transistores de la IBM 709, con 6 veces mejor rendimiento y la mitad de precio. La IBM 1401 de 1959, llamada *Data Processing System,* estaba compuesto por las IBM 729, una unidad de cintas magnéticas para almacenamiento, la IBM 1403 una impresora y la IBM 1402 una unidad lectora de tarjetas perforadas. DEC (*Digital Equipment Corporation*) vendió su primer PDP-1 en 1960, una computadora de transistores de 18 bits, que sentó las bases para las minicomputadoras,

con un precio mucho menor a las mainframes, alrededor de 120,000 dólares; se fabricaron 53 [45].

En 1962 la IBM 1440 era una computadora mainframe para contabilidad y sistemas de información financiera. Otra computadora pero para aplicaciones de computación científica de gran escala fue la IBM 7094 de 1962. La UNIVAC III también fue completamente de transistores, pero era incompatible con sus antecesores, era para aplicaciones científicas y comerciales, por ello incluía el lenguaje de programación COBOL.

Dada la amplia aceptación del término electrónica, el desarrollo de las computadoras electrónicas y las redes de comunicaciones, en 1963 el AIEE e IRE se fusionaron para formar el IEEE (Institute of Electrical and Electronic Engineers).

En 1964 se comercializó la CDC6000, la primera supercomputadora, era la más cara y rápida del mundo. En 1965 se construyó la PDP-8 de DEC, fue la primera minicomputadora (junto con la CDC160), construida con transistores; dado su éxito se produjeron casi 50,000, cada una valía cerca de 20,000 dólares. Las versiones PDP-8 de 1968 ya incluían tecnología TTL, es decir, circuitos integrados SSI.

II.3.1 Las computadoras de segunda generación en México

En el ámbito académico, en 1963 la UNAM rentó una computadora Bull Gamma 30, de segunda generación para sustituir a la Bendix. En 1965 compró una IBM-1440 para trabajos administrativos, tal computadora fue creada para pequeñas y medianas empresas; y para 1967 se sustituyeron los equipos por la mainframe IBM 360/40 de segunda generación, fabricados desde 1964 [46, 47].

II.4 La generación 3: 1965-1975, circuitos integrados SSI y MSI

En 1964 se fabricaron las compuertas TTL 7400 con grado militar y la comercialización se hizo masiva en 1966. En 1965 se produjeron las primeras memorias ROM de 256, 512 y 1024 bits; las mejoras tecnológicas en las escala SSI y MSI se dan con los contadores, registros y ALU hasta que en 1968 se alcanzó la total madurez en los CI de MSI. Posteriormente la industria mundial de CI maduró hasta que Suiza llevó los CI (MSI) a los relojes, mientras que Japón los llevó a las calculadoras en 1967 [48]. En 1969 se produjeron los CI de LSI (LSI-*Large Scale Integration*-Escala de Integración Grande), y ese mismo año Japón fabricó calculadoras con tecnología LSI [49].

Las mainframes de tercera generación, ya eran equipos más económicos que las computadoras de generaciones anteriores, tenían costos iniciales mínimos de aproximadamente 100,000 dólares por usar circuitos integrados, sin embargo, también tenían módulos de circuitos con transistores discretos.

En 1964 IBM anunció la serie de mainframes IBM 360 y su primer cliente la recibió en 1965, tal computadora tenía una arquitectura CISC diferente a sus antecesoras, ya que usaba microprogramación. IBM introdujo la tecnología SLT (*Solid Logic Technology*), una tecnología previa a la de SSI, con un CPU de 32 bits y capacidad de direccionamiento de 24 bits y 16MB para el almacenamiento. Con ella se podrían conectar hasta 44 equipos periféricos y con el sistema operativo 360 compatible para todos los equipos de la serie 360. Algunos modelos de la serie ya trabajaban como estaciones de trabajo. Aproximadamente de 1964-1971, IBM con su Serie 360 llegó a ocupar el 70% del mercado de las computadoras. Varias IBM 360 modelo 75 producidas en 1966 ya podían conformar los sistemas de control aéreo [50, 51]. En 1965 RCA anunció la serie Spectra 70 y en 1966 la Burroughs B2500/3500, todas ellas con CI monolítico.

En 1966 se produjo la mainframe SDS 940 (*Scientific Data System*, que después compraría Xerox) diseñada principalmente con circuitos integrados en UC Berkeley para SDS. Tenía una CPU de 32 bits y se le podían conectar una gran cantidad de periféricos. También se produjo la SDS Sigma 7**,** una mainframe de CI de 32 bits [52]. Ese mismo año salió la PDP-10 de DEC (*Digital Equipment Corporation*), era de transistores, diodos, compuertas básicas y FlipFlops en CI con SSI; tenía CPU de 36 bits y 18 bits para direcciones, para lo que usaba un arreglo para sus interfaces llamado *Flip Chip*. La PDP-10 contaba con una arquitectura que permitía manejar 366 instrucciones, podía usar BASIC, FORTRAN y COBOL, también usaba caracteres bajo código ASCII. Su sistema

operativo era de tiempo compartido y podía atender a un máximo de 63 usuarios. Su consola tenía pantalla con tubo de rayos catódicos y teclado modularmente integrado. Para la comunicación remota tenía una capacidad para 32 modems y contaba con interfaces seriales RS-232; sus manuales son tan extensos que se dividen en 8 tomos, cada unos de ellos muy detallados [53]. En 1968 la japonesa Fujitsu desarrolló la FACOM 230-60 con multiprocesador, para lo que usaba dos CPU de CI [54]. Las SDS sigma 7, SDS 940, IBM360/75 y PDP-10 jugaron el papel protagónico en la primera red WAN (*Wide Area Network-Red de Área Amplia*) funcional en 1969.

II.4.1 En México y América Latina

En México la computación recibió un fuerte impulso con la llegada de Harold Macintosh al CINVESTAV-IPN entre 1964-1965, DPCCE-UNAM (hoy IIMAS), entre 1965-1966, y la ESFM-IPN entre 1966-1975. Durante ese periodo la UNAM adquirió una PDP-8 y junto con el IPN siguieron actualizando sus equipos. Los primeros egresados en computación en México fueron del IPN en 1965, de la carrera de comunicaciones y electrónica [55]. En 1966 Brasil adquirió su primera computadora, una IBM 1130 [56]. Al final de la década de los 60, el ITESM (Instituto Tecnológico de Estudios Superiores de Monterrey) en Monterrey, Nuevo León, compró su primera minicomputadora: la IBM 1620 (se produjeron casi 2,000 desde 1960). Con este equipo el ITESM creó la primera licenciatura en computación del país, secundada por la UNAM y el IPN. Al principio de los años 70 la BUAP (Benemérita Universidad Autónoma de Puebla) adquirió la minicomputadora IBM-1130 de tercera generación (se produjeron casi 10,000 desde 1965). En 1973 la BUAP creó la licenciatura en Ciencias de la Computación con la asesoría de MacIntosh, quien desde 1975 labora en el Departamento de Aplicación de Microcomputadoras del Instituto de Ciencias (ICUAP) de la BUAP. En la década de los 70 eran tan pocas las computadoras en México que IPN, UNAM y BUAP compartían sus computadoras para la ejecución de programas computacionales. En esa misma década la UANL (Universidad Autónoma de Nuevo León) creó su licenciatura en computación y le siguieron varias universidades más en México [55,57]. Para 1970 se estimaba una población mundial de casi 4 mil millones y en México habían poco más de 48 millones, cuya población económicamente activa era de poco más de 12 millones; esta información nos da una idea del mercado potencial para el consumo de productos, incluyendo los tecnológicos [7].

II.5 La generación 4: Desde 1975, computadoras con LSI y VLSI

En 1970 se produjeron las primeras memorias PROM y también UNIX. Para 1971 ya se fabricaban las memorias EPROM, también se inventó el microprocesador 4004 [58]. En 1973 se inventó el lenguaje C, pero fue hasta 1975 cuando se construyó la 1ra computadora personal, empleando CI, cuyas escalas de integración fueron LSI y VLSI. En 1977 se comercializaron las microcomputadoras Apple, Commodore y TRS-80 (Tandy Radio Shack con procesador Z-80) y en algunos casos se vendieron como kits. Ese mismo año, se introdujeron las famosas minicomputadoras DEC-VAX-11, como sucesoras de las PDP-11. A continuación se abordarán algunos aspectos generales de las computadoras de cuarta generación.

II.5.1 Elementos básicos de una computadora y su secuencia de arranque

Una computadora con arquitectura Von Newman consta de:

1. Procesador de información, uno o varios CPU: *Datapath*, Unidad de control, registros.
2. Unidades de comunicaciones para la entrada y salida de información: para conectar teclado, monitor, mouse, digitalizadores, impresoras, graficadores.
3. Unidades de almacenamiento de información: Interna para conectar RAM, EEPROM, Caché, etc, o externa para conectar discos duros, compactos o cinta magnética.

Toda computadora, por poco o muy poderosa que sea, desde aquellas que se usan en robots hasta las que componen a los *switches* y *routers*, se encuentren en tierra, satélites o estaciones espaciales, todas tienen una secuencia de arranque.

La secuencia de arranque se ejemplificará con el caso del sistema operativo MSDOS [6].

Paso 1: El programa BIOS [*Basic Input Output System*], el cual se encuentra dentro de una memoria ROM, PROM, EPROM o EEPROM, realiza las pruebas POST [Power On Self Test], las cuales consisten en: Inicializar los circuitos de soporte, inicializar los dispositivos (drives, disco duro, teclado) e inicializa el vector de interrupciones y se ejecuta el **BOOTSTRAP**, proceso que consiste en hacer la lectura del primer sector de disco, el sector cero.

Paso 2: Se carga el IBMBIOS.COM o el IO.SYS para indicar los límites de memoria.

Paso 3: Se carga el IBMDOS.COM o MSDOS.SYS para definir interrupciones del DOS

Paso 4: Se carga el COMMAND.COM, el cual se instala en dos partes de la memoria:

a) La parte residente (kernel o núcleo) y b) La parte transitoria.

Paso 5: Si existen los archivos CONFIG.SYS y AUTOEXEC.BAT se ejecutan en ese orden configurando a la computadora.

Paso 6: Finalmente, aparece el *prompt, el cual* indica al usuario que la computadora se encuentra lista para recibir órdenes. El *prompt* es diferente en función del sistema operativo empleado. En las computadoras modernas, todos los pasos anteriores aparecen como una caja negra para el usuario final, el cual solamente ve interfaces gráficas de usuario (GUI- *Graphic User Interfase*) [6].

La descripción del proceso de arranque de una computadora es fundamental para entender en un futuro cómo es que arrancan todas las computadoras y equipos de telecomunicaciones como “switches y routers”, además de que permite evitar conceptos erróneos o en su caso corregirlos.

II.5.2 Memorias

Con la microelectrónica se crearon los circuitos integrados en sus distintas escalas de integración: SSI, LSI, VLSI y UVLSI, lo que facilitó el surgimiento de las memorias y las computadoras de tercera generación, apareciendo finalmente las computadoras personales. En 1970 se popularizaron las memorias ROM de 8Kb (8192 bits), las cuales eran del mismo tamaño que los registros de 8 bits, de modo que los fabricantes de mainframes y de minicomputadoras cambiaron sus memorias de núcleo magnético. Más tarde se fueron desarrollando las memorias RAM, DRAM, SRAM, SDRAM, NVRAM, ROM, PROM, EPROM, EEPROM, CDROM, DVD, DVD-R, DVD-RW, etc., así como sus tecnologías.

Cabe aclarar un concepto y corregir una concepción errónea, las memorias semiconductoras que se emplean comúnmente para conectarlas al puerto de comunicaciones USB, las llaman comúnmente “memorias USB”, en realidad son memorias *flash*; es decir, memorias EEPROM. No existen las memorias USB, ya que el puerto de comunicación de una memoria no define el tipo de tecnología a la que pertenece la misma [6].

II.5.3 Microprocesadores

Antes de 1964 la arquitectura de una computadora estaba atada a su propia implementación, sin embargo, en 1964 la IBM *System* 360 en 1964 fue el parte aguas, el principio de la arquitectura de computadoras moderna, pues ofreció un cierto nivel de compatibilidad haciendo que una serie de computadoras pudiera ejecutar las mismas instrucciones. El IBM *System* 360 distinguía la arquitectura de computadora de la implementación del hardware. Entendiendo a la arquitectura de computadora como la estructura abstracta de una computadora que debe conocerse para poder programar en lenguaje de máquina. La aparición de la microprogramación, permitió mediante el uso de microinstrucciones acelerar 10 veces los procesamientos, lo que condujo también a popularizar el diseño del conjunto de instrucciones, para la que habían dos caminos, uno es hacer instrucciones grandes que se ejecutasen en varios ciclos de reloj CISC (*Complex Instruction Set Computers*), gracias a un intérprete; o hacer instrucciones esbeltas que se ejecutaran en un menor número de ciclos de reloj sin usar interpretación RISC (*Reduced Instruction Set Computers*) [59]. En 1980 nació la arquitectura RISC, la cual permitió simplificar el hardware y hacer sinergia entre la arquitectura y los compiladores [60].

En 1970 Intel comercializó el primer procesador, el 4004 de 4 bits para datos a 740Khz con 46 instrucciones y 16 registros, en un chip de 16 terminales, con 2,300 transistores. En 1972 el procesador 8008 de 8 bits para datos a 2Mhz en un chip de 40 terminales. Conocer su arquitectura es muy importante para obtener el mejor provecho de ellos. A éstos los diferencian su número y poder de su conjunto de instrucciones y los ciclos de reloj que usan cada una de las instrucciones. También es importante conocer el ancho de banda de sus bus de datos, direcciones y control, el tamaño y línea se sus bus de datos y direcciones. La tabla II.2 muestra un resumen de procesadores para microcomputadoras populares en las décadas 70 y 80 [6, 61].

Intel (74) / Altair (75) / IBM (81)	MOS Technology / Apple (77) / Motorola (79)
➢ En 1974 el procesador 8080 de 8 bits para datos a 2Mhz, en un chip de 40 pines. ➢ **En 1975 la ALTAIR 8800 era la primera computadora personal vendida como un kit**, usaba el 8080, lenguaje ensamblador guardada en cinta de papel, empleaba interruptores y leds, usó el Bus Altair o Bus S-100, el cual fue modificado y renombrado como IEEE-696 en 1983. ➢ En 1979 el procesador 8088 de 16 bits a 10Mhz, en un chip de 40 pins, mismo que se empleó para la primera **IBM-PC en 1981, segunda computadora personal**. ➢ En 1982 se produjo el 80286 y apareció la PC-XT ➢ En 1985 el procesador 80386 de 32 bits como la tercera generación de procesadores. ➢ En 1989 el 80486 con más de 1millón de transistores, que ya incluía en el mismo chip un FPU [Floating Process Unit] o coprocesador matemático. ➢ En 1993 el Pentium tenía un poder casi 5 veces mayor al 80486. ➢ En 1998 se liberan el Pentium II Xeon para servidores, el Celeron para el mercado de bajo costo y el StrongARM para handhelds y equipos de comunicaciones ➢ En 1999 se liberan el Pentium III y Pentium III Xeon ➢ En 2000 se libera el Pentium 4, mientras que para el 2001 para servidores el Xeon y el Itanium. ➢ En 2003 el procesador Centrino ya incluía capacidad para WiFi, con lo que se detonó la explosión de las notebooks y laptops. ➢ En 2006 se introducen los procesadores de 2 y 4 núcleos en un CI, el Core 2 Duo y Core 2 Quad. ➢ Desde 2008 se han centrado en hacer más pequeños los procesadores, que ahorren energía y que incluyan mejores características para comunicaciones móviles. ➢ En 2011 y 2013 se liberaron las generaciones 2 y 3 de los procesadores de varios núcleos.	➢ En 1975 MOS Technology vendió el procesador 6502 de 8 bits; ese mismo año Motorola liberó el MC6800 (con casi 6,800 transistores), usado por la TRS-80. En 1976 la Apple I usó el 6502. ➢ **En 1977 la Apple II,** con base en el 6502, **primera computadora personal comercial** con teclado, monitor y lector de discos. ➢ En 1979 Motorola vendió su procesador 68000 de 32 bits. *En 1983 se vendieron cerca de 3.5 millones de computadoras personales.* ➢ En 1984 la Apple Macintosh usa un 68000, tenía un disco floppy de 3.5". Ese año se vendió el Motorola MC68020. ➢ En 1987 Salió la Macintosh II con procesador 68020 y también se produjo el MC68030. ➢ En 1990 se liberó el MC68040.

Tabla II.2. Procesadores populares para microcomputadoras en las décadas 70, 80, 90 y 2000. Durante los 80, Apple, Commodore, Amiga y Atari emplearon el 6502 en sus primeros modelos y luego aquellos de la familia 68000.

Por su parte uno de los procesadores totalmente RISC fue el MIPS I (***M****icroprocessor without* ***I****nterlocked* ***P****ipeline* ***S****tages*) de 32 bits liberado en 1985 por la compañía MIPS Technologies. Una página web donde se puede obtener información sobre una gran lista de procesadores y sus comparativos es la referencia [62].

II.5.4 Micro controladores

Los primeros controladores o micro controladores también se comercializaron en la década de los 70, para aplicaciones que requerían computadoras insertadas en otros sistemas; es decir, un controlador o micro controlador es una computadora en un chip. La diferencia con una computadora personal es que, un controlador no requiere de muchos puertos de comunicaciones, ni de mucha memoria, razón por la que muchos de los primeros controladores sólo tenían memoria hasta 64Kb en RAM y 4 puertos de comunicación: 2 de tipo serial y 2 de tipo paralelo. Por lo general los microcontroladores emplean una arquitectura Harvard en lugar de una del tipo Von Newman.

Los fabricantes de procesadores hicieron sus versiones de micro controladores, por ejemplo Motorola ofreció los MC68EC020, MC68EC030 y MC68EC040 a partir de los procesadores MC68020, MC68030 y MC68040 respectivamente, lo propio hicieron Intel, AMD e IBM, etc. Estos micro controladores se usaron en impresoras, tarjetas para video, consolas para video juegos, algunas computadoras personales, conmutadores telefónicos y routers.

En la actualidad, dada la facilidad para programar micro controladores, uno de los más populares es el **PIC**16F84 de 8 bits con 35 instrucciones, donde PIC (*Peripheral Interface Controller)*, otro es el **PIC**16C73 de 8 bits con 35 instrucciones [6].

II.5.5 Circuitos auxiliares empleados en las tarjetas de microcomputadoras

El factor de éxito que permitió el gran desarrollo de las computadoras personales fue el amplio soporte de circuitos integrados con sus varias funciones como: el 8251 controlador de comunicaciones, 8253 temporizador programable de intervalos, 8255 Interface programable de periféricos o PIC, 8257 Controlador DMA, 8259 Controlador programable de interrupciones, 8284 generador de reloj, 8282 latch octal, 8286 transceptor de bus octal, 8288 controlador de bus, 8289 árbitro de bus, el 8250 UART para comunicaciones seriales del estándar RS232, el 8255 PPI Interface programable de periféricos, el 8089 coprocesador de entrada y salida [6].

II.4. La computadora como una máquina multinivel

La definición de computadora ha evolucionado con el tiempo, para los primeros diseñadores de arquitecturas de computadoras, una computadora era sólo una máquina de estados; después se hizo generalizada la definición de que una computadora era simplemente hardware, después era la fusión de hardware con software. Una de las definiciones más completas permite entender a una computadora como un sistema multinivel o una máquina multinivel compuesta básicamente de máquina real y máquinas virtuales; ambas se pueden dividir en varios niveles. La figura II.2 muestra un diagrama de una computadora conformada por un sistema digital y máquinas virtuales, el software se presenta mediante interfaces CLI (*Command Line Interface*) o GUI (*Graphic User Interface*). También presento una adaptación con propósitos didácticos de una computadora y de un servidor, tomando como base la idea de Tanenbaum respecto de la computadora como una máquina multinivel [60].

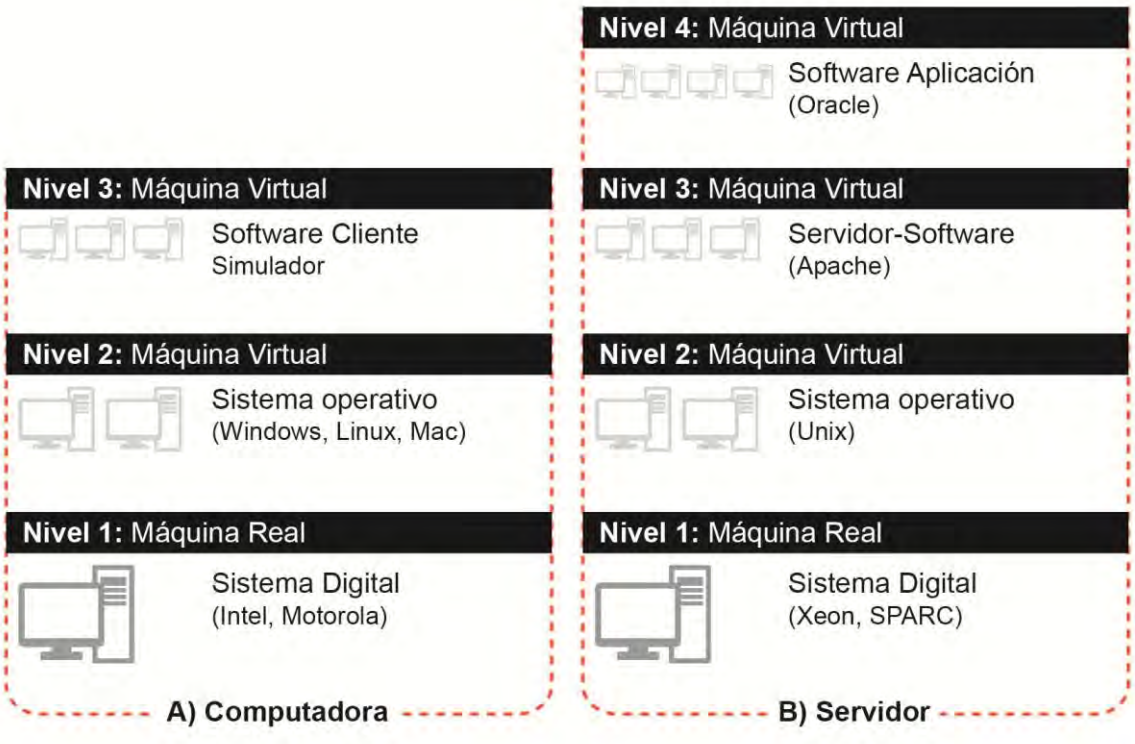


Fig. II.2 Computadoras vistas como máquinas multinivel.

II.5 La 4ta generación en México

En México desde 1977 y durante la década de los 80 fue un periodo de gran auge de las computadoras, pues las universidades y empresas tanto públicas (CFE y PEMEX principalmente) como privadas introdujeron minicomputadoras y microcomputadoras, las cuales podían verse incluso en algunos centros comerciales. Debido a las necesidades del mercado se presentó una primera fuerte migración de profesores de las universidades o instituciones de educación superior hacia las empresas públicas o privadas, un fenómeno cíclico que se repitió en los años 2000 y nuevamente en 2006, pero sólo hacia empresas privadas. Las universidades públicas tenían clara la aplicación como herramientas computacionales, pero IPN, UNAM y UAP decidieron además hacer desarrollos propios que se quedaron dentro de las instituciones. El ICUAP creó la microcomputadora CP-UAP una computadora con base en el procesador NEC V-20. En 1984 la SEP (Secretaría de Educación Pública) anunció su proyecto MICROSEP, con la idea de dotar a todas las escuelas del país, desde primaria hasta preparatorias o bachilleratos de microcomputadoras. El proyecto inició en 1985, primero participaron empresas para ofrecer un producto con base en el 6809E de TRS, como el *Computer Color* para la Microsep 1600. Posteriormente participaron en algunos prototipos IPN y la UNAM de manera intermitente en un segundo intento, pero con procesadores 80186 o 80188 de Intel para la Microsep 16, usaban el lenguaje de programación Basic; hubieron muchos cambios como era de esperarse y . Finalmente en 1988, la SEP entregó casi 5,000 sólo en algunas preparatorias y bachilleratos y de allí no pasó a mayores. Personalmente fue la segunda computadora con la que tuve contacto ese mismo año. La Microsep fue fácil de olvidar, era una tecnología del 77, un kit que seguía teniendo un gran parecido a las TRS. Al final de la década de los 80, el ITESM en Monterrey, UDLAP en Puebla y el ITAM en la Ciudad de México habían actualizado sus equipos y se encontraban mejor armados tecnológicamente que las universidades públicas, las cuales habían tenido en los 70 una gran época. Las universidades privadas se enfocaron principalmente en las Apple II y Macintosh, mientras que las públicas en IBM PC y PC-compatible. Respecto de los lenguajes de programación, Fortran y Basic dejaban de ser populares, dando paso principalmente a Pascal [6, 55,57].

II.6 Autoevaluación para el capítulo II

1. Defina computadora.
2. Indique cuál fue la primera computadora digital y a qué generación pertenece.
3. ¿Cuál es la diferencia entre la arquitectura de Harvard y la arquitectura de Von Neumann?
4. Explique el proceso de arranque de una computadora.
5. ¿Qué es un “end system”?
6. ¿Cuál es la diferencia entre microcontrolador y microprocesador?
7. Indique 3 diferencias entre CISC y RISC y expanda sus siglas.
8. Mencione 3 procesadores comerciales CISC y 3 procesadores RISC.
9. ¿Cuál es el procesador que se recomienda como mínimo para usarse en un servidor?
10. Ofrezca la clasificación de circuitos integrados con base en su escala de integración.
11. Indique los 4 nombres (corto y expandido) de las memorias semiconductoras tipo ROM empleadas en computadoras.
12. Ofrezca una clasificación de memorias RAM.
13. ¿Existen las memorias USB?, explique.
14. Indique 3 aspectos relevantes de la computación en México.
15. Indique 3 aspectos relevantes de la computación en América Latina.
16. Como recomendación cinematográfica está la película “código enigma” de 2015 para conmemorar los 100 años del natalicio de Alan Turing.

PARTE II: LAS REDES DE DATOS Y SU ESTANDARIZACIÓN

Una vez que las computadoras se hicieron comerciales en 1950 y que se llegó a su madurez en los 60, también se dio de manera natural la necesidad de interconectar a las computadoras. Se abordan pues los primeros 40 años en la evolución de las redes de datos (1965-2005).

CAPÍTULO III: EL NACIMIENTO DE LAS REDES DE DATOS

III. El nacimiento de las redes de datos

Las redes de computadoras marcaron una revolución, cambiaron la manera en cómo se realizan todas las actividades económicas, sociales, culturales y de educación entre otras. Fueron 10 años lo que tardó en que las computadoras comerciales en los países creadores de tecnología llegaran a aquellos en vías de desarrollo y algo similar ocurrió con las redes de computadoras incluyendo la internet. Gracias a esta tercera revolución industrial o la revolución de las TIC que nos coloca en la sociedad de la información y el conocimiento, actualmente, un producto creado en un lugar del mundo puede comprarse en otro en cuestión de segundos. En este capítulo se hace una revisión al nacimiento y evolución de las primeras redes de datos y así como se han definido generaciones para computadoras y sistemas operativos, propongo agrupar a las redes de datos, también en generaciones. La taxonomía que propongo no existe por el momento, sin embargo, hago la propuesta ya que sin duda en el futuro se emplearán tales de manera común; el criterio que empleo para proponer tal clasificación tiene que ver con la arquitectura propia de las redes de datos. Cronológicamente se aborda desde 1960 con la concepción sistematizada de las redes de datos hasta 1995 con el nacimiento de internet comercial.

III.1 La primera generación

Desde la aparición de los primeros circuitos eléctricos, pasando por la invención de los relés, bulbos y transistores hasta los circuitos integrados se había trabajado con la tecnología de conmutación de circuitos (*circuit switching*); esta es la que se usaba en las redes telefónicas analógicas y digitales. Cabe mencionar que quienes se preparan en electrónica, estudian en sus primeros cursos de dispositivos y circuitos eléctricos, dispositivos y circuitos electrónicos tanto analógicos como digitales este tipo de tecnología. Fue hasta 1961 cuando Leonard Kleinrock**,** en EEUU, modificó radicalmente la idea de los métodos de conmutación de circuitos a la conmutación de mensajes (*message switching*) con su artículo "Information flow in large communications nets". En 1964 Paul Baran**,** en EEUU, construyó la primera red de comunicaciones distribuida, la cual se podía conectar con varios nodos. Donald Watts Davies, en el Reino Unido, también desarrolló un sistema como Baran, acuñó el término "paquete" y "conmutación de paquetes", para describir los "bloques de datos" y el protocolo del manejo de mensajes en los dos sistemas indicados.

En 1964 ambas ideas se incorporaron en la ARPANET (*Advanced Research Projects Agency NETwork*). En 1966 ARPA usó conmutación de paquetes e inició un proyecto para conectar a las

universidades de EEUU. Mientras tanto, las computadoras mainframe de las décadas de los 50 y 60 de primera y segunda generación brindaban servicios como computadoras centralizadas en un determinado campus para atender a varios cientos de usuarios. Por ejemplo, en la UCLA (University of California-Los Angeles) se había desarrollado la red de área local (LAN- *Local Area Network*) más grande del mundo, en 1969, la UCLA contaba con 30 estaciones de comunicaciones CC-30 (*Computer Communications*) que se encontraban en todo el campus y se conectaban a 56Kbps, vía PSTN, con una computadora central IBM 360/75. Entonces quedaba la idea de comunicar a los colaboradores de proyectos de 2 campus de la Universidad de California, UCLA y UCSB (University of California-Santa Barbara) con el SRI (Standford Research Institute en California), de modo que se requirió ampliar la red para conectar en principio a 3 redes LAN y lograr la primera red de área metropolitana (MAN-*Metropolitan Área Network*). Los primeros resultados concretos se obtuvieron en 1969, cuando ya se tenían los equipos que podían comunicar dos o más redes, los procesadores de mensajes de interface o IMP (*Interfaz Message Processor*), que consistían en una minicomputadora Honeywell DDP-316 [63]. Una vez que se tenían los primeros IMP, con computadoras de tercera generación se conectaron 2 computadoras, la SDS Sigma 7 desde el nodo 1 en UCLA, hacia la SDS 940 en el nodo 2 en SRI en septiembre de 1969. Luego se les unió la IBM 360/75 en el nodo 3 en UCSB en octubre y finalmente se integró la DEC-PDP-10 como nodo 4 en la Universidad de Utah en octubre de 1969. Con esto nació la primera MAN, la cual fue construida por ARPANET, la red precursora de lo que hoy conocemos como la Internet. La comunicación se hacía vía la red telefónica empleando un modulador y demodulador o MODEM a 56 Kbps por PSTN. La figura III.1 muestra la disposición física de ARPANET, cuyos 4 nodos pudieron tener una conexión estable hasta diciembre de 1969 [64, 65].

Fig. III.1 En diciembre de 1969 ARPANET, primera WAN, contaba con sus 4 primeros nodos en EEUU.

Originalmente en 1969, la dirección IP de 4 bytes se dividió en el campo del número de red, que correspondía a los 8 bits más significativos y el campo restante, los 24 bits menos significativos; los 8 bits para el número de redes sólo permitían que existieran 254 redes diferentes.

En 1969 se creó el *Network Control Protocol* (NCP) protocolo que proveía las bases para la aplicación de la transferencia de archivos al comunicar los nodos de ARPANET, mismo que estuvo funcionando desde 1969 hasta 1973, cuando se le sustituyó por TCP. En septiembre de 1969 se definió el protocolo TELNET, el cual formaba parte del NCP como un subsistema definido como el *Network Subsystem for Time Sharing Host.* Un *host* se definió como cualquier computadora conectada a una red; y para emplear una *user-host* (terminal-host) remota como si fuera una terminal en un server –host (servidor), con ello se definió el modelo cliente servidor [66]. El modelo cliente servidor se hizo popular en la década de los 80, como un modelo de "computación distribuida", después de casi 20 años de "computación centralizada" con los mainframes; por esta razón al modelo cliente servidor le llamamos la segunda ola de la computación.

En la década de los 70 se desarrollaron varios protocolos propietarios de las distintas compañías que producían computadoras y que también competían en la industria de las redes de datos, como Xerox PARC, Ethernet, Novel Networks Protocol, DEC Protocols, IBM Protocols, etc. ARPANET usaba el protocolo NCP, pero también fue necesario contar con protocolos de comunicación. En diciembre de 1970 ARPANET contaba con 13 nodos y ya comunicaba a las dos costas de EEUU. En 1971 ARPANET tenía 18 nodos y no se dieron cambios espectaculares.

En 1972 nacieron el *File Transfer Protocol (FTP*) protocolo para la transferencia de archivos entre computadoras conectadas remotamente, y el *e-mail* aquel para la transmisión de mensajes de correo electrónico, ambos se convirtieron en los más populares [67]. Ese año Robert Kahn y Lawrance Roberts decidieron demostrar las capacidades de ARPANET en la *1st ICCC (International Conference on Computer Communications)* en Washington DC, durante la cual el uso de ARPANET se elevó en un 67% y ya contaba con 23 nodos. En 1973 Robert Metcalfe publicó una propuesta de Ethernet en Xerox. El mismo año, la ARPANET contaba con 41 nodos, dos de ellos ya eran los primeros enlaces satelitales, uno con Hawaii y el otro con Noruega, y de allí se extendió un enlace hacia Londres, Inglaterra [63, 64, 65]. Los IMP empleados en cada nodo para la comunicación desde 1969, se sustituyeron en 1973 por los *gateways*. En 1974 Vinton Cerf y Robeth Kahn, los arquitectos de ARPANET, publicaron una propuesta de protocolo para la intercomunicación paquetes en la red, la cual fue la base para desarrollar varios RFC, ellos con base

en el conjunto de protocolos de Xerox, el llamado PARC Universal Packet y por primera vez a la INTERNET dentro de ARPANET se le consideró como una interconexión de redes [68].

En 1975 Xerox desarrolló la Ethernet Experimental como red local; mientras tanto el DoD-ARPA declaró a ARPANET como una red completamente operacional. Este momento lo aprovecharon los contratistas de ARPANET, quienes crearon la primera compañía de comunicaciones por paquetes, *Telenet Communications Corporation,* la cual inició sus servicios en 7 ciudades de EEUU. Ese año se liberó la primera versión del protocolo TCP, cuyo trabajo se inició en 1973.

En 1976 Xerox publicó la primera versión de la red experimental Ethernet y la patentó en 1977. También en 1976 se creó el *Protocol handbook*, el cual contenía el compendio de todos los protocolos para ARPANET y otras redes.

En 1977 se probó TCP con enlaces satelitales, así como la factibilidad de contar con interconexiones de red mediante conexiones de redes de radio, teléfono y satélites. Ese año ARPANET contaba con 60 nodos y lo que había iniciado como la red ARPANET en realidad ya eran 16 redes por lo que se crearon los RFC "Assigned Numbers". Para noviembre ARPANET tenía asignado el número 10 dentro del apartado ANN (Assigned Network Number) para el empleo de los protocolos que se desarrollaban bajo el ARPANET [69].

En 1978 se generaron los rudimentos del TCP, al cual se le dividió en 2 componentes, uno fue el TCP (*Transmission Control Protocol* – Protocolo de Control de Transmisión), el cual era un protocolo *host to host* y el *Internet Protocol* (IP) un protocolo de interconexión encargado de pasar paquetes individuales desde un host a un switch o entre switches. El mismo año ISO (International Organization for Standarization) generó un modelo provisional de la arquitectura de sistemas abiertos para redes como una medida para contrarrestar la proliferación redes de datos y sus estándares propietarios bajo arquitecturas cerradas, tal modelo no era un estándar, sino un modelo provisional [70].

En junio de 1979 ISO publicó el modelo de referencia de OSI como una guía, no como un estándar [71]. Mientras tanto ARPANET ya contaba con 25 redes y se actualizó el *Protocol Handbook* [72].

En 1980 se liberó el *DoD Standard Internet Protocol*, una dupla a la que se le llamó TCP/IP, aquella que fue madurando desde 1978 hasta 1983 [73]. Uno de los protocolos, el IPv4 ya mostraba un Encabezado de Datagrama de Internet (*Internet Datagram Header*). Ese mismo año se preparó un plan de transición para cambiar el NCP por TCP/IP y se liberó una versión mejorada del FTP [74, 75]. ARPANET había crecido de 33 redes en enero a 38 redes en septiembre [76,77]. Ese mismo

año el consorcio DIX (DEC-INTEL-XEROX) liberó la primera versión de Ethernet; y dadas las condiciones IEEE inició sus trabajos para estandarizar el *Token Ring* de IBM y Ethernet como un protocolo internacional [78].

En 1981 ARPANET contaba con 40 redes, lo que conformaba una Internet no comercial [79]. El éxito de ARPANET fue tal que se planearon importantes cambios; la Sección de Ciencias de la Computación de la *National Science Fundation* (NSF) creó su propia red, la Computer Science Network (CSNET) a semejanza de ARPANET. La CSNET fue un proyecto de 1981 a 1985, que comunicaba centros de computación en EEUU, pero también comunicó a EEUU con las principales universidades, centros de gobierno e industriales y centros de investigación de Europa y Asia. También en 1981 RFC 801 planteó la necesidad de realizar el cambio de NCP a TCP/IP, el cual se realizó el 1 de enero de 1983.

También se definió al protocolo ICMP (*Internet Control Message Protocol* - Protocolo de Mensajes de Control de Internet) como parte integral de IP para informar respecto de errores en los datagramas empleados en IP; allí mismo se indicó que los *gateways* son los dispositivos que interconectan redes [80]. Además se publicó el RFC que planteaba ya las especificaciones del protocolo de programa de Internet de DARPA TCP para ARPANET [81].

Para noviembre de 1982 DIX liberó Ethernet II en el que se definieron las especificaciones lar las capas física (PL-*Physical Layer*) y la capa de enlace de datos (DLL-*Data Link Layer*) [82, 83]. Dada la importancia de Ethernet FDARPA generó el RFC 826 en el que definieron los protocolos ARP y RARP para la conversión de direcciones físicas o direcciones MAC en lógicas o direcciones IP y viceversa [84]. Dadas las limitaciones en el número de redes disponibles, el RFC 791 de 1981 permitió que se empleara el direccionamiento de redes por clases, ubicando el espacio de direcciones en 5 clases de direcciones (Clases A, B, C, D, E) para remediar el agotamiento de las direcciones de red.

Denomino **primera generación de redes de datos** (1969-1982) para incluir a aquellas redes que emplearon IMP, NCP, un máximo de 254 redes, tales como ARPANET y MILNET. Las redes LAN nacieron en los 60 y las WAN en diciembre de 1969, ambas usaron la tecnología de paquetes de datos con lo que se completó la transición de las redes de conmutación de circuitos las de redes de conmutación de paquetes.

III.2 La segunda generación

En 1983 sucedieron varios hechos muy importantes: Se liberó la tercera versión de Ethernet bajó el estándar IEEE 802.3 con lo que Ethernet se convirtió en un estándar internacional, el cambio a la trama de la versión de Ethernet II fue "LENGTH" en lugar de TYPE [85]. También se separaron las redes civiles de la militar, ARPANET tenía 113 nodos, con conexiones de *backbone* entre 45 Mbps y 90 Mbps. Al desprenderse la red MILNET (Militar Network), esta se quedó con 68 nodos y dejó a ARPANET con 45 nodos. También se conectó la exitosa CSNET con ARPANET. En junio ARPANET sustituyó el conjunto de protocolos NCP por el conjunto de protocolos TCP/IP, durante la transición varios nodos de ARPANET quedaron temporalmente desconectados hasta que la rede se logró estabilizar, y TELNET, como parte de TCP/IP, se redefinió como *Telnet Protocol Specification* [86]. Otro hecho importante que detonaría en un futuro las redes de computadoras es que ese año se vendieron en el mundo aproximadamente 3.5 millones de computadoras personales.

Para 1984 ya había tal cantidad de servidores que se inventó el DNS (*Domine Name Systems* -Sistema de Nombres de Dominio) para poder organizar a tales servidores en dominios y hacer la resolución de direcciones IP, para hacerlos más fáciles de acceder. Por su parte la NSF quiso replicar el éxito de la CSNET dentro de todas sus áreas, por lo que la NSF decidió crear la red NSFNET. Mientras tanto ISO liberó su primer estándar, el ISO/OSI 7498 como un modelo de referencia básico para sistemas abiertos de redes de datos [87].

En 1985 nació la NSFNET para comunicar a todas las universidades de EEUU para apoyarlas en sus proyectos de investigación, para ello inició con 5 nodos centrándolos en sus centros de supercomputadoras académicas con las que contaban creando un BACKBONE (Red principal) conectado a 56 Kbps vía PSTN, la intención de la NSFNET fue crear una INTER-NET o RED de REDES de índole académica conectada a la ARPANET, al cual conectaba a 100 universidades y centros de investigación en EEUU y Europa. En términos de sus backbone ARPANET tenía desde su nacimiento una arquitectura jerárquica completamente centralizada, mientras que la NSFNET desde su nacimiento tenía una arquitectura interconectada empleando el concepto de red de redes interconectadas. Por su parte la NSF ya no dio dinero a la CSNET ya que era autosuficiente con las cuotas de más de 165 universidades, organismos de gobierno y empresas conectados a esta.

Para 1988 mientras ARPANET contaba con sus 45 nodos, la NSFNET contaba con 13 nodos y su backbone se comunicaba vía un enlace para voz y datos que se componía de 24 canales DS0 (*Digital Signal*). Cada DS0 tiene un ancho de banda de 64Kbps, lo que da por resultado un

enlace de 1.5Mbps llamado DS1 o T1 (T1-Carrier) o E1 fuera de EEUU. Toda la red consistía en una colección de AS (*Autonomous System* - Sistema Autónomo) de modo que cada AS se administra vía una única entidad que tiene un determinado control técnico y administrativo de la infraestructura, en ese entonces todo EEUU conformaba un único AS. En este punto ya había gran claridad respeto de interconectar infraestructura de la red de datos dentro de un mismo AS y otro tema era interconectar 2 o más AS. De este modo en junio del mismo año se liberó el estándar del RIP (*Routing Information Protocol*), un protocolo que trabaja dentro de un mismo AS, es decir, un protocolo del tipo IGP (*Internal Gateway Protocol*). RIP permitía el intercambio de información de ruteo entre *gateways* y *host*, para lo que empleaba algoritmos del tipo "vector-distancia" como el *Bellman-Ford;* RIP se empleaba para interconectar redes de "tamaño moderado" que usaran tecnologías "razonablemente homogéneas"; RIP se genera con base en el programa "routed" que se había implementado en el sistema operativo UNIX, distribución BSD, para comunicar *gateways* entre sí desde 1970. Por otro lado para interconectar un AS con otro AS se empleaba el protocolo EGP (*External Gateway Protocol*) entre otros, para ese mismo año ya se les llamaba "protocolos de enrutamiento inter-AS" [88].

En 1989 se liberó el ISO/OSI versión 2 [89]. También se liberó el protocolo BGP (*Border Gateway Protocol*) para interconectar a los AS. El BGP es un protocolo de enrutamiento de sistemas inter-autónomos, para lo cual emplea el puerto 179 de TCP para realizar sus conexiones; para esa fecha los routers de Cisco y los sistemas de conmutación nodal de NFSNET ya manejaban tal protocolo. Para ese mismo año se publicó el *NSFNET Routing Architecture*, el cual dio una característica muy versátil a la NSFNET, en él se definieron los ***Regional AS*** y las ***NSS AS. El Regional AS*** es un número AS de una red regional y una red regional solamente puede tener un único número AS. La ***NSS AS*** es un número AS del backbone de la NSFNET, el cual por ser un "CORE backbone" puede tener varios AS. Para entonces la NSFNET era homóloga a la red ARPANET y la red científica de la NASA [90].

En 1990 el backbone ARPANET quedó desarticulado dejando su lugar a la NSFNET y con ello todo el desarrollo y crecimiento se centra en la NSFNET. Dado el crecimiento en el uso del protocolo TCP/IP, las principales compañías de computadoras en EEUU no desperdiciaron la oportunidad para dejar este protocolo disponible para cualquier computadora dentro del mercado de EEUU.

Denomino **segunda generación de redes de datos** (1983-1990) para incluir a aquellas redes que emplearon Gateway en lugar de IMP; TCP/IP en lugar de NCP, y que incluyeron direccionamiento por clases A, B, C, D, E. Ejemplos son ARPANET (V2), CSNET y NSFNET.

III.3 La tercera generación

En 1991 el backbone de la NSFNET había crecido a 16 nodos para conectar a más de 3,500 redes y tal era la demanda de servicio que se inició la transición a un "backbone de banda ancha", de este modo los enlaces T1 de backbone se irían migrando a enlaces T3 (E3 o DS3 = 28 DS1) cuyo ancho de banda era de 45Mbps. Para este momento ya habían tres niveles de redes: El nivel de backbone de la NSFNET (varios AS), el nivel de las redes regionales (un AS), y el nivel de las redes de los campus de las universidades y centros de investigación, a partir de lo cual se usan de manera coloquial las designaciones de los niveles core, distribución y acceso respectivamente. Ese mismo año se creó el CIX (Commercial Internet eXchange), el cual era un punto donde se podía tener un libre intercambio de tráfico entre la NSFNET y el tráfico de las redes comerciales ya implementadas de manera independiente, lo cual alimentó la idea del advenimiento de un internet comercial. También ese año la universidad de Minnesota introdujo el sistema Gopher, en realidad le acompañaba un protocolo TCP/IP en la capa de aplicación, una aplicación que mostraba archivos y directorios bajo una estructura de árbol, la cual facilitaba a los usuarios el manejo y la organización de la información y con base en ello, para diciembre del mismo año Tim Berners-Lee del CERN en Europa desarrolló la WWW (*World Wide Web***)** versión 1, la cual era un sistema de archivos ligados por hipertexto y a los cuales se podía acceder vía la internet, misma que fue socializada a otros centros de investigación de física; la WWW era un sistema conformado por 6 elementos: un protocolo HTTP (*Hyper Text Transfer Protocol*), un lenguaje HTML (*Hyper Text Markup Language*), un WEB browser WWW, un web server-software, un web server-hardware y las primeras páginas web [88]. En enero de 1993 habían 50 *websites* (sitios web), para febrero se anunció que Gopher ya no sería de acceso libre, y los desarrolladores de la WWW aprovecharon para dejarla libre y gratuita en abril, de modo que se dio una gran migración de Gopher a WWW, así que para julio ya habían 130 *web sites* y en marzo de ese año se liberó formalmente *The Internet Gopher Protocol, a distributed document search and retrieval protocol*. En noviembre de 1993 la NCSA (*National Center for Supercomputing Applications*) de la Universidad de Ilinois liberó una "versión 1.0" del visor de la web (Web Browser) llamado *Mosaic*, una aplicación cliente que soportaba los protocolos FTP y Gopher, era el primer sistema que incluía imágenes a color como parte de una página web (web page) dentro de un *website* y un mes después 40,000 usuarios habían bajado copias de Mosaic y el número de *web sites)* en el mundo fue de 623.

Para abril 1994 ya había 1 millón de usuarios, por lo que para diciembre de ese mismo año, la NCSA libera la versión comercial de *Mosaic* llamada *Netscape***,** y partir de allí gracias a la web y

los visualizadores (browsers), internet se hace muy popular, ese diciembre de 1994 ya habían 10,022 sitios web dentro de la NSFNET [91]. Para esa fecha el protocolo gopher ya había sido superado por el HTTP, un protocolo que funcionaba como protocolo petición y respuesta bajo el modelo de computación cliente-servidor [92]. También ISO /OSI actualizó su modelo con base en los cambios de IEEE [93]. Para noviembre se hizo imperante clarificar la diferencia entre *gateways*, computadoras de propósito general usadas desde 1973, y los routers [94].

Para 1995 el crecimiento de internet era exponencial, ya contaba con más de 100,000 redes tanto públicas como privadas tan solo dentro de EEUU, de modo que para el 30 de abril de 1995 la NSFNET queda desarticulada para desaparecer y dejar su lugar a la "Internet comercial" que todos conocemos actualmente, de modo que los usuarios se conectarían con su ISP (*Internet Service Provider-Proveedor de servicios de internet*) y él los conectaría a internet, de modo que el gobierno de EEUU puso fin al control de la infraestructura de su red abriendo la puerta al sector privado, mientras que la internet tenía para julio de 1995 un total de 23,500 sitios web [88]. La tabla III.1 muestra la línea de tiempo resumen para las grandes redes hasta la llegada de internet comercial.

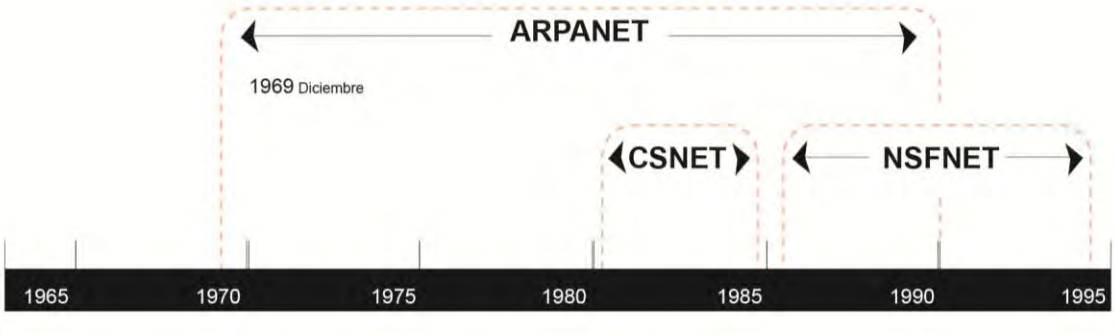


Tabla III.1. Línea de tiempo de 25 años para las redes grandes {WAN[MAN(LAN)]} previas a la Internet

Para junio de 1999 se liberó la primera versión madura de HTTP 1.1, un ejemplo claro de web estática es mi página web: "http://ewh.ieee.org/sb/mexico/uacm/jicv/jicv.html". Además el consorcio W3C vía Tim Berners-Lee anunció la llegada de la "Web 2.0", la web semántica, la cual se empezó a materializar hasta alrededor de 2002 y ha ido tomando forma pero no ha llegado todavía a su madurez [92]. Desde 2012 los browsers más populares mundialmente son Chrome de Google, Internet Explorer de Microsoft y Firefox de Mozilla.

Denomino tercera generación de redes de datos (1990-2012) para incluir a aquellas redes que emplearon Routers en lugar de *gateways*, TCP/IPV4, direccionamiento por clases A, B, C, D, E, una arquitectura por sistemas autónomos y protocolos de enrutamiento. Ejemplos son NSFNET e internet comercial e Internet II. Y denomino cuarta generación de redes de datos (2012-) para incluir a aquellas redes que emplearon Routers, TCP/IPV6, una arquitectura por sistemas autónomos y protocolos de enrutamiento avanzados y las redes que se gestan en respuesta al espionaje y la guerra en el ciberespacio.

III.3.1 Internet en México

En 1990, la empresa REDUNO fue la primera en importar un router de CISCO, de allí se expandió como ISP (*Internet Service Provider* - Proveedor de servicios de internet) con fines empresariales para redes corporativas. En México para 1995 algunas universidades y centros de investigación ya contaban con internet, los servicios que más usábamos en esa época eran los servicios de e-mail y aquellos de los servidores ftp. En 2008 existían 438 empresas como ISP, de los cuales el 50% no cumplía con la mínima calidad del servicio que es dar al menos la velocidad prometida al usuario, daban el 50% de velocidad, aun considerando que la velocidad de bajada (*download*) es mucho mayor a la velocidad de subida (*upload*); ese mismo año México ocupaba el lugar 44 de 64 países en el empleo de tecnologías de la información (TI) y específicamente en materia de telecomunicaciones tenía un retraso de 4 años respecto del 1er mundo; actualmente las cosas no han cambiado mucho. En 2009 alrededor de 4,600 millones (67% de la población mundial) contaban con servicios de telefonía celular, la penetración era del 100% en los países desarrollados y del 57% en aquellos en vías de desarrollo; por sus parte, la penetración en banda ancha internet era de 640 millones de abonados a banda ancha móvil y 490 millones a banda ancha fija. Con la finalidad de medir el grado de inserción de un país hacia una sociedad del conocimiento se cuenta con el Índice de desarrollo de las TIC (IDI), el cual es un índice que presenta una escala de 1 a 10, formado por 11 indicadores que indican el acceso, uso y conocimientos TIC de un país. Antes de 2007 los informes de IDI tenían fuertes variaciones en las posiciones que ocupaban 159 países, entre 2007 y 2008 las posiciones se han estabilizado y no presentan cambios abruptos; se distinguen dos grandes bloques, el de los países desarrollados y el grupo de países menos adelantados (PMA). Los 10 primeros del primer grupo en orden del puntaje más alto al menor lo componen Suecia, Luxemburgo, República de Corea, Dinamarca, Países Bajos, Islandia, Suiza, Japón, Noruega y Reino Unido. Por su parte México se encontró en 2013 en la posición 77 detrás de países

latinoamericanos como Argentina, Uruguay, Chile, Trinidad y Tobago, Brasil, Venezuela, Panamá, Colombia, Jamaica, Costa Rica, Perú [88].

III.4 Autoevaluación para el capítulo III

1. ¿Cuál es la función de una red de computadoras?
2. Genere un cuadro referente a las generaciones de redes de computadoras propuestas por el autor.
3. Indique la diferencia entre conmutación de circuitos y la conmutación de mensajes.
4. ¿En qué año se propone la conmutación de paquetes y por qué es ésta importante?
5. ¿A quienes se les considera los arquitectos de ARPANET/ INTERNET?
6. Indique la diferencia principal entre la primera y la segunda generación de redes
7. Indique la diferencia principal entre la segunda y la tercera generación de redes
8. ¿Cuál es la diferencia entre internet y la WWW?
9. Mencione las diferencias entre web 1.0 y web 2.0
10. Liste los protocolos indicados en este capítulo, expandiendo sus siglas en inglés y español.
11. Indique cuál es el ISP que usted utiliza normalmente
12. Indique el motivo por el cual se diseño el IPV6?

CAPÍTULO IV: LA ESTANDARIZACIÓN EN REDES DE DATOS

IV. La estandarización en las redes de datos

Cuando se crearon las primeras redes de computadoras, en la década de los años 60, sólo podía haber comunicación entre computadoras del mismo fabricante y como muchos sistemas se desarrollaban de manera propietaria había problemas de incompatibilidad al querer hacer conexiones con otras redes; las principales compañías que creaban protocolos de comunicación eran Xerox, Novell, DEC, IBM. En este capítulo se abordan desde los sistemas propietarios en redes de datos a la estandarización pasando por Ethernet e ISO-OSI como modelos para redes de datos y se incluyen 4 prácticas de laboratorio con la finalidad de esclarecer conceptos.

IV.1 Ethernet.

Como se revisó en el capítulo anterior entre 1973 y 1977 Xerox creó, desarrolló y patentó Ethernet; para dar fuerza a Ethernet, se creó el mencionado consorcio DIX. En septiembre de 1980**,** DIX publicó la primera versión de "las especificaciones de la Red de Área Local Ethernet", donde se describía la arquitectura e implementación del funcionamiento de Ethernet. La versión Ethernet DIX 1 cubre la arquitectura e implementación de Ethernet con base en un modelo funcional de 2 capas: la PL (*Physical Layer* - capa física) o capa de nivel 1 o L1 y la DLL (*Data Link Layer*- capa de enlace de datos) o capa de nivel 2 o L2 [78].

La capa física (PL) especifica las características mecánicas, eléctricas, funcionales y procedimentales, tales como la topología de bus (conocida entonces como *Branched non-rooted tree*), el segmento de red, los repetidores, los *transceivers*, para transmitir a una velocidad de 10Mbps.

En la actualidad los trasceivers quedan dentro de las tarjetas de red (*Network Interface Card* - NIC). Las especificaciones eléctricas aplicables para el cable coaxial de 50 Ohms con señalización de banda base (sin modulación) para frecuencias en una banda de 20MHz, un máximo de 1024 equipos y una longitud total máxima por segmento de 500 metros, de tal modo que tomó el nombre de "10BASE5". Un ejemplo de topología de bus que emplea 10BASE5 se indica en la figura IV.1.

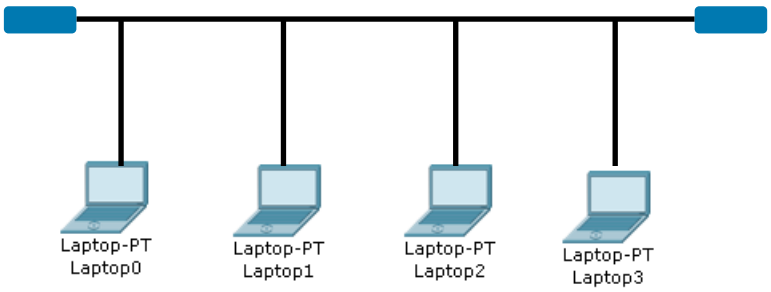


Fig. IV.1 Topología de Bus, en ambos extremos se incluyen terminadores.

Por otra parte, la DLL se dividió en 2 subcapas, la subcapa MAC (*Medium Access Control*-Control de Acceso al Medio) y la subcapa LLC (*Logical Link Control*-Control de Enlace Lógico). La DLL especifica tanto el procedimiento de control de enlace para la subcapa MAC, como el protocolo de mensajes para la subcapa LLC. El primero usa CSMA/CD (*Carrier Sense Multiple Access/ Collition Detection*- Acceso Múltiple por Detección de Portadora/ Detección de Colisiones) y a su vez define 2 funciones, el encapsulamiento de datos y la administración del enlace. El segundo usa tramas de tamaño variable que se entregan bajo la premisa del mejor esfuerzo. El servicio que provee esta capa hacia las capas superiores son "envío de trama" y "recepción de trama", cuyo "modelado de procedimientos" se hizo empleando algoritmos que se escribieron en notación del lenguaje de programación Pascal, pero se implementaron con micro-código en máquinas de estados a nivel de hardware [78, 82].

La trama contenía 5 campos: uno para las dirección MAC destino, la dirección MAC fuente, los datos (paquete de la capa superior o capa de nivel 3), el tipo de protocolo y el código de redundancia cíclica o CRC que consiste en un código para la detección de errores. En la sección IV.3.2 se presentará la trama de la versión 3 de Ethernet por ser una mejora de la versión 1 [85].

IV.2 La estandarización para los sistemas abiertos: ISO/OSI.

En 1978 y 1979 se publicaron los primeros borradores OSI (*Open Systems Interconnection*-Sistema de Interconexión Abierto) de ISO, sin embargo, en 1984 ISO liberó el primer estándar para sistemas abiertos, como el modelo de referencia OSI en el ISO 7498:1984 [70, 71, 87]. Tal estándar se generó con base en el trabajo emprendido por Ethernet de DIX y TCP/IP de DARPA [73, 74, 78, 81, 82]. ISO/OSI es un conjunto de estándares que buscan asegurar la compatibilidad e interoperabilidad entre las distintas tecnologías de redes. El modelo OSI es el modelo arquitectural primario para las redes, describe cómo se comunica la información desde las aplicaciones a una computadora, a través de los medios de la red hacia una aplicación que corre en otra computadora.

En 1989 se liberó el ISO 7498-2:1989 como la segunda parte del estándar para tratar el tema de la arquitectura de la seguridad [89]. En 1994 se liberó el estándar ISO/IEC 7498-1:1994, para reemplazar la primera edición de 1984 y en 1997 el ISO/IEC 7498-3:1997 agregaron observaciones para nombres y direcciones [93, 95]. Cada capa del modelo tiene una función específica e indica sus dispositivos de hardware o de software asociados; la figura IV.2 muestra el modelo OSI de 7 capas y su mapeo al modelo TCP/IP de 5 capas.

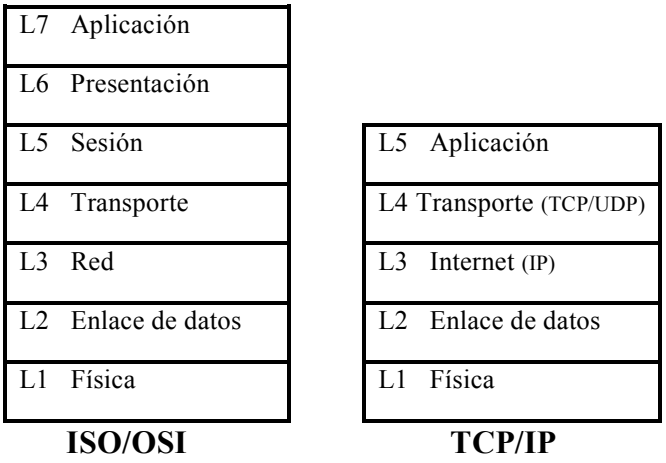


Fig. IV.2 Capas funcionales del modelo ISO/OSI y su mapeo al modelo TCP/IP

En la figura IV.3 se indican algunas características generales que permiten comprender los alcances y la utilidad del modelo ISO/OSI.

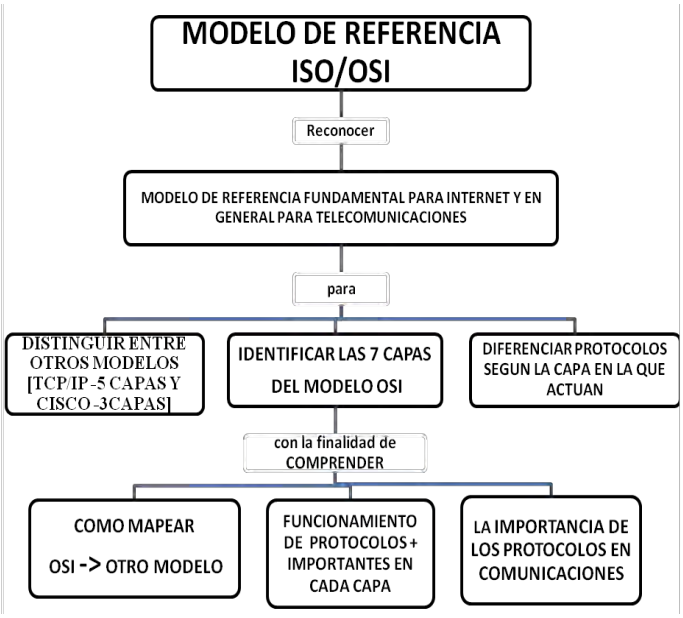


Fig. IV.3. Mapa del modelo OSI

En la tabla IV.1 se ofrece un resumen de las ventajas de contar con el modelo de referencia ISO/OSI.

Reduce la complejidad	El modelo jerárquico divide la operación en capas para hacerlo manejable.
Describe una tecnología interoperable	Permite que los desarrolladores de aplicaciones se especialicen en el diseño y desarrollo, ya que los cambios se hacen sólo en una capa.
La estandarización de interfaces	Se pueden definir interfaces estándar para la integración multi-fabricante tipo “plug & play”.
Es un modelo didáctico	El mejor modelo para enseñar “cómo se transmiten los datos en una red”.

Tabla IV.1 Ventajas del modelo de referencia ISO/OSI.

Con la finalidad de resumir la influencia que permitió el origen de ISO/OSI en 1984 como un estándar, se presenta la línea de tiempo de la figura IV.4, la cual incluye los eventos importantes para Ethernet y TCP/IP.

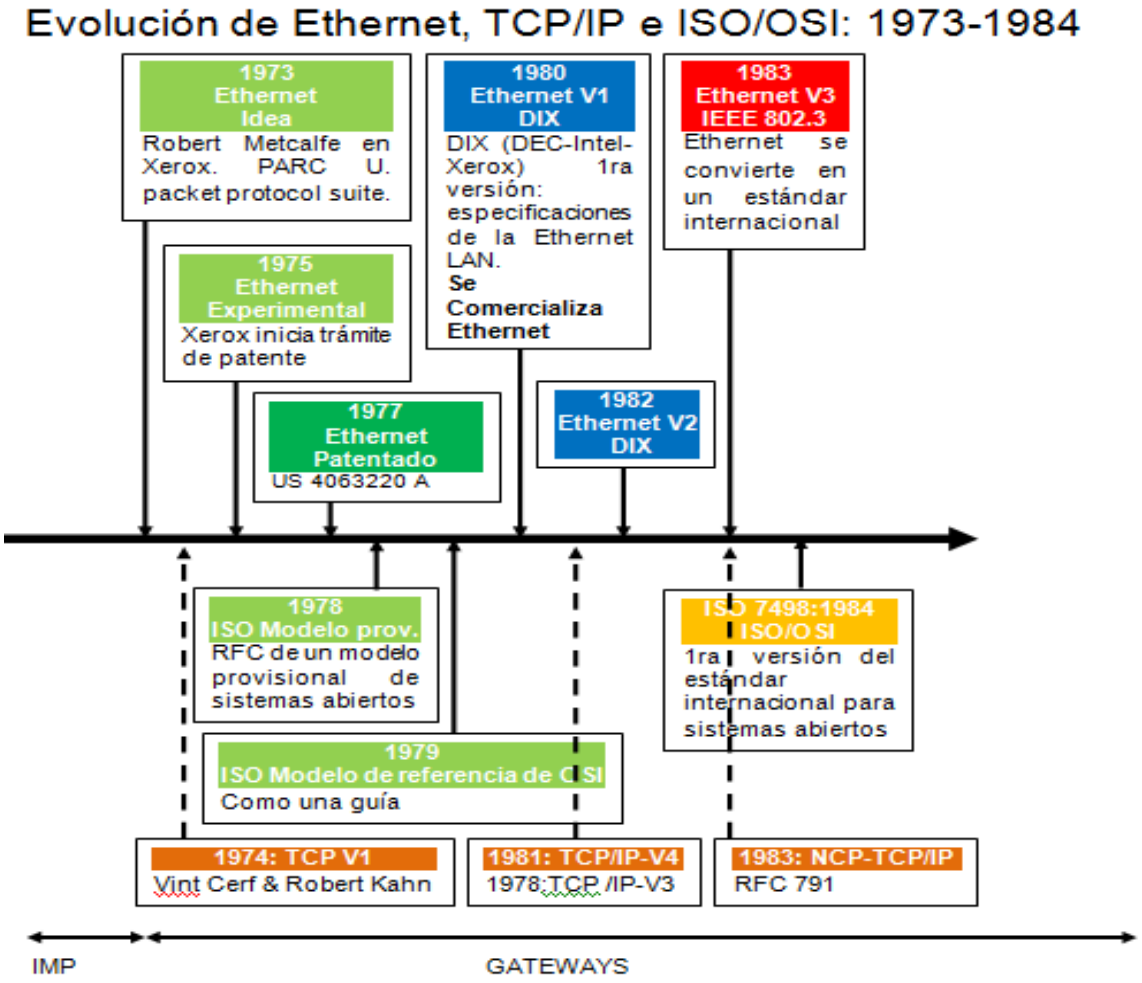


Fig. IV.4. Línea de tiempo para Ethernet, TCP/IP e ISO/OSI, desde su origen hasta su estandarización.

En 1996 Robert Metcalfe recibió la *IEEE Medal of Honor* por "El liderazgo ejemplar y sostenido en el desarrollo de la estandarización y comercialización de Ethernet". En 2000 Leonard Kleinrock, Paul Baran, Davis y Roberts recibieron la *IEEE Internet Award* por sus contribuciones al concebir, analizar y demostrar las redes conmutación de paquetes, tecnología fundacional de la internet [96].

IV.2.1 El encapsulamiento y desencapsulamiento de datos.

El "encapsulamiento de datos" es un proceso de conversión de los datos del usuario que inicia en la capa 7, con el que se puedan enviar paquetes por una red. Conforme la información se mueve a lo largo de las capas, en cada capa se añade un "encabezado" (HDR-Header) que tiene datos de control necesarios para los dispositivos en el receptor; así la capa de aplicación agrega el "encabezado de la capa de aplicación" (L7-HDR) a los datos originales del usuario y de allí se envían a la capa de presentación, la cual a su vez agrega un encabezado (L6 HDR) y así sucesivamente hasta que llegan a la capa 2 donde además del HDR se agrega un campo FCS (*Frame Check Secuence*) para la detección de errores como se indica en la figura IV.5. El proceso de "desencapsulamiento" es inverso y se presenta una vez que los paquetes llegan a la capa uno del *host* receptor y éstos van pasando desde la capa 1 a la capa 2, 3 y así sucesivamente hasta llegar a la capa 7 del *host* receptor [79, 82].

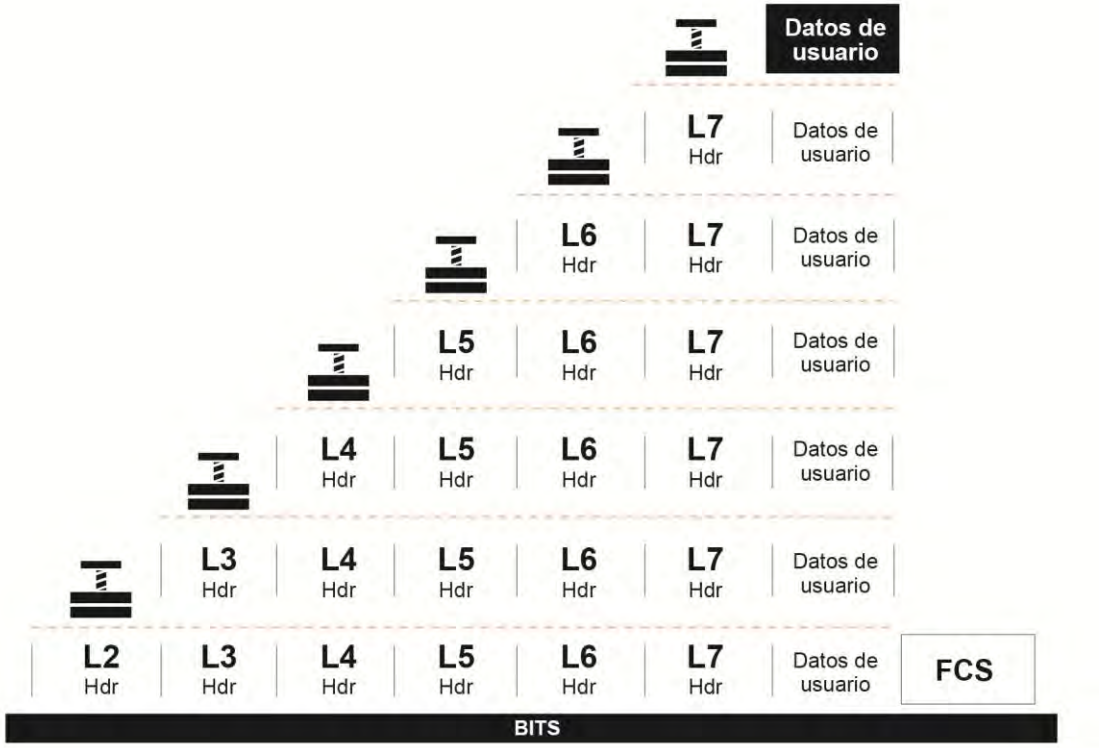


Fig. IV. 5. Proceso de encapsulamiento y desencapsulamiento en cada capa. Los paquetes de la capa 3 se encapsulan dentro de la trama de la capa 2.

En la siguiente sección se hará una revisión de algunos de los protocolos más comunes en las distintas capas del modelo ISO/OSI

IV.3. Las capas ISO/OSI y algunos de sus protocolos

IV.3.1 La capa física y sus protocolos

La capa física o de nivel 1 define las especificaciones eléctricas, mecánicas, funcionales y procedimentales, que permiten transmitir y recibir bits entre dos hosts. Las especificaciones eléctricas definen por ejemplo los niveles de voltaje (ej. +5 v, GND, 0v) y el tiempo del cambio en sus niveles de voltaje. Las especificaciones mecánicas definen las distancias de transmisión máximas, los conectores físicos como en el caso del estándar "RS-232", el cual define conectores DB-9 y DB-25, así como una distancia máxima de 2.5 mts. Las especificaciones funcionales definen que terminal mecánica o física corresponde a cada terminal eléctrica, por ejemplo en un conector determinado, la terminal 1 corresponde a tierra, la terminal 2 a la terminal para la transmisión, la terminal 3 para recepción, etc. Las especificaciones procedimentales sirven para definir como se deben activar, mantener y desactivar la capa física entre los sistemas terminales, de modo tal que permitan transmitir y recibir bits entre dos hosts.

Nota: No deben confundirse protocolos que definen estándares con puertos de comunicación ni con conectores. El caso típico se da cuando la gente confunde al estándar USB con la memoria flash y llaman a la memoria flash por el estándar que usa para comunicarse con el exterior, el USB. Un hub es un equipo de capa 1, es un repetidor, en nada se relaciona con una MAC.

La manera más fácil de crear una red es con dos computadoras. La manera de realizar esta comunicación puede ser alámbrica o inalámbrica, ya sea mediante un enlace de microondas, conexión por fibra óptica para distancias de medianas a grandes o por cable de cobre para distancias largas o medianas (si se usa la infraestructura PSTN mediante el modem) o cortas (si se hace vía directamente las interfaces de una computadora con cable). Para realizar la comunicación entre computadoras se usan protocolos, los cuales son un conjunto de reglas que controlan el flujo de información entre dos computadoras, para lo cual se definen interfaces.

Entre la décadas de los 60, 70 y 80 se desarrollaron protocolos de comunicación e interfaces que empleaban determinados protocolos, entre ellos están: *Omnibus*, *Unibus* (empleados en equipos DEC-PDP), *Centronics*, HP-BUS (HP-IB de 1965), GPIB, IEEE-488

(1Mbps en 1975, con alcance máximo de 20 mts.), IEEE1284 (paralelo bidireccional Centronics), *Fire Wire* (para electrónica de consumo), RS232 (Recommended Standard).

IV.3.1.1 Comunicación serial: RS232 y USB

La conexión entre dos computadoras para distancias cortas ha sido una práctica común, principalmente la comunicación serial bajo el estándar RS232, ya sea usando el conector DB9 o DB25 con un cable tipo "null". Para las computadoras personales, la tarjeta del estándar RS232 empleaba un UART (*Universal Asynchronous Receiver Transmiter*), un CI que convertía la información proveniente de un bus de 8 bits en paralelo a una salida serial, tal CI era auxiliado por otros CI para conformar los puertos de comunicación serial del estándar RS232. El RS232 ha evolucionado con el tiempo, de modo que se tienen por ejemplo las versiones RS422, RS423, RS449, RS530, pero a toda esa gran familia se le sigue considerando solamente como RS232.

En 1996 apareció el estándar USB (*Universal Serial Bus*) como la evolución del estándar RS232 y dado su gran éxito, éste se convirtió en el *bus* serial estándar para conectar todo tipo de equipos a una computadora *host* o *end system*, el cual puede ser toda computadora, servidor, impresora, teléfono IP, etc. En el caso de las microcomputadoras, USB ha sido la interface más exitosa en su historia. USB usa un modelo *hub-root-host* que le permite desprender de su *hub* una dirección raíz y de allí poder conectar hasta un máximo de 127 dispositivos de comunicación, pero en los equipos reales existe solamente una limitación energética dado que, por ejemplo, la versión USB 1.0 permite extraer un máximo de 150mA hasta 2.5W por puerto por equipo, de modo que la limitación extraída dada por el número de puertos habilitados en función de la capacidad de la fuente de alimentación. La tabla IV.2 resume algunas características de las 3 versiones de USB con las que contamos hasta hoy [97].

Versión	Año de liberación	Ancho de banda	Tiempo de transferencia de un archivo multimedia		
			4 MB	1 GB	25 GB
USB 1.1 (Full speed)	1996	12 Mbps	5.3 seg	22 min	9 hrs
USB 2.0 (Hi-speed)	2000	480 Mbps	0.1 seg	33 seg	12 min
USB 3.0 (Super -speed)	2008	4.8 Gbps	0.01 seg	3.3 seg	80 seg.

Tabla IV.2. Versiones de USB.

Durante los años 70, 80 y 90 fue común como ejercicio, comunicar 2 computadoras usando RS232, para lo cual era necesario programar en los lenguajes Fortran o Pascal o C, pero para la segunda mitad de los 90 comunicarlas vía USB se hizo práctica común. Sin embargo, conforme se hicieron populares las tarjetas de red o NIC también era práctica común comunicarlas de este modo. La comunicación entre dos computadoras también se conoce como la comunicación de una red punto a punto (P2P-*Peer To Peer*). Más adelante proponen un par de prácticas de laboratorio, las cuales incluyen simulaciones con la finalidad de clarificar conceptos relacionados con las capas 1, 2 y 3.

IV.3.1.2 Cables de par trenzado para redes de computadoras

En un principio, para comunicar computadoras y redes de computadoras se usaron distintos estándares, como los ya mencionados, también se uso par trenzado (*Twisted Pair*), del llamado categoría 1 y 2, ambos presentaban bajas prestaciones hasta que en 1990 se liberó comercialmente el cable par trenzado categoría 3 o "cat 3", el cual permitió un ancho de banda de 10Mbps. En 1991 aparece la versión de la TIA/EIA 568 (*Telecommunications Industry Association/Electronic Industries Alliance*) para definir estándares para el cableado estructurado. En 1995 se hace una revisión y se genera la TIA/EIA 568-B o ISO/IEC 11801:1995, el cual indicó que las categorías 1 y 2 eran buenas para voz más no para datos y se definieron los detalles particulares para las "categorías 3, 4 y 5". El cable UTP (*Un-Shielded Twisted Pair)* se emplea básicamente para reducir la "interferencia por RF" y el *crosstalk*, términos que el lector conoce. La tabla IV.3 resume las categorías de cables UTP disponibles en el mercado.

Categoría	Ancho de banda	Ancho de banda de señal	Estándar
Cat 3	10 Mbps	16 Mhz	10BASE-T [IEEE 802.3i] (1990)
Cat 4	16 Mbps	20 Mhz	Token Ring
Cat 5	1,000 Mbps 1Gbps	100 Mhz	10BASE-T, 100BASE-TX [IEEE 802.3u] (1995), 1000BASE-T [IEEE 802.3ab] (1999)
Cat 5e Enhanced	3,000 Mbps 3Gbps	350 Mhz	Mismos cables que Cat 5, todos a 100 mts. Reduce Crosstalk
Cat 6	10,000 Mbps 10 Gbps	250 Mhz	10BASE-T, 100BASE-TX, 1000BASE-T 10GBASE-T [IEEE 802.3an] (2006) Pero se limita la distancia a 55 mts.
Cat 6ª	10 Gbps	500 Mhz	Igual que para Cat 6 pero mayor frecuencia y mejoras en la reducción en interferencia y crosstalk. [10GBase-T a 100 mts].
Cat 7 y 7ª	10 Gbps	700 Mhz/1 Ghz	Cat 6A mejorado
Cat 8	40 Gbps	2 Ghz	10GBASE-T [IEEE 802.3bq] (2013) Distancias cortas (20 mts.) usados en Data Centers a nivel de rack.

Tabla IV.3. Categorías de cables UTP en el mercado.

El conjunto de estándares IEEE 802.3 definen la capa física y la capa de enlace de datos, en particular la subcapa MAC para Ethernet cableado para las tecnologías LAN y MAN. Para el caso de los estándares para medios, IEEE 802.3 emplea las letras como en los estándares para 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T y 40GBASE-T [85].

IV.3.2 La capa DLL y sus protocolos: CSMA en Ethernet

La "capa de enlace de datos o capa 2" define cómo se formatean los datos para su transmisión y como se controla el acceso al medio físico, incluye la detección de errores para asegurar la entrega de datos, para lo cual realiza comunicación vía tramas (frames) en las que se indica la dirección MAC origen y destino. Los bridges y switches son equipos de capa 2 y usan tabla de direcciones MAC. Para este caso nos debemos remitir a la trama de Ethernet II o la trama definida por IEEE 802.3; en el caso del encapsulamiento desde la capa 7 a la capa 2, se debe conformar la trama como se indicó anteriormente. Para el caso del desencapsulamiento desde la capa 2 a la capa 7, en el caso de encontrar errores en la capa 2**, e**ntonces se descarta la trama el paquete y solicita la retransmisión; en el caso de no existir errores, entonces la capa de enlace de datos lee e interpreta las señales de control del encabezado HDR, después descarta el L2 HDR y su FCS y transfiere los datos hacia L3 con base en la información de control que leyó anteriormente. Es por ello que cada capa del *host* emisor se comunica con la capa homóloga del *host* receptor, para lo cual en la capa 2 existe tráfico de "frames o tramas".

Una trama de Ethernet II se define con base en 6 campos: una es el "preámbulo" (*preamble*), el cual consiste en una señal de sincronía a 5Mhz generado por una secuencia de unos y ceros en 8 bytes; el siguiente campo es "la dirección MAC destino" de 6 bytes; el siguiente campo es "la dirección MAC fuente" de 6 bytes; el campo "type" indica el protocolo de la capa superior; a continuación sigue el "campo de los datos (*Data*)", el cual está compuesto por el paquete proveniente de la capa de red, la cual quedó encapsulada con una longitud variable entre 46 bytes y 1500 bytes; y finalmente el campo FCS (Frame Check Secuence- Secuencia para la Verificación de la Trama), el cual se encarga de detectar posibles errores vía un CRC (Ciclic Redundancy Code - Código de Redundancia Cíclica). La trama Ethernet II se muestra en la figura IV.6 [83, 85].

Preámbulo	**Dirección MAC destino**	**Dirección MAC origen**	**Tipo**	**Datos**	**FCS**
8 bytes	6 bytes	6 bytes	4 bytes	46-1500 bytes	6 bytes

Fig. IV.6. Trama o *frame* Ethernet II en la capa DLL.

Dado que la dirección MAC forma parte de una trama Ethernet, en la figura IV.7 se muestra como se compone una dirección MAC definida en una NIC o WNIC.

Bit de broadcast	Bit local	OUI	Vendor
1 bit	1 bit	22 bits	24 bits

Fig. IV.7. Composición de una Dirección MAC en una NIC o WNIC, resulta en 48 bits (6 bytes)

En telecomunicaciones con la finalidad de transmitir sobre un medio (cobre, aire o fibra óptica), o para compartir su capacidad con otras terminales o equipos que se encuentren conectados al mismo, se utilizan métodos para el acceso a un canal, también conocidos como métodos de acceso múltiple. La pregunta a resolver es ¿cómo comparto el medio de transmisión canal de comunicación o medio físico como UTP, fibra óptica, aire? La solución está en la multiplexación, pero cuando se realiza la multiplexación en la capa física para conexiones full dúplex o punto a puntos nos encontramos en la conmutación de circuitos (*circuit switching*). Existen cuatro tipos básicos de acceso al canal:

A) FDMA (*Frecuency Division Multiple Access* - acceso múltiple por división de frecuencia), usa multiplexación por división de frecuencia. Por ejemplo, se puede dividir a una "única portadora inicial" en 4 portadoras distintas o 4 frecuencias portadoras (HF, LF), una para cada terminal sobre las cuales se puedan transmitir las 4 terminales. Si las conexiones fueran por fibra óptica, se usaría una variante de FDMA, por longitud de onda, es decir, WDMA de modo que en lugar de transmitir a 4 diferentes frecuencias se transmitiría a "4 distintos colores", uno por cada terminal: 400nm para el violeta, 660nm para el rojo, 700nm para un infrarrojo cercano, 5000nm para el infrarrojo medio.

B) TDMA (*Time Division Multiple Access* - acceso múltiple por división de tiempo) usa multiplexación por división de tiempo, en el caso de tener un canal de frecuencia y dividir el tiempo de transmisión en, por ejemplo, 4 ventanas de tiempo o ranuras de tiempo (time-slots) o turnos, una para cada terminal. Por ejemplo, los primeros 10 segundos transmite y recibe la terminal 1, los segundos 10 segundos transmite y recibe la terminal 2, los terceros 10 segundos transmite y recibe la terminal 3, los cuartos 10 segundos transmite y recibe la terminal 4 y en la siguiente ranura de tiempo la secuencia cíclica se repite, 1, 2, 3, 4 y luego nuevamente 1, 2, 3, 4, etc. Por ejemplo, GSM (*Global System of Mobile Communication*), tecnología celular de segunda generación (2G), emplea TDMA como el modo de acceso al canal, con un alcance máximo de 35Km.

C) CDMA (Code Division Multiple Access - acceso múltiple por división de código). En este caso, sólo quienes conocen el código pueden entender. Por ejemplo, UMTS (*Universal Mobile*

Telecommunications System), tecnología celular de tercera generación (3G), emplea CDMA como modo de acceso al canal con un alcance máximo de 8 Km.

D) SDMA (Space Division Multiple Access - acceso múltiple por división de espacio). Es equivalente a emplear distintas direcciones.

La capa DLL se dividió en dos subcapas: la MAC (*Media Access Control*) la cual permite la interacción entre la capa física y la capa DLL, y la subcapa LLC (*Logical Link Control*) la cual permite la interacción entre la capa DLL y la capa de red.

Específicamente para el caso de la multiplexación en la conmutación de paquetes (*packet switching*) encontramos 2 formas de acceder al medio, donde se requiere de protocolos MAC, que actúan en la capa 2 del modelo ISO/OSI o TCP/IP: CSMA/CD, un protocolo de la subcapa MAC de acceso múltiple empleado en IEEE 802.3, y el CSMA/CA, un protocolo definido para IEEE 802.11 [85].

Ejemplos de protocolos que trabajan en las capas 1 y 2 de ISO/OSI o de TCP/IP son: Ethernet, USB, Bluethoot, WiFi, etc.

IV.3.2.1 La dirección MAC de un host

PRÁCTICA 1: Una vez que los conceptos de trama y dirección MAC son claros teóricamente, se propone la siguiente práctica con el objetivo de que el lector refuerce los conceptos teóricos sobre la dirección MAC. Obtenga la(s) MAC de una "computadora", vía simulador, vía su equipo físico, sea este una computadora de escritorio (desktop), notebook, minibook, laptop, teléfono celular, televisor con conexión a internet, etc., [88].

Actividad 1- vía simulador: Acceda al simulador "Cisco Packet Tracer", el cual es gratuito y puede bajar vía internet a su computadora, explore sus principales bibliotecas de componentes. Acceda a un *end system* para obtener en la pestaña de configuración la MAC de su NIC.

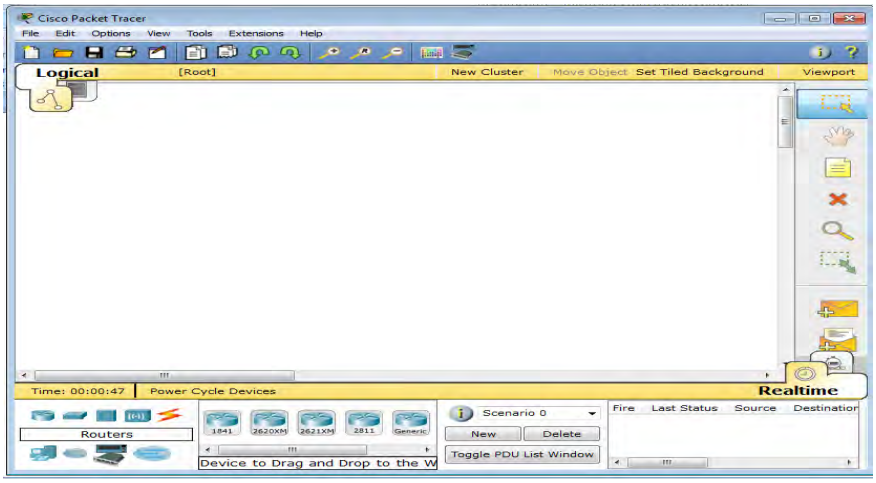


Fig. IV.8. GUI (Graphic User Interface) principal de ***Cisco Packet Tracer.***

Tome una computadora tipo desktop desde la biblioteca de *End systems* hasta el área de trabajo y abra con un doble *click* y observe la dirección MAC de la NIC de la computadora en cuestión.

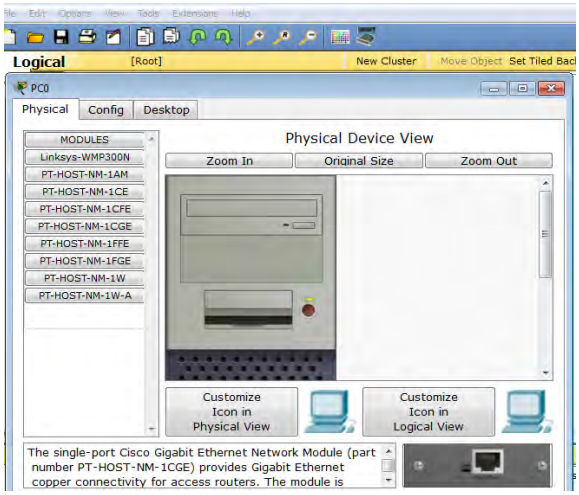


Fig. IV.9. Vista de un *End device*, computadora tipo desktop.

Ahora cambie a la pestaña de configuración gráfica CONFIG.

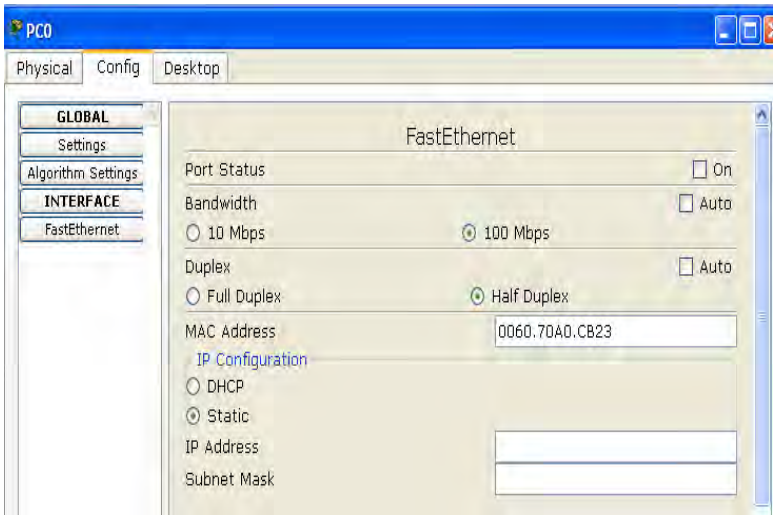


Fig. IV.10. La dirección MAC de la interfaz FE en una computadora del simulador está presente, pero no presenta el formato canónico.

Actividad 2- vía computadora: Acceda a la interface CLI del sistema operativo, por ejemplo en caso de que este sea Windows use CMD. Emplee el comando "ipconfig/all" para determinar la(s) direcciones MAC de la NIC(s) que contenga una computadora, lo indico en plural ya que en el caso de una laptop, notebook o minibook, por lo general tienen al menos la tarjeta de Ethernet y también la de WiFi (IEEE 802.11), como se indica en la figura siguiente.

```
C:\>ipconfig
Configuración IP
Nombre del host MILAB
Adaptador de Ethernet
Estado de los medios: conectados
Descripción: Realteck PCIe GBI family controller
Dirección física: 3C-07-71-55-9D-28
DHCP habilitado: si
Adaptador de LAN Inalámbrica WiFi
Estado de los medios: conectados
Descripción: BCM 4314 Wireless Network Adapter
Dirección física: BF-78-37-05-D8-92
DHCP habilitado: si
```

Fig. IV.11. Informe de IPCONFIG, la dirección MAC de la NIC Ethernet es 3C:07:71:55:9D:28 y la dirección MAC de la WNIC de WiFi es BF:78:37:05:D8:92

Actividad 3- vía teléfono celular: Acceda a la interface del sistema operativo de su teléfono celular, vaya a "ajustes" y en "acerca del teléfono" encontrará la dirección MAC WiFi.

Actividad 4: Resolver el cuestionario:

1. Indique la dirección MAC de la NIC de una computadora vía su simulador.

_____

2. ¿Puede una computadora tener varias direcciones MAC?
(SI / NO)_____. ¿Cuál es el motivo?

_____

3. Indique la dirección MAC de la NIC de su computadora.

_____

4. Indique la dirección MAC de la WNIC de su computadora (en caso de ser una Laptop, etc.)

_____

5. Si se desconecta una computadora de su cable de red o se le desconecta de una red inalámbrica: indique el (los) caso(s) que aplique:

(A) La computadora cambia su dirección MAC.
(B) No aparece la dirección MAC de la computadora.
(C) La computadora no cambia su dirección MAC.
(D) La dirección MAC no depende de la computadora.
(E) Se pierde la dirección MAC.
Solución _____

IV.3.3 La capa de red y los protocolos ARP e ICMP

La capa de red o capa 3 o capa de inter red (*Internetwork*) provee la conectividad y la selección del camino entre 2 sistemas huésped que pueden estar en redes separadas geográficamente. Los switches de capa 3 y los routers usan direcciones MAC, también llamadas direcciones físicas, de 48 bits y direcciones IP, también llamadas lógicas, de 32 bits para determinar el camino que deben seguir los paquetes desde su origen hacia su destino. Algunos protocolos para esta capa son: IPv4, IPv6, ARP, RARP, ICMP. En la capa 3 existe tráfico de paquetes, así como en la capa 2 existe tráfico de tramas, así como en la capa 1 existe tráfico de bits.

El protocolo ICMP (*Internet Control Message Protocol*- protocolo de mensajes de control de internet) es el protocolo que usa IP para reportar errores y mensajes de control en la capa de red. El protocolo ARP (*Address Resolution Protocol* – protocolo de resolución de direcciones) se emplea para hacer un mapa dinámico de las direcciones IP o lógicas de la capa 3 de internet a las direcciones MAC o físicas de la capa 2 en las redes LAN/MAN, para lo cual las redes deben soportar un tipo de comunicación *broadcast, para lo cual* usa la tabla ARP. Por su parte el protocolo RARP (*Reverse Address Resolution Protocol* – protocolo de resolución de direcciones inverso) usa un *end system* para encontrar su propia dirección IP, al mapear una dirección física hacia una dirección lógica. Si dividimos a la capa 3 en dos subcapas, una alta y una baja, el protocolo ICMP pertenece a la subcapa superior que interactúa con la capa de transporte; mientras que los protocolos ARP y RARP pertenecen a la subcapa inferior que interactúa con la capa DLL [80, 84, 85].

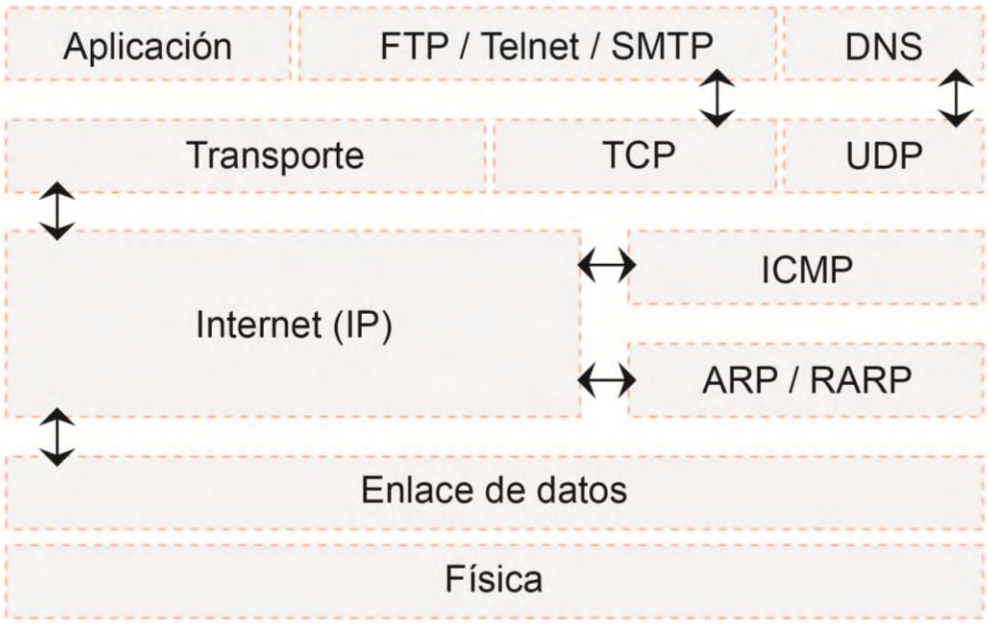


Fig. IV.12. Protocolos de capa 3 interactuando con capa 2 y capa 4 vía el protocolo IP.

Para agrupar los *host* dentro de redes, el protocolo IPv4 empleó una dirección lógica de 32 bits y se definieron direcciones IP dentro de clases de redes, para lo cual se definieron 5 clases de redes: A, B, C, D, E. La figura IV.13 indica el rango de direcciones IP públicas para host dentro de las clases A, B y C. La clase D se emplea para la comunicación *multicast* y la clase E se emplea para experimentación [98].

Clase	Rango de direcciones IP públicas para hosts	Rango de direcciones IP privadas para hosts	Máscaras de subred "Natural"
A	**RED** . host . host . host		255.0.0.0
	$2^7 - 2 = 126$ Redes:	$2^{24} - 2 = 16{,}777{,}214$ host	
	1.0.0.1 - **126**.255.255.254	**10**.0.0.1 - **10**.255.255.254	
B	**RED** . **RED** . host . host		255.255.0.0
	$2^{14} = 16{,}384$ Redes:	$2^{16} - 2 = 65{,}534$ host	
	128.0.0.1 - **191.255**.255.254	**172**.16.0.1 - **172**.31.255.254	
C	**RED** . **RED** . **RED** . host		255.255.255.0
	$2^{21} = 2{,}097{,}152$ Redes:	$2^8 - 2 = 254$ host	
	192.0.0.1 - **223.255.255**.254	**192**.168.0.1 - **192**.168.255.254	
D	**224.0.0.0 - 239.255.255.255**	**MULTICAST**	

Fig. IV.13. Rango para las direcciones IPv4 públicas y privadas para *host* para las clases A, B y C.

Observe que para la "clase A" no se consideran las redes (**0.**0.0.0) y la (127**.**0.0.0), de allí que a 128 se le quiten 2 y quede un total de 126 redes. Y para el caso de los host, no se consideran aquella con terminación (0) la cual indica la red y aquella con terminación (255), reservada para broadcast.

La dirección 127.0.0.1 se emplea para el *localhost*, es decir, cuando se hace referencia a la dirección del mismo host que una persona este empleando, por ejemplo cuando un host se destina a ser un servidor consultamos que este servidor este activado colocando en un browser "http://localhost" o http://127.0.0.1, en este caso los paquetes no salen hacia una LAN se redirigen hacia la misma computadora que los generó como un "bucle de retorno". En una computadora se puede preguntar a la misma computadora el nombre que se le ha dado a ese host (*local host*) vía el sistema operativo mediante el comando "hostname".

El ICANN (*Internet Corporation for Assigned Names and Numbers*) es el organismo a cargo de asignar direcciones públicas de IP [las direcciones IP para los equipos conectados directamente a la red pública de Internet]. El ICANN remplazó al IANA (*Internet Assigned Numbers Agency*) en 1998.

Clases	Máscara de subred en decimal	Máscara de subred natural en binario	Ej. de dirección IP con la máscara de subred en decimal
A	255.0.0.0	**11111111**.00000000.00000000.00000000	10.1.2.20/8
B	255.255.0.0	**11111111.11111111**.00000000.00000000	172.1.5.30/16
C	255.255.255.0	**11111111.11111111.11111111**.00000000	192.168.0.10/24

Tabla IV.4. Direcciones IP para host y su respectiva máscara de subred natural para IPv4.

Con la finalidad de ejemplificar el empleo de la dirección MAC o dirección física (en L2) y de la dirección IP o dirección lógica (en L3), a continuación se muestra la topología de una red casera típica, que usa direcciones IP privadas, en la que conviven los estándares IEEE 802.3 (Ethernet) para computadoras de escritorio o portátiles, televisores y componentes de juegos; y la IEEE 802.11 (WiFi) para computadoras portátiles, teléfonos celulares y tabletas. El *modem router* que le provee al usuario su ISP, por lo general toma la dirección 192.168.1.254, como en la figura IV.14.

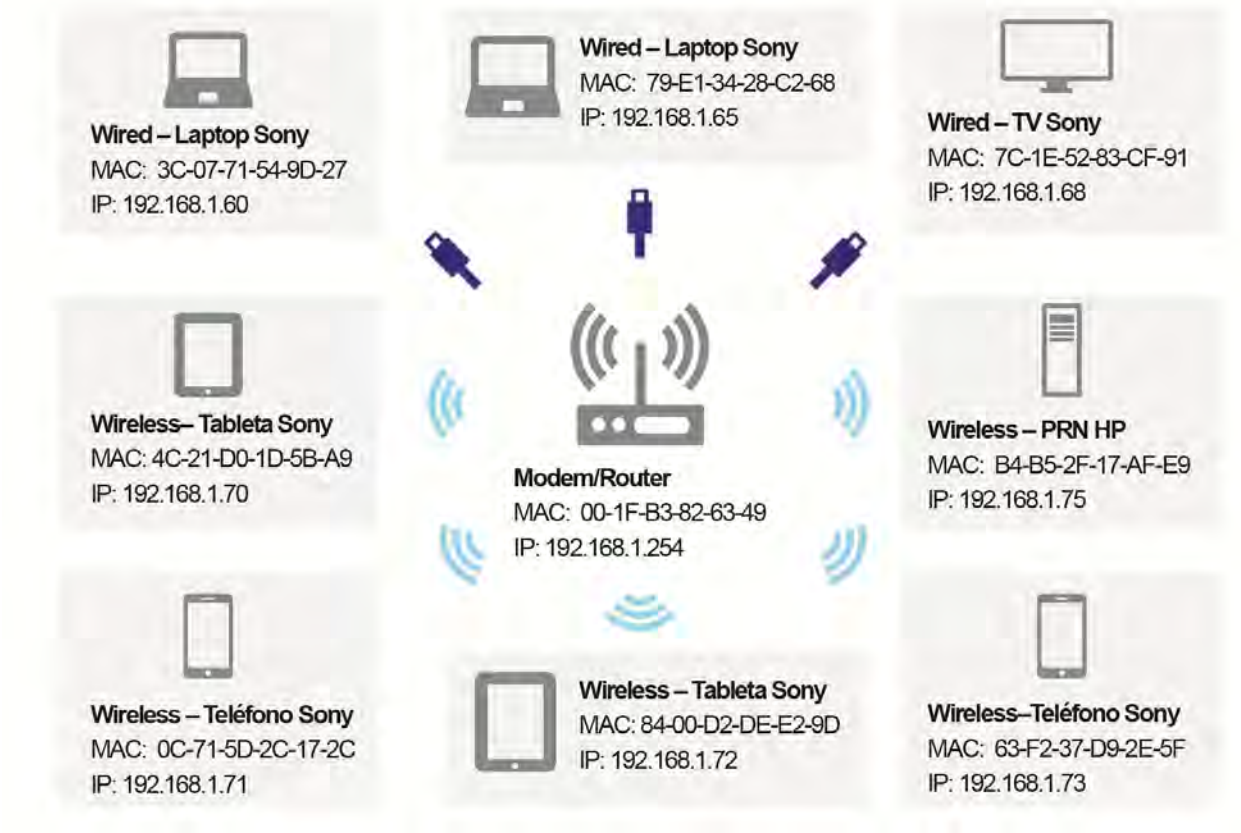


Fig. IV.14 Ejemplo de topología de una red casera en la que conviven los estándares IEEE 802.3 (alámbrico) e IEEE 802.11 (inalámbrico).

Ya sea que nos conectemos a Internet vía alámbrica mediante Ethernet o vía inalámbrica vía **wifi**, es necesario tener claro cuál es la dirección IP que tenemos asignada, para ello empleamos el comando **ipconfig**, como se indica en la figura IV.15.

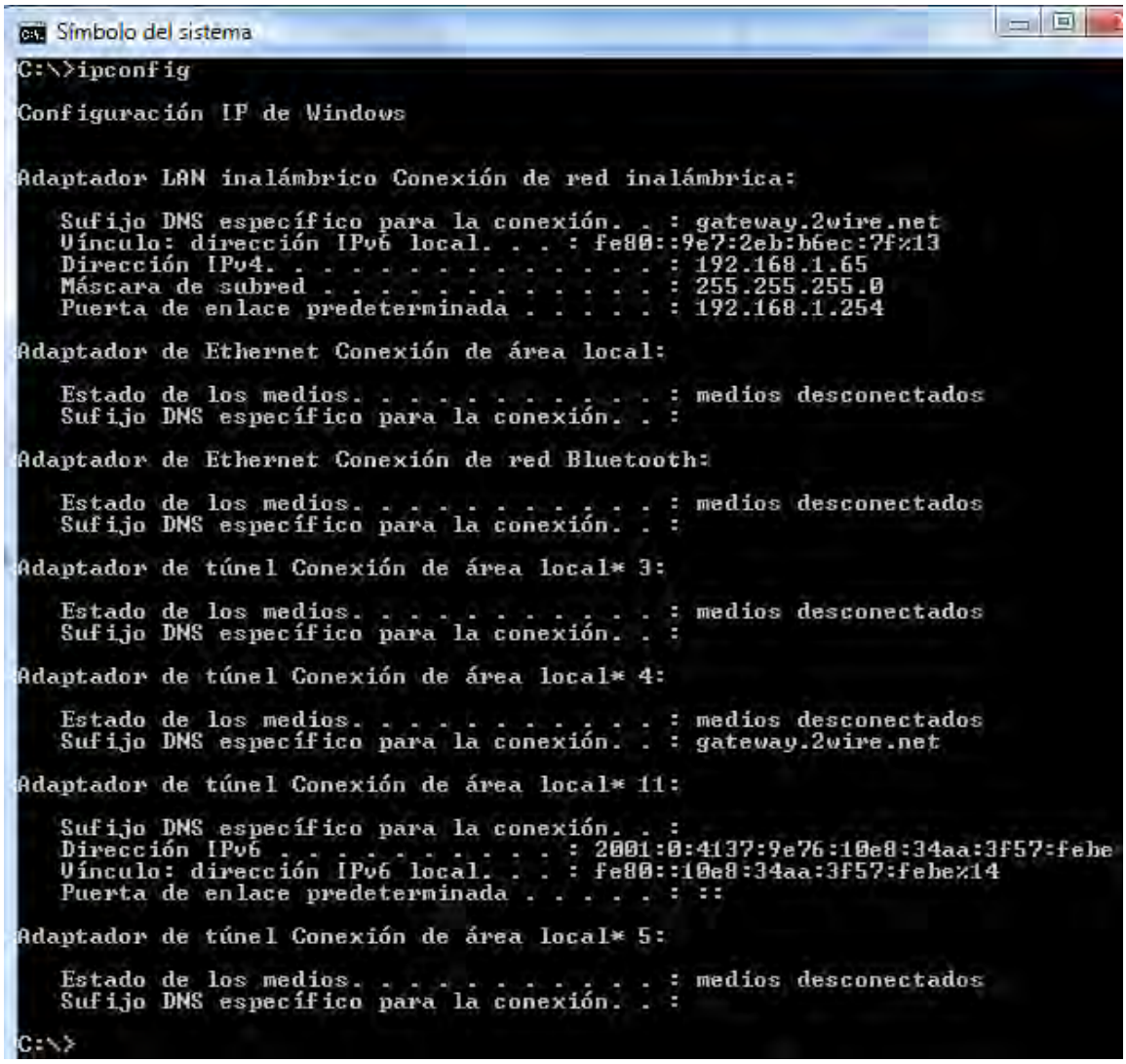


Fig. IV.15 Obtención de las características de conectividad vía *ipconfig*.

El comando "ipconfig" nos indica en este caso que existe una conexión vía *WiFi*, y que el nombre del router de infinitum empleado lleva por nombre "gateway.2wire.net**";** en realidad la conexión se hace vía un modem ADSL (*Asymmetric Digital Subscriber Line*- Línea del suscriptor de tipo digital y asimétrica) configurado como router. La ADSL es una tecnología que se emplea para conectar computadoras a Internet vía los 2 alambres de la infraestructura de telefonía en la llamada última milla, es decir, desde la central telefónica del proveedor de telecomunicaciones hacia la casa del abonado o suscriptor del servicio, de allí el nombre.

A continuación se presenta una práctica que permitirá reforzar el funcionamiento de los protocolos ARP e ICMP al enviar un ping entre 2 host.

A manera de resumen emplearé diagrama de clases de UML (*Unified Modeling Language)* para resaltar aquello que se requiere al conectar una red LAN. Todo host conectado a una red,

tiene un nombre, una dirección MAC fija, una dirección IP, una dirección de máscara de subred y una dirección IP de su gateway. Un diagrama de clases UML puede incluir:

a) Las clases usadas en el sistema.
b) La relación estática ente las clases
c) Los atributos (variables) y métodos (operaciones) de cada clase
d) Las restricciones de conexión entre los objetos.

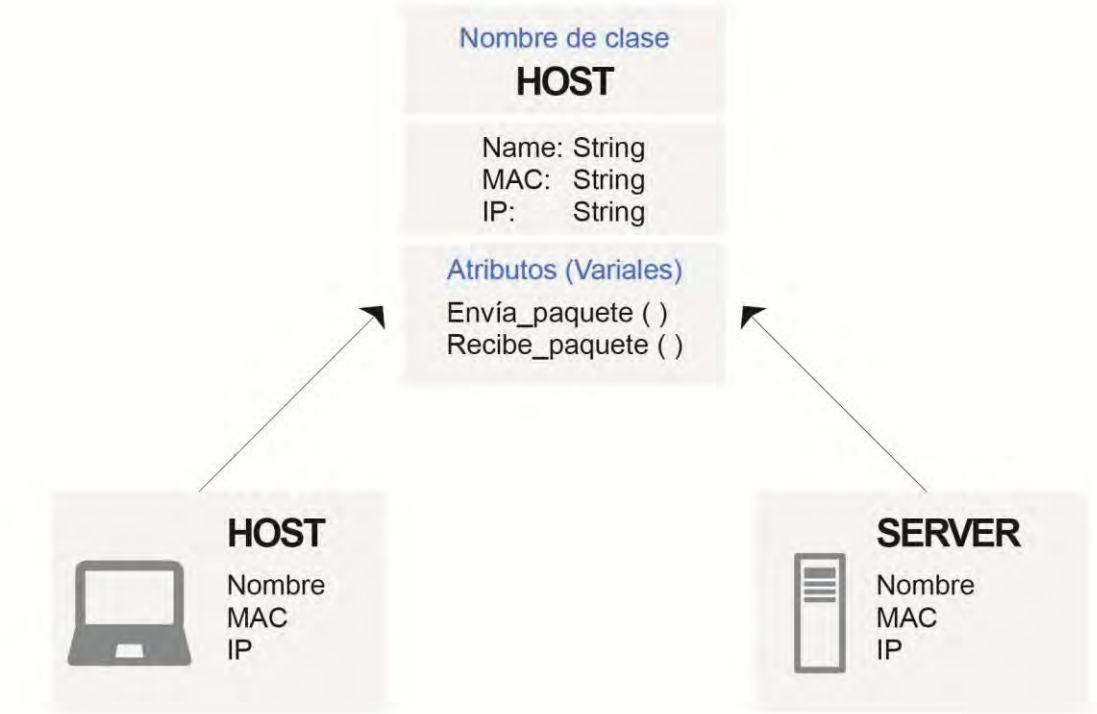


Fig. IV.16. Diagrama de clases para hosts. Los atributos o variables tienen nombre, tipo y valor inicial.

IV.3.3.1 Direcciones físicas y lógicas en un host

PRÁCTICA 2: El objetivo es que el lector se familiarice con las direcciones física y lógica de su computadora, así como la máscara de subred natural para cada una de las tarjetas de red con las que cuente un determinado host, el cual puede ser su computadora de escritorio, portátil, tableta o teléfono celular.

Actividad 1: Acceda vía CLI a la línea de comandos del sistema operativo y obtenga vía el comando "ipconfig", las direcciones MAC e IP de cada una de las tarjetas de red con las que cuenta su host, ya sea computadora de escritorio o portátil. Replique para obtener una pantalla como la fig. IV.15

Actividad 2: Acceda al panel de control en el sistema operativo Windows o equivalente en otro sistema operativo para acceder a las funciones de red bajo el protocolo IPv4, como se indica en la figura IV.17.

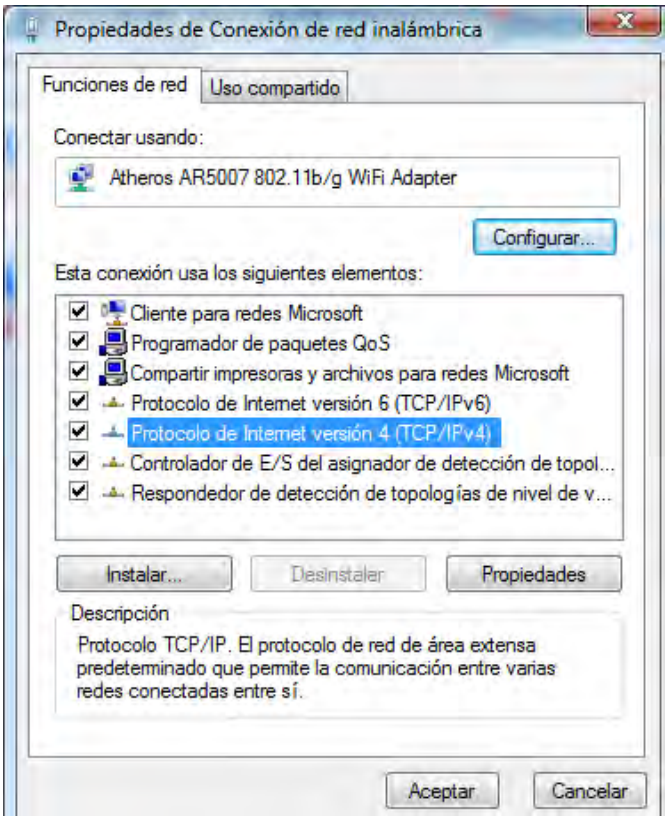


Fig. IV.17. Selección del protocolo TCP/IP v4 y activación de las propiedades.

De allí obtenga las propiedades del protocolo IPv4 como se muestra en la figura IV.18 y observe los campos que corresponden la dirección IP, la máscara de subred y el Gateway o puerta de enlace que corresponde la dirección que tiene asignado un determinado *modem router o router* en una determinada red.

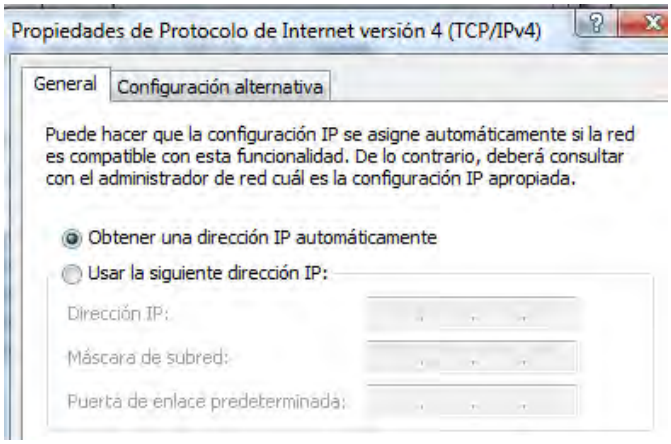


Fig. IV.18. Este resultado se da ya que la configuración de IP se asigna automáticamente.

Ahora replique para obtener las pantallas iguales o similares a aquellas de las figuras IV.17 y IV.18.

IV.3.3.2 Comunicación en una red punto a punto vía Ethernet

PRÁCTICA 3: El objetivo es que el lector emplee dos computadoras personales y pueda realizar la comunicación entre ambas, para lo cual debe conectarlas con cable UTP. Para conectar las 2 NIC, configure las direcciones IP en cada computadora, verifique que es posible la conectividad mediante un "ping" y finalmente haga una transferencia de archivos.

Actividad 1- vía simulador: Acceda al simulador para crear una red P2P (Peer To Peer- punto a punto) conectándolas vía Ethernet como se muestra en la figura IV.19.

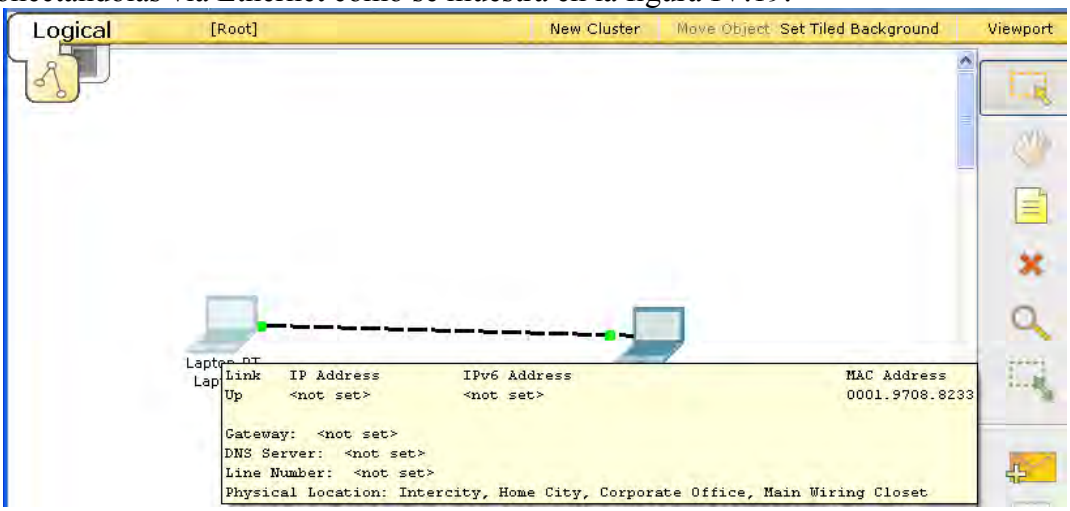


Fig. IV.19 Conexión entre 2 computadoras y vista de sus respectivas MAC y puertos activados, pero sin IP configurada.

Si ahora deseo enviar PDU de una a otra me indicará el error "puerto no funcional"

Actividad 2-Vía simulador: Configurar la IP y máscara de red para ambas computadoras. Ejemplo: Si se trata de una 192.168.1.1, su máscara de red será 255.255.255.0. La otra PC podría ser 192.168.1.2, misma subred. Observe la figura IV.20.

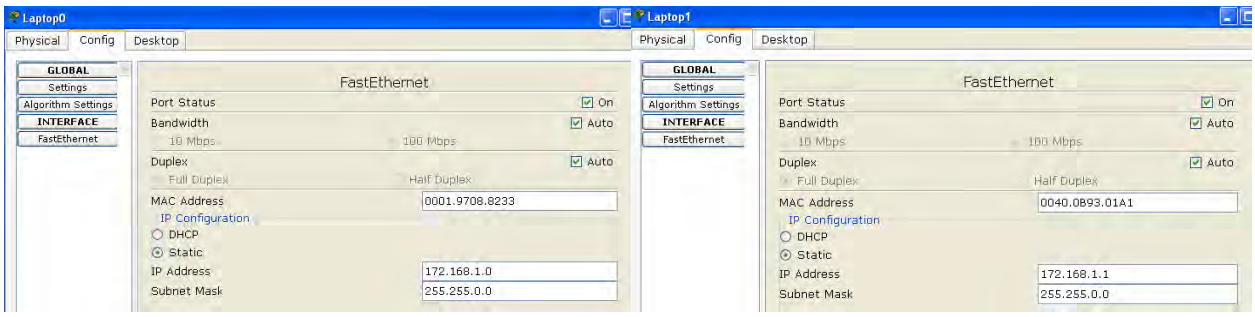


Fig. IV.20 "Configuración" de IP y su máscara de subred

Actividad 3-Vía simulador: Enviar paquetes PDU simples desde una PC a otra y rastrear todos los movimientos que ocurren durante el encapsulamiento y des-encapsulamiento; considere protocolos empleados, en cada capa, tramas y paquetes. Observe la figura IV.21.

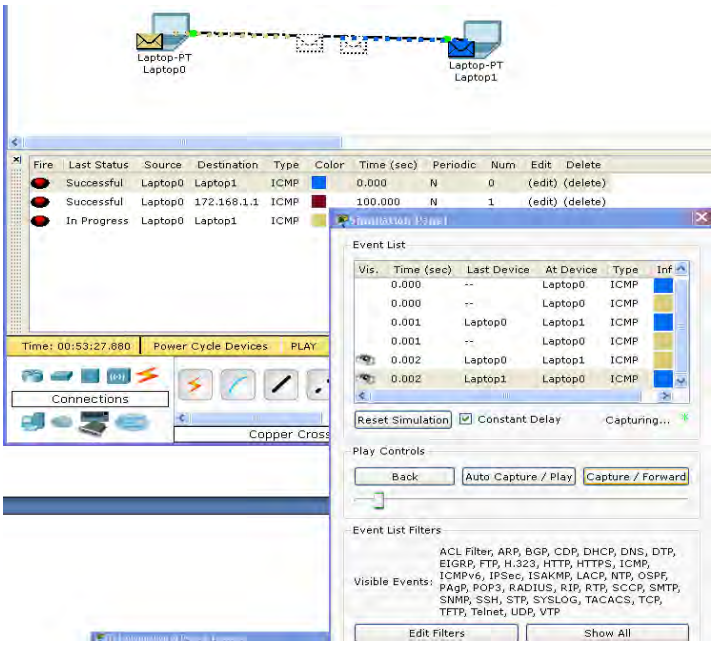


Fig. IV.21 El panel de simulación muestras la lista de eventos y la captura de paquetes, de modo que se observa paso a paso la transferencia de paquetes.

La figura IV.22 muestra el proceso de encapsulamiento, el cual inicia en la capa 3 con el proceso ICMP, que usará al protocolo ICMP. Observe la secuencia en las figuras IV.23 a IV.28.

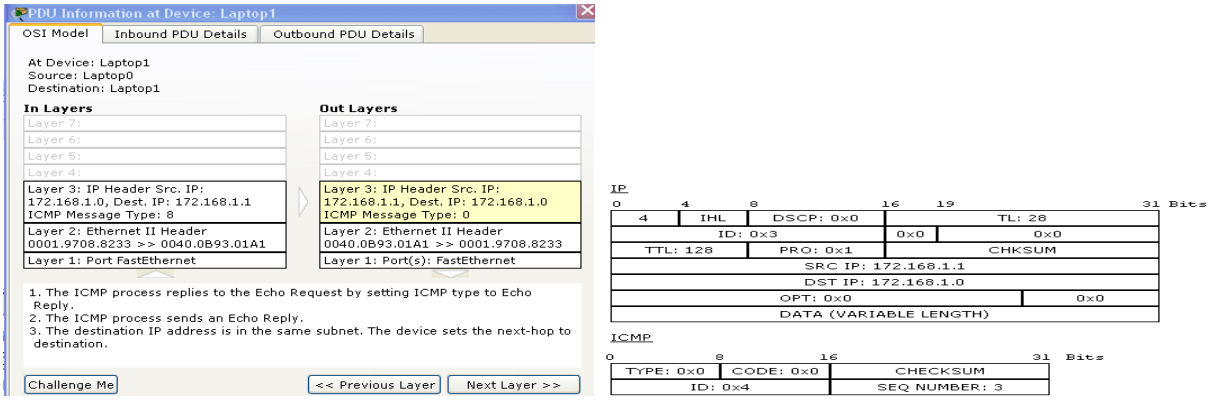


Fig. IV.22 Mapeo del encapsulamiento y des-encapsulamiento durante el envío de paquetes. La figura muestra el encapsulamiento de un paquete ICMP en la capa 3 (Out Layers), el cual es procesado mediante el proceso llamado ICMP. En la pestaña de "**Inbond PDU Details**" se observa cómo se conforma el paquete.

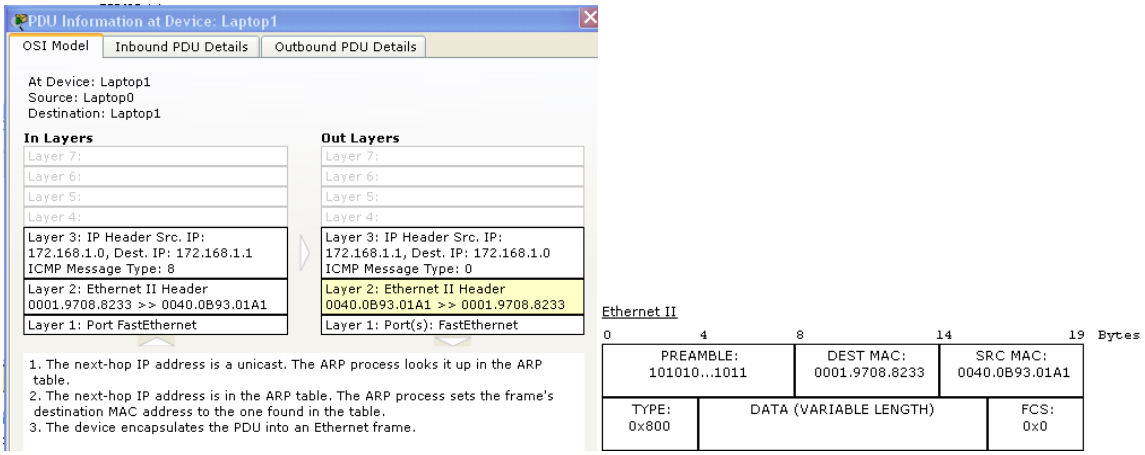


Fig. IV.23 Encapsulamiento en la capa 2. Se encapsula el PDU dentro de una trama Ethernet II y se muestra la estructura de la trama.

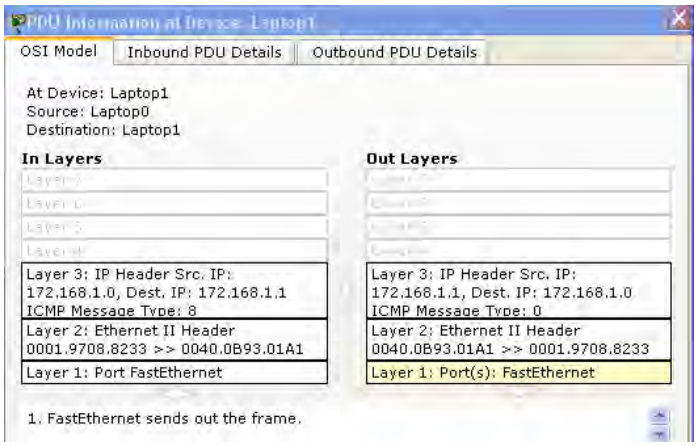


Fig. IV.24 La trama generada en la capa 2 se envía a través de la capa 1.

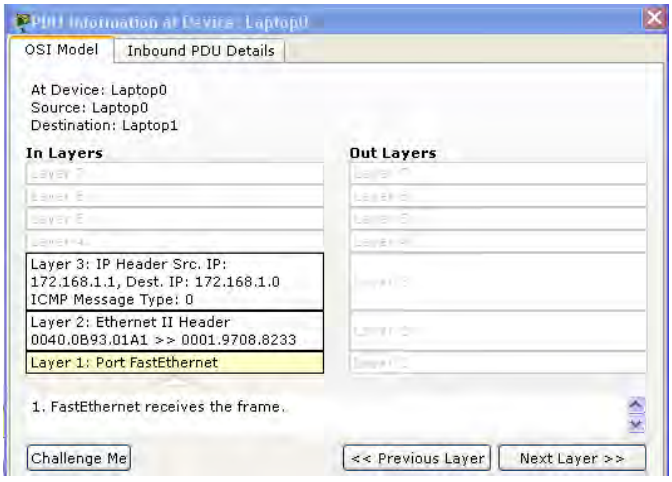


Fig. IV.25 Mapeo del des-encapsulamiento en la capa 1 del host destino: La trama o frame enviada vía capa 1 (medio físico y puerto FE de la NIC) llega a su destino y para subirla a la capa 2 requiere el proceso de des-encapsulamiento.

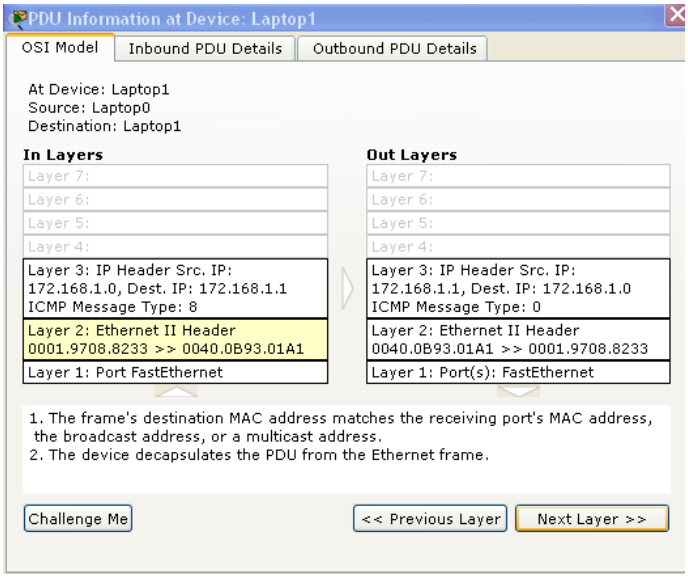


Fig. IV.26 Mapeo del desencapsulamiento en la capa 2 del host destino: Se des-encapsula el PDU a partir del frame Ethernet II. (En la trama el type es ICMP)

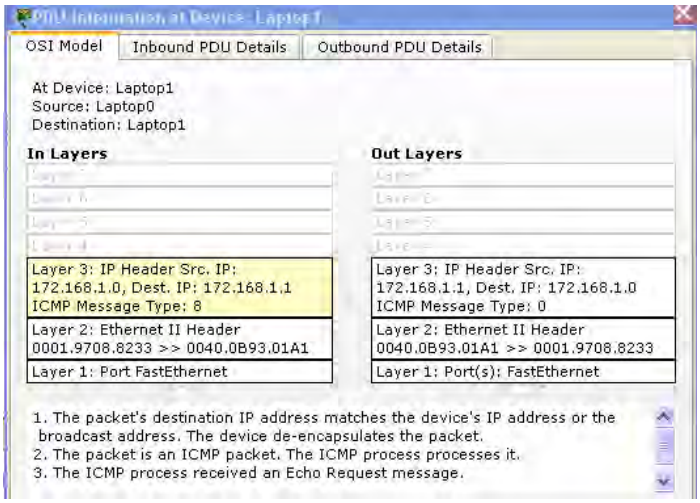


Fig. IV.27 Mapeo del des-encapsulamiento en la capa 3 del host destino: El paquete PDU enviado de la capa 2 a la capa 3 lo toma el proceso ICMP, el cual procesa al paquete, tal PDU es un paquete ICMP.

Finalmente se observa en la simulación tipo "realtime" como exitoso.

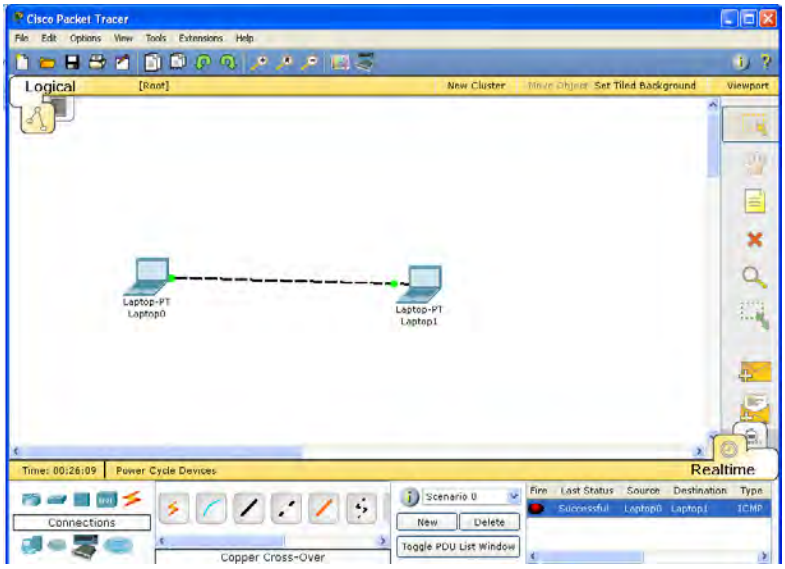


Fig. IV.28 Simulación de la transferencia de paquetes exitosa.

Actividad 4- práctica: Ahora pase de la teoría y la simulación a la práctica, envíe ping de una máquina a otra y viceversa, para comprobar la conectividad, y haga alguna transferencia de archivos.

Actividad 5- práctica: Cambie la dirección IP de una computadora o su máscara de red y trate de enviar paquetes o de probar con "ping". Anote sus resultados y explique. Finalmente anote sus conclusiones.

Actividad 6- práctica: Obtenga el nombre de su host.

IV.3.4 La capa de transporte y los protocolos TCP y UDP

La capa de transporte o capa 4 establece, mantiene y cierra los circuitos virtuales apropiadamente entre aplicaciones desde una perspectiva lógica usando "puertos". Para enviar la información la segmenta desde el host que envía la información con la finalidad de reducir los errores de transmisión recepción para reensamblarlos en el host que recibe la información. La capa 4 provee la entrega ya sea segura o no segura (conexión *end-2-end)* de datagramas UDP (*User Data Protocol*). El datagrama incluye un pseudo-encabezado que incluye la dirección destino y si el equipo destino ve que se mandó información a un puerto inactivo regresa la señal de inalcanzable. El UDP (sin conexión) no garantiza la entrega de datos debido a que los paquetes (datagramas) se pueden perder duplicar o entregar erróneamente, tampoco recupera paquetes perdidos o corruptos, sin embargo, es rápido. Algunos protocolos para esta capa son: TCP; UDP; RSVP; DCCP y SCTP. En la capa 4 existe tráfico de "datagramas" a través de los puertos, así como en la capa 3 existe tráfico de "paquetes". La capa 4 aísla las capas superiores de los detalles de cómo llegan los datos de un *host* a otro. Además la capa 4 provee los siguientes servicios a la capa de sesión: Establecimiento de conexión en L4, liberación de la conexión L4 y la transferencia de datos. El diagrama de la figura IV.29 muestra la interacción entre algunos protocolos de las capas 3, 4 y 5 [85].

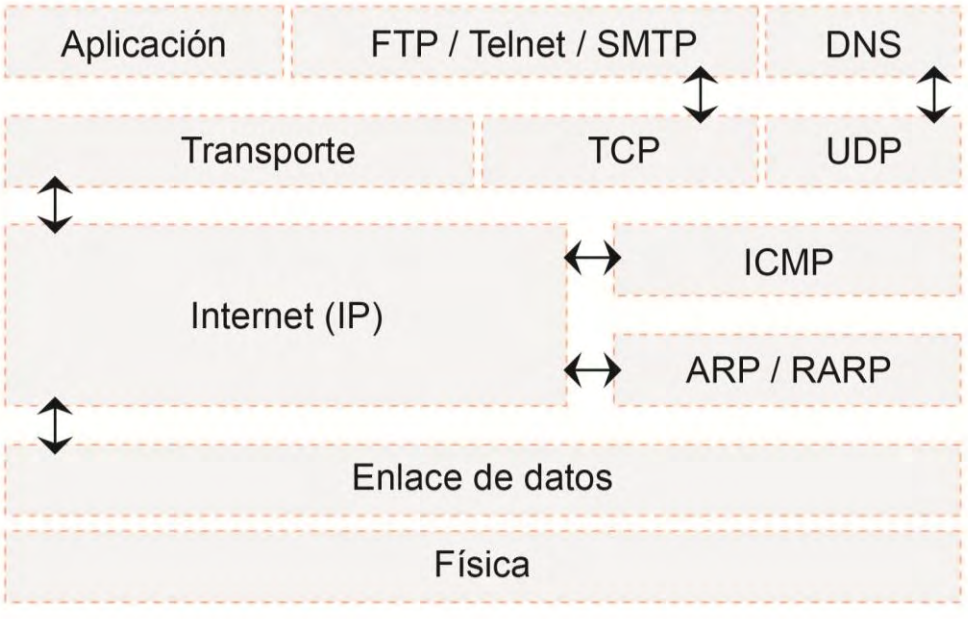


Fig. IV.29. Protocolos de capa 4 interactuando con capas 3 y 5, vía los protocolos TCP y UDP.

IV.3.5 La capa de sesión y sus protocolos

La "capa de sesión o capa 5" en ISO/OSI establece o inicia, administra o mantiene activas y finaliza las sesiones adecuadamente entre dos host que se comunican. También sincroniza el diálogo entre las capas de presentación de los dos huéspedes (*host*) y administra el intercambio de datos. Por ejemplo, los servidores *web* tienen muchos usuarios, de modo que hay muchos procesos de comunicación abiertos en un determinado momento, entonces es importante tener un registro de qué usuario se comunica por qué camino. Además de regular la sesión, esta capa ofrece elementos que proveen la eficiencia en la transferencia de datos, clases de servicio (CoS) y reporte de excepciones de la capa de sesión, presentación, y problemas en la capa de aplicación mediante la separación de datos a través del control de diálogo. La figura IV.30 muestra el envío de una señal de sincronía para establecer una sesión y su acuse de recibido (ACK), aunque no se incluye en la figura, para cerrar una sesión se envía una señal de "fin" y se espera por el correspondiente acuse de recibido.

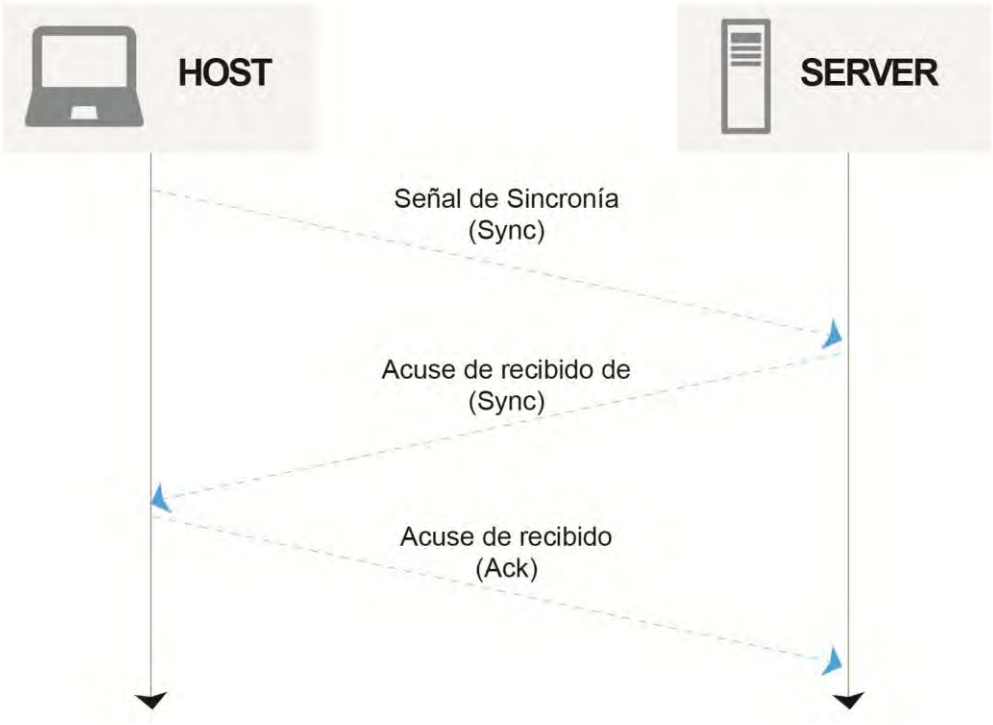


Fig. IV.30. Estableciendo el inicio de sesión.

Los servicios de esta capa se usan en ambientes de aplicación que emplean protocolos RPC (*Remote Procedure Calls*). Las primeras implementaciones a las invocaciones remotas se dieron en la red de ARPANET en la década de los años 80. Los primeros en implementarlas fueron

Xerox y SUN para el sistema operativo UNIX, de tal modo que se integró al NFS (*Network File System*). En el caso de Java, en la actualidad lo conocemos como Java RMI (*Remote Method Invocation*), la cual provee una funcionalidad similar a la de los métodos de UNIX-RPC. Debe considerar que un host puede tener varias sesiones, es decir, puede comunicarse con otros host o con otros servidores. Al usar el browser la gente abre varias "pestañas" y abre diferentes páginas *web*, ya que se está comunicando con varios servidores o con otros hosts. Las aplicaciones incorporan funcionalidades de las capas 5, 6 y 7, como los exploradores *web* o *browsers* o clientes de correo electrónico vía GUI o CLI. En internet se usa el protocolo TCP/IP. Los protocolos de la capa de aplicación (5, 6 y 7 en ISO/OSI) más empleados están indicados en la tabla IV.6.

Protocolo	Descripción	Puertos L4
DNS (Domain Name Service)	Protocolo de servicio de nombres de dominio	53
HTTP (Hypertext Transfer Protocol)	Protocolo para transferir archivos vía WWW	80
FTP (File Transfer Protocol)	Transferencia de archivo de manera interactiva, vía cliente por CLI o GUI	20 > datos 21> control
Telnet	Emulación de terminal, empleado para acceder a servidores y equipos de red vía remota	23
SMTP (Simple Mail Transfer Protocol)	Transferencia de correo electrónico y archivos adjuntos	25

Tabla IV.6. Protocolos de aplicación en TCP/IP.

Para emplear cada uno de los protocolos indicados, se requiere iniciar sesiones, por lo que se aplican los protocolos SIP y SCP. El SIP (*Session Initiation Protocol*) es un protocolo de comunicaciones de señalización usado para controlar las sesiones de comunicación multimedia como voz y video sobre IP. El SCP (*Session Control Protocol*) es un protocolo que permite a un servidor y cliente tener múltiples conversaciones sobre una conexión TCP [88].

IV.3.6 La capa de presentación y sus protocolos

La “capa de presentación o capa 6” en el modelo ISO/OSI, asegura que la información enviada a la capa de aplicación de un sistema sea legible por la “capa de aplicación o capa 7” de un sistema a la capa 7 de otro sistema. Para ello presenta la información que procesa al realizar alguna de sus 3 funciones principales, la encriptación de datos, la codificación y conversión de datos o servicios de traducción y la compresión.

1. “La encriptación de los datos” se emplea al transmitir datos para que se desencripten a la llegada al equipo destino.
2. “La compresión de datos” se hace en el equipo origen, tal que se puedan descomprimir en el equipo destino.
3. “La codificación y conversión de datos (traducción)” de la capa de aplicación se realiza para garantizar que los datos del equipo origen se puedan interpretar por la aplicación adecuada en el equipo destino. Por ejemplo: cuando una computadora A se comunica con otra B, se puede dar el caso de que la computadora A emplee el código EBCDIC para representar caracteres, mientras que la B emplee el código ASCII para representar los mismos caracteres, entonces es necesario que la capa de presentación realice la traducción entre múltiples formatos de datos, para lo cual usa un formato común.

Para que las computadoras puedan manipular a los textos, los gráficos y al audio se requiere de la codificación. “Codificar” es un proceso mediante el cual se traduce la información de un lenguaje a otro, usando un diccionario de equivalencias. Mientras que un “código” es un sistema de signos, símbolos, etc, generalmente convencional y arbitrario que sirve como medio de comunicación o que transmite determinada información. Cualquier persona ha oído hablar de códigos, como el código postal, el código genético, el código Morse, los códigos de señales, etc. La tabla III.7 muestra el código Morse y un ejemplo clásico.

Los códigos que nos interesan son aquellos usados por las computadoras, mismos que por lo general son códigos binarios. Podemos encontrar códigos para la detección y corrección de errores en la transferencia de información desde una unidad funcional a otra de la computadora. Ejemplos: desde la memoria principal hasta el procesador, de algún medio masivo de almacenamiento, como un disco compacto o disco duro o una cinta hacia la memoria principal o la CPU. También podemos encontrar códigos para el intercambio de la información para la comunicación de datos en las computadoras; estos son los códigos tratados en esta sección.

A -*	B -***	C-*-*	D-**	E*	F**-*
G--*	H****	I**	J*---	K-*-	L*-**
M--	N-*	**O---**	P*--*	Q--*-	R*-*
S***	T-	U**-	V***-	W*--	X-**-
Y-*--	Z--**	1*---	2**--	3***--	4***-
5*****	6-****	7--***	8---**	9----*	0-----

Tabla IV.7. Código Morse. La palabra "SOS" se escribe "***/---/***"

A. **Códigos para textos:** El EBCDIC (***E**xtended **B**inary **C**oded **I**nterchange **C**ode* - código extendido para el intercambio decimal codificado en binario) es un código de 8 bits creado por IBM para representar caracteres como números; es un código muy usado en super, mainframes y midi computadoras. El código ASCII (***A**merican **S**tandard **C**ode for **I**nformation **I**nterchange* - código estándar estadounidense para el intercambio de información) es un código para representar caracteres en idioma inglés como números, donde a cada letra se le asigna un número; este código se usa en computadoras personales para representar texto, donde cada caracter tiene un equivalente decimal y hexadecimal. Los archivos almacenados en el formato ASCII se llaman archivos ASCII, y son populares entre los formatos de los editores de texto y procesadores de palabras. El código ASCII ha evolucionado por lo que encontramos 3 tipos principales de código ASCII, el estándar, el extendido y el ISO latín 1; el ASCII estándar es un código que usa 7 bits para cada caracter, de modo que podemos representar a (2^7) 128 caracteres (del 0 al 127), y los primeros 32 se usan como caracteres de control de comunicaciones para transferir información con otras computadoras o impresoras; la tabla III.8 ejemplifica tal código. Dadas las necesidades de colocar más caracteres se creó el ASCII extendido, este es un código que usa 8 bits para cada caracter, de modo que podemos representar a (2^8) 256 caracteres (del 0 al 255), es por ello que podemos tener conjuntos de caracteres más grandes, sobre todo para representar caracteres que no pertenecen al inglés, letras mayúsculas, minúsculas, números, signos de puntuación, símbolos gráficos y símbolos matemáticos. Un estándar más universal es el ISO Latín 1, el cual es usado por muchos sistemas operativos y navegadores de la Web. El UNICODE busca ser un código universal, es estándar para representar caracteres y enteros, usa 16 bits que puede representar a 65,536 (2^{16}) caracteres únicos. Conforme la globalización avanza UNICODE va reemplazando al código ASCII como el formato de codificación de caracteres estándar.

Decimal	código	Ingles	Español
00	NUL	Null	Caracter nulo
01	SOH	Start of heading	Inicio de cabecera
04	EOT	End of transmission	Fin transmisión
05	ENQ	Enquiry	Interrogación, consulta
06	ACK	Acknowledge	Acuse de recibo
07	BEL	Bell(audible signal)	Timbre
08	BS	Backspace	Retroceso
09	HT	Horizontal tab	Tabulación horizontal
13	CR	Carriage return	Retorno de carro
24	CAN	Cancel	Cancelación
27	ESC	Escape	Cambio, escape
32	SP	Space	Espacio

Tabla IV.8. Caracteres de control para ASCII estándar

B. **Códigos para gráficos:** Los gráficos, al igual que los textos, las fotografías e imágenes se deben pasar a un formato que la computadora pueda manipular, entre ellos están los gráficos de mapas de bits (filas y columnas de bits) y los gráficos vectoriales (usan ecuaciones matemáticas y son escalables) que presentan mejor calidad. Los formatos típicos para mapas de bits son: BMP (*bitmap*), TIFF (*Tagged Image File Format*) y GIF (*Grafical Interchange Format*); mientras que los gráficos vectoriales son: EPS (*Encapsulated Postscript*), WMF (*Windows Metafile Format*), HPGL (*Hewlett Packard Graphics Language*). Para los gráficos en movimiento existen formatos para compresión de video: formato AVI (*Audio Video Interleave*), Quicktime y MPEG (*Motion Pictures Expert Group*). Además existen estándares como MIME (*Multipurpose Internet Mail Extensions*) usados para codificar datos como imágenes, en texto ASCII, para su transmisión a través del correo electrónico. Específicamente MIME se creó para permitir la transmisión de datos no ASCII a través de correo electrónico y para adaptarse a tipos y representaciones arbitrarias de datos. Cada mensaje MIME incluye datos que informan al recipiente del tipo de datos y de la codificación usada para convertir los datos en ASCII; por ejemplo, una imagen con formato GIF se puede convertir en su representación ASCII de 7 bits mediante la codificación *base64*, de modo que para ver la imagen, el

sistema de correo receptor debe convertir la codificación *base64* a binario y correr una aplicación que presente una imagen GIF en la pantalla del usuario.

C. **Códigos para audio:** Los formatos típicos para audio son *wav* (*wave* - forma de onda), formato de audio convencional por lo que generan archivos grandes y el formato MIDI (*Musical Instrument Digital Interface*) es un formato que almacena instrucciones para el sintetizador, no audio convencional y genera archivos de menor tamaño que el formato *wav*. También se aplicaron los algoritmos de MPGE para audio y se hicieron muy populares por su alta tasa de compresión, los formatos MP3 y MP4 [88].

IV.3.7 La capa de aplicación y sus protocolos

La "capa de aplicación o capa 7" de ISO/OSI, es la capa donde los programas de aplicación API (*Application Programming Interfaces*) interactúan directamente con el sistema operativo para proveer los servicios de red como la transferencia de archivos, emulación de terminal, impresión, mensajería, etc. No provee servicios a otra capa, pero si da servicio a las aplicaciones fuera del modelo OSI, por lo que al proveer la interfaz de usuario es la capa más cercana al mismo. Las capas superiores 5, 6 y 7 no tienen idea alguna sobre el direccionamiento de la red

IV.3.7.1 Aplicación para medir la velocidad de transferencia de datos

PRÁCTICA 4: El objetivo es que el lector emplee una aplicación que le permita conocer la velocidad a la que su computadora se conecta a internet en función del servicio contratado con su ISP.

Actividad 1: Acceda al medidor de velocidad de conexión a internet en Mbps, IFETEL, México http://www.micofetel.gob.mx/micofetel/medidor_de_velocidad [Última visita: junio de de 2014], la cual indica la dirección vía nombre de dominio de IFETEL- Instituto Federal de Telecomunicaciones, agencia gubernamental mexicana, para obtener los resultados de las mediciones del ancho de banda de su red así como su velocidad de bajada y subida de archivos, como se indica en la figura IV.31.

Fig. IV.31 Prueba de ancho de banda para una conexión residencial.

Actividad 2: Repita el ejercicio desde 10 ubicaciones diferentes y tabule sus resultados.

IV.4. Autoevaluación para el capítulo IV

1. Indique la función principal de una NIC o WNIC.

_____
_____

2. Mencione 3 ventajas de los modelos de referencia como ISO/OSI

1	
2	
3	

3. Describa la función de la capa física del modelo ISO/OSI

_____
_____
_____
_____

4. Describa la función de la DLL del modelo ISO/OSI

_____
_____
_____
_____

5. Indique los elementos que componen una dirección MAC y el número de bits para cada campo.

Nombre de campo	# bits

6. Complete los nombres de los campos para una trama Ethernet II o IEEE 802.3 y el número de bits empleados.

Nombre de campo	# bits

7. Invente una dirección MAC válida

8. Describa la función de la capa de Red del modelo ISO/OSI

_____
_____
_____

9. Indique el rango de direcciones IP públicas para *hosts* en las clases de redes indicadas.

Clase	Rango de direcciones IP para hosts
A	
B	
C	

10. Describa la función de la capa de Transporte - ISO/OSI

_____
_____
_____

11. Describa la función de la capa de Sesión - ISO/OSI

_____
_____
_____

12. Describa la función de la capa de Presentación - ISO/OSI

_____
_____
_____

13. Al crear una red punto a punto entre dos computadoras vía Ethernet. ¿Es necesario indicar la dirección IP del Gateway? Justifique su respuesta:

_____
_____

14. Indique un protocolo para cada una de las capas del modelo ISO/OSI

Capas	Protocolos
L1:Física	
L2	
L3	
L4	
L5	
L6	
L7	

CAPÍTULO V: LA ARQUITECTURA “CLIENTE–SERVIDOR”

V. La arquitectura “cliente servidor”

Una vez que las redes de computadoras se generalizaron, en la década de los años 80 (en México a mediados de los 90), los servicios FTP y de correo electrónico se hicieron de uso masivo gracias a las computadoras personales y los sistemas distribuidos, los cuales permitieron que la arquitectura “cliente servidor”, concebida en los 70, se convirtiera en la segunda gran ola de la computación desde los 80. En este capítulo daremos una vista a la “arquitectura cliente servidor”; se incluyen cuatro prácticas de laboratorio en las que se realiza la instalación y configuración básica de servidores, vistos como máquina real y como máquina virtual.

V.1. Software y sistemas operativos

El software se define como la suma total de los programas de cómputo, procedimientos, reglas, documentos y datos asociados, que forman parte de la operación de un sistema de cómputo [99]. Por su parte, los sistemas operativos controlan los recursos de una computadora y ofrecen la base sobre la cual se pueden escribir o ejecutar programas de aplicación. Los sistemas operativos se pueden clasificar según el criterio de ejecución como centralizados o distribuidos. Los sistemas operativos centralizados aplican para un solo procesador, eran típicos de los mainframes y también lo fueron de las computadoras personales, ejemplos de estos son: CP/M, MS-DOS, DR-DOS, MS-Windows, OS2, Unix, System 7 de MAC. Por su parte los sistemas operativos distribuidos y paralelos que aparecen ante cada usuario como si esta fuera una única computadora; ejemplos de sistemas operativos de este tipo son: *amoeba, mach, chorus, dce*.

Los sistemas operativos se pueden clasificar bajo el criterio del “número de usuarios que atienden”, en tal caso existen los “monousuarios” y los “multiusuarios”, éstos últimos, son capaces de proporcionar servicios a varios usuarios mediante sus terminales al mismo tiempo, dándole la sensación al usuario de que él es el único al que el sistema operativo está atendiendo. Existe el caso de los sistemas operativos multiusuario de tiempo compartido, en el que para un procesador dado, la atención a cada usuario, se divide a intervalos temporales.

Los sistemas operativos también se pueden clasificar por las tareas que realizan con el procesador, en tal caso se clasifican en “monotareas”, aquellos que ejecutan un solo proceso la vez y “multitareas” (multiprogramación), aquellos que pueden ejecutar más de un programa a la vez para un mismo usuario [100, 101, 102].

V.1.1 Sistema operativo UNIX

A) Años 60

En 1968 se liberó el SO *multics,* el cual fue escrito en el lenguaje de alto nivel PL/1, fue uno de los primeros en proporcionar un entorno multiusuario. En 1969 Ken Thompson desarrolló el SO UNICS (UNiplexed Information & Computing Service) tomando las mejores características de *multics.* UNICS originalmente se escribió en el lenguaje ensamblador (conjunto de primitivas que dependen de la arquitectura de la computadora) para la DEC-PDP-7 y posteriormente tomó el nombre de UNIX. En 1971 Dennis Ritchie creó el lenguaje de programación "*C"*, el cual es de alto nivel y de propósito general. En 1969 se transfirió UNIX a la PDP-11, modelos 20, 40, 45 y 70, cuyas arquitecturas son muy parecidas, sin embargo, surgió la necesidad de hacer a UNIX portable.

B) Años 70

En 1973 Thompson y Ritchie, reescribieron UNIX en lenguaje "C" en un 95%, el otro 5% se mantuvo en ensamblador. En 1975 los laboratorios Bell de AT&T ofrecieron, a un costo mínimo, el UNIX a las instituciones educativas, sin darles el código fuente, incluyendo la 5ta edición del manual de referencia. En 1978 surgió la séptima edición de UNIX, el llamado clásico, y con ella muchos clones. Las dos versiones principales de UNIX son el "UNIX System V" de AT&T y el "UNIX BSD" (Berkeley Standard Distribution).

C) Años 80

En 1983 A. Tanembaum creó el primer UNIX para microcomputadoras llamado MINIX (mini-UNIX); ese mismo año AT&T introdujo el UNIX System V, todo un estándar. En 1984 surgió el ambiente gráfico "xwindows" en UNIX, bajo el proyecto "Athenas" en el MIT de EEUU. Entre 1986 y 1988 BSD y AT&T liberaron sus nuevas versiones de UNIX y para 1988 IBM, DEC y HP formaron el OSF (*Open Software Foundation*), el cual buscó promover los sistemas abiertos en los sistemas operativos, a semejanza de lo sucedido en equipos electrónicos o *hardware*.

D) Años 90

En 1990 Richard Stallman, todo un personaje, creó la FSF (*Free Software Foundation*) y surgió la idea GNU empleada en lo que conocemos como software libre, el cual no significa necesariamente gratuito. Ese mismo año, ya que habían varias versiones de UNIX, se realizó la estandarización POSIX (*Portable Operating System Interface for Computer Environments*) con base en el "UNIX System V interface definition" de AT&T.

Algunas características de UNIX son: Transportabilidad, capacidad multiusuario; capacidad multitarea; sistema de archivos jerárquico; operaciones de entradas y salida independientes de los dispositivos; interfaz de usuario. Ésta ultima incluye al *Shell script* (guiones) que permite que UNIX también sea un lenguaje de programación.

Es muy común que el sistema operativo que usen los servidores sea UNIX o Linux, en cuyo caso es muy recomendable conocer y usar con habilidad los comandos básicos vía CLI, por lo que se recomienda practicar con los comandos "*ls, dir, cd, cd.., cd\, pwd, bin, get y put*", para poder navegar dentro de los directorios de un servidor. Los comandos "*put"* y "*get"* sirven para subir y bajar archivos respectivamente [103, 104].

V.2. Arquitectura cliente servidor en los sistemas de información

La arquitectura "cliente-servidor" es un modelo que se emplea en sistemas de información, en el que las transacciones se dividen en procesos independientes que cooperan entre sí para intercambiar información, servicios o recursos. Se denomina "cliente" (client) al proceso que inicia el diálogo o solicita los recursos, y "servidor" (server) al proceso que responde a las solicitudes. En este modelo, las aplicaciones se dividen de forma que el servidor contiene la parte que debe ser compartida por varios usuarios, y en el cliente permanece sólo lo particular de cada usuario, como se muestra en la figura V.1. El modelo nació en 1973, fue desarrollado por Xerox-PARC.

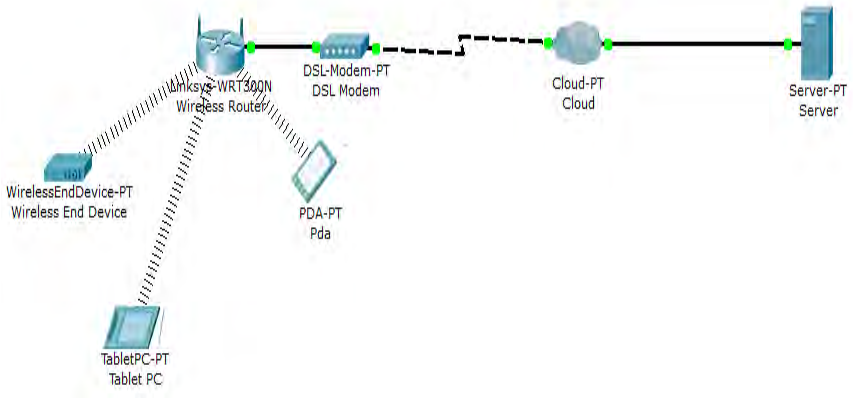


Fig. V.1 Principales componentes de una arquitectura "cliente-servidor".

Las principales características de la arquitectura "cliente- servidor" son:

1. El servidor presenta a todos sus clientes una interfaz única y bien definida.
2. El cliente no necesita conocer la lógica del servidor, sólo su interfaz externa.
3. El cliente no depende de la ubicación física del servidor, ni del tipo de equipo físico en el que se encuentra, ni de su sistema operativo.
4. Los cambios en el servidor implican pocos o ningún cambio en el cliente.

Con la finalidad de clarificar el modelo cliente servidor se empleará un "diagrama de casos de usos" en UML (*Unified Modeling Language*). Un diagrama de casos de uso es un escenario que describe cómo se va a usar un determinado software o hardware en una determinada situación; este cuenta con "actores", la "caja del sistema" y las "interacciones", las cuales se deben visualizar en un diagrama. Los casos de usos son parte del qué, es decir, del análisis, mas no del cómo, es decir del diseño. En cada diagrama sólo se debe colocar un sistema [104]. La figura V.2 ejemplifica el

modelo "cliente servidor" mediante un diagrama de casos de uso en UML. En este caso el sistema a analizar es un servidor; aunque un web browser también es un sistema, en sentido estricto, en este caso el sistema que se analiza es el servidor por lo que el web browser se convierte en un sistema externo o actor que necesita información. Cabe aclarar que al hablar del servidor como sistema, se hace referencia al servidor de software.

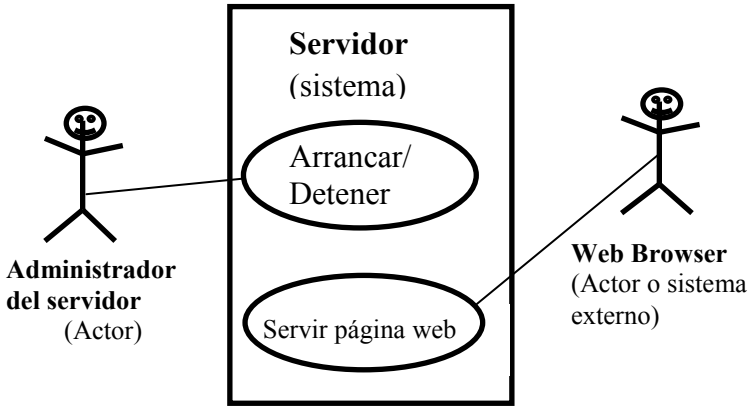


Fig. V.2 Diagrama de casos de usos para el sistema servidor.

En el caso del protocolo HTTP, éste genera una "conversación" o "petición-respuesta" para la comunicación entre un cliente y un servidor. La figura V.3 muestra el diagrama de casos de uso para el caso en el que un *web browser* es el sistema; en este caso el servidor es un actor o sistema externo.

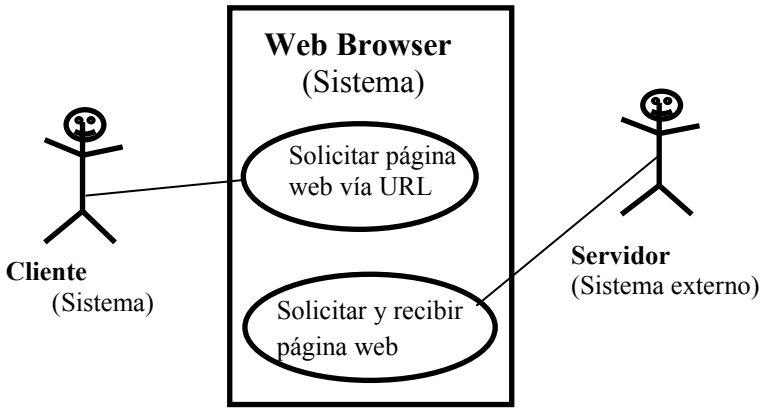


Fig. V.3 Diagrama de casos de usos para el sistema ***web browser***.

Un *WEB BROWSER* es una aplicación de software, la cual permite que un usuario visualice e interactúe con el contenido de una página web. Ejemplos de *web browsers* populares son: Netscape, Internet Explorer, Chrome, Mozilla, Firefox, Opera, Safari, entre otros. En muchas ocasiones es

necesario ampliar la funcionalidad de los *web browsers*, esto se hace con aplicaciones llamadas PLUG-INS o ADD-ONS, por ejemplo: *Flash Player, Java, Java scripts, Active Controls, Media Player, QuickTime Player, Shockwave Player, Real One Player y Acrobat Reader*, entre otros.

V.2.1 Intranet vs internet.

"Intranet" es una red privada que normalmente pertenece a una empresa u organización determinada. Las redes intranet, usan los mismos protocolos de "internet" y pueden incluir el mismo tipo de contenido; se usan normalmente para almacenar información interna de la empresa, como directivas o prestaciones a sus empleados.

Una de las diferencias que hay entre internet y una intranet es la que refiere a las direcciones de las páginas. En internet, las direcciones de las páginas web se componen normalmente de un nombre de dominio completo, en función de la forma en que el administrador haya configurado la red, por ejemplo: www.ieee.org. En intranet, el nombre de dominio completo, no suele ser necesario para obtener acceso a los sitios *web* y es posible acceder escribiendo solamente, por ejemplo: http://serviciosyprestaciones.

Dado que el administrador controla estrictamente la seguridad, la configuración de seguridad del contenido de la intranet puede ser menos restrictiva que la que se emplea para el contenido que proviene de internet, de allí que sea posible que un usuario observe una advertencia en las páginas *web* que consulte. Si la seguridad de la intranet está habilitada, un determinado *browser* reconocerá la diferencia entre las direcciones y usará la configuración de zona de seguridad apropiada, por lo que se requiere configurar el navegador para tener seguridad en la intranet.

V.3. Conexión a servidores

Cuando un usuario emplea ya sea la interfaz CLI o GUI para acceder a un servicio que presta un determinado servidor en internet o intranet, puede acceder a él conociendo ya sea su "dirección IP" o su "nombre de dominio" (Domine Name). En el caso de usar la dirección IP la comunicación entre un cliente con un servidor puede ser directa; pero en el caso de que se use el nombre de dominio, se requerirá que un servidor DNS (Domine Name Server) realice las traducciones de los nombres de dominio a direcciones IP.

La mayoría de la gente, usuarios con conocimientos mínimos de computación, cuenta con un "nombre de dominio" y accede a servidores de tipo *web* mediante un *browser;* sin embargo, hay ocasiones en las que pudiera no estar disponible el servidor DNS. Para ejemplificar la correspondencia entre las direcciones IP y sus correspondientes nombres de dominio, se usa la tabla V.1.

Caso	IP	Servicio / DN
1	172.17.102.1	FwCiscoE3.uacm.edu.mx; Firewall y servidor DSN.
2	172.17.102.2	radio.uacm.edu.mx
3	172.17.102.3	correo.uacm.edu.mx
4	172.17.102.4	desarrollo.uacm.edu.mx; www.uacm.edu.mx
5	172.17.102.8	wolf.uacm.edu.mx
6	172.17.102.15	sistemabibliotecario.uacm.edu.mx
7	172.17.102.18	estudiantes.uacm.edu.mx

Tabla V.1. Relación de direcciones IP y sus correspondientes nombres de dominio aplicables hasta 2012 en la UACM

En este punto como ejercicio el lector responda a 2 preguntas básicas:

1. Las direcciones IP corresponden a redes: ¿públicas o privadas?
2. Las direcciones IP corresponden a redes de clase: ¿A, B, C, D o E?

A continuación se muestran las imágenes resultantes de acceder a servidores empleando la dirección IP en un *browser explorer*. Actualmente no recomiendo el uso del *browser explorer* de MS ya que presenta serios problemas de seguridad. Un ejemplo típico de un *web browser* inseguro fue IE6 (Internet Explorer de Microsoft versión 6), el cual nació en el año 2000, cuando la Internet era muy diferente a lo que es ahora; en 2010 IE6 llegó al límite y fue sustituido por el IE8. En 2010 las posiciones de los *browsers* por dominio de mercado eran *IE* (Microsoft), *Firefox* (Mozilla-2002) y *Chrome* (Google-2008). Desde el año 2012 *Chrome* es el más usado, tendencia que se mantiene hasta 2015.

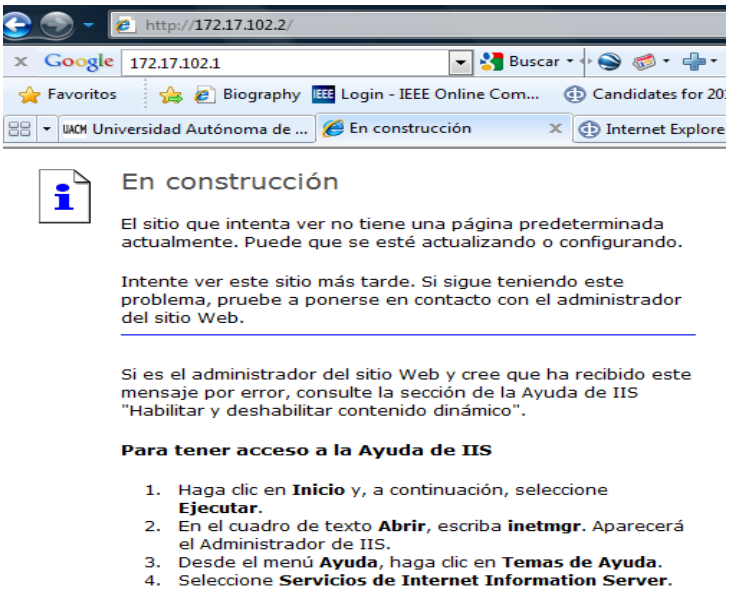


Fig. V.4 Página *web* para el caso 2 de la tabla V.1. [172.17.102.2]

La figura V.5 muestra la página *web* de un servidor de correo.

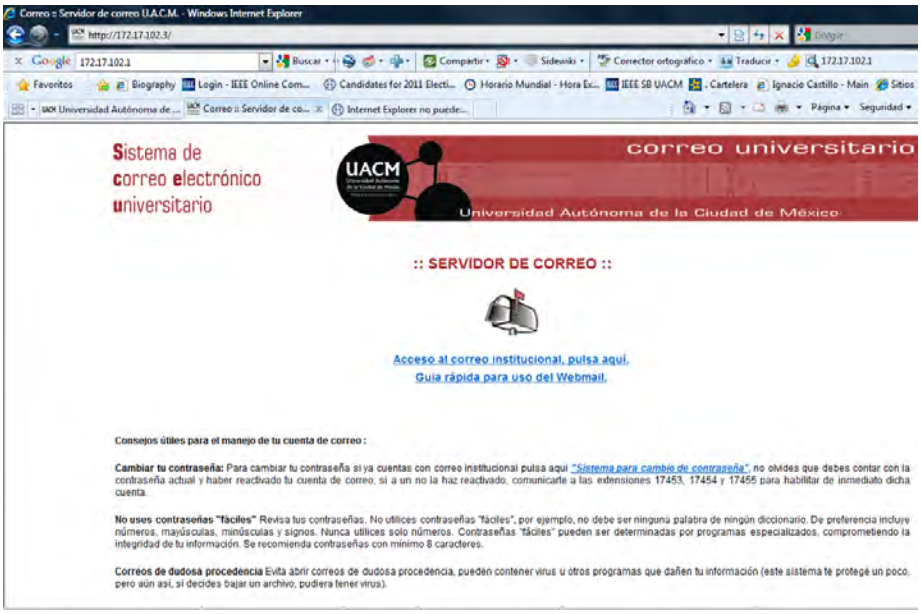


Fig. V.5. Página web para el caso 3 de la tabla V.1. [172.17.102.3].

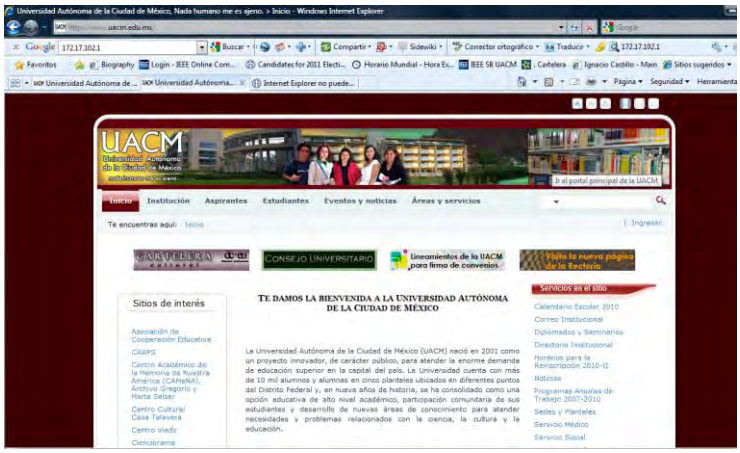


Fig. V.6. Página web para el caso 4 de la tabla V.1. [172.17.102.4].

La figura V.7 muestra el mensaje de error 500 para la página *web* solicitada.

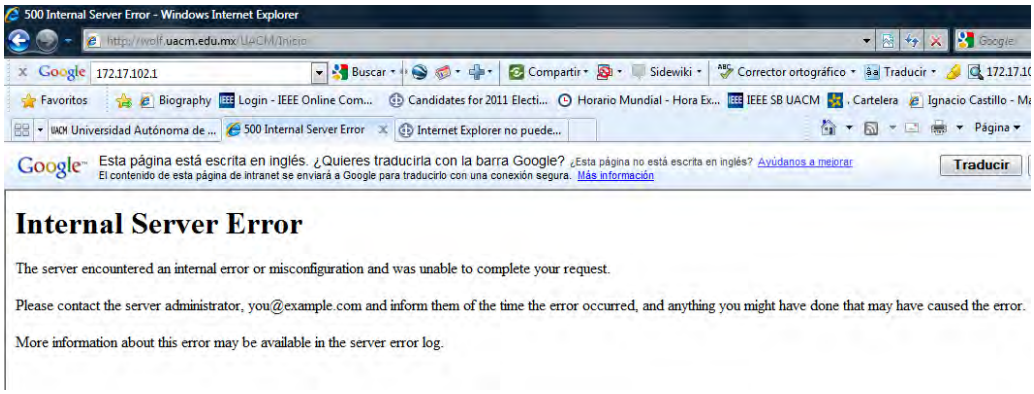


Fig. V.7. Página web para el caso 5 de la tabla V.1. [172.17.102.8].

La figura V.8 muestra la página *web* por la que se accede a un servidor de base de datos.

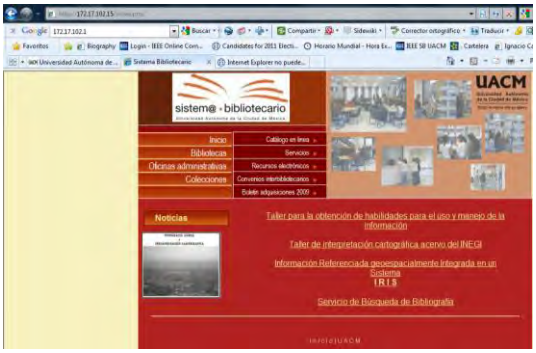


Fig. V.8. Página web para el caso 6 de la tabla V.1. [172.17.102.15].

La figura V.9 muestra la página *web* por la que se accede a otro servidor de base de datos.

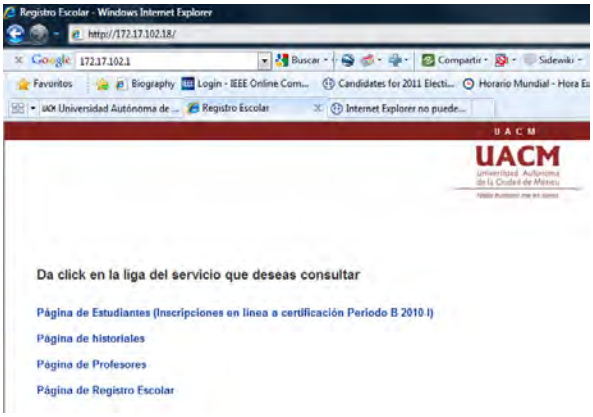


Fig. V.9. Página web para el caso 7 [172.17.102.18].

A continuación se muestran otros ejemplos de respuesta de servidor. La figura V.10 muestra la página *web* con el mensaje "Problemas en el servidor" mediante la aplicación que provee vía el servidor.

Fig. V.10. Error de aplicación con servidores

A continuación se muestran a manera de ejemplo otros errores con servidores; la figura V.11 muestra uno que ya se ha convertido error común en servicios de "facebook".

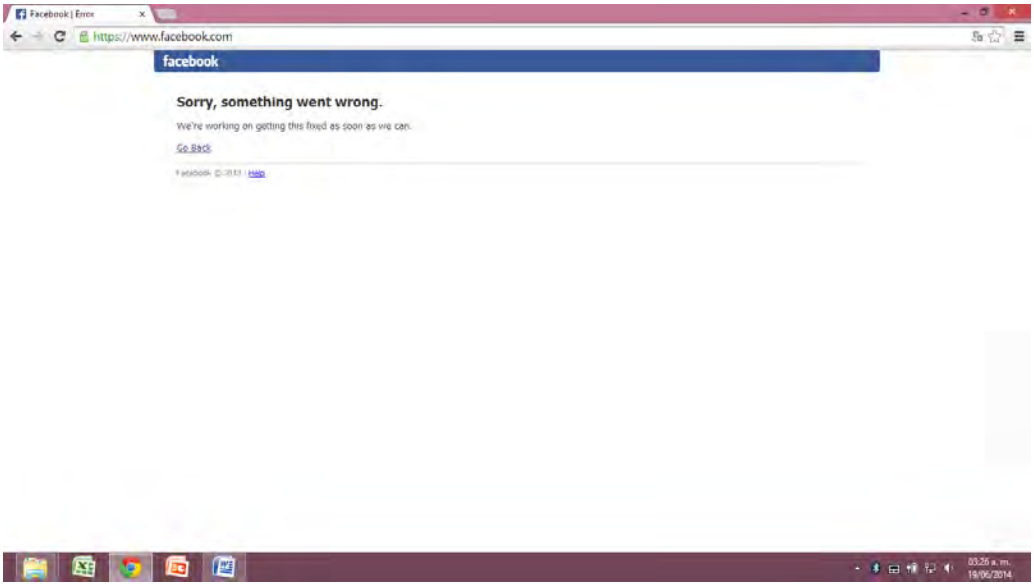


Fig. V.11 Sitio web de "facebook" fuera de línea. La fecha se indica en la esquina inferior derecha.

Si ahora nos preguntamos, cómo es que los administradores de las páginas web realizan las actividades de altas y modificaciones de una página *web* en un servidor, la respuesta está en una actividad rutinaria, se conectan a un servidor vía el protocolo ftp. La figura V.12 muestra un ejemplo de conexión a un servidor hipotético vía ftp, para realizar transferencias de archivos entre un *host* y un servidor.

```
C:\ftp nuyoo
Connected to nuyoo.utm.mx
220 nuyoo ftp server (univ(v)) system V realease 4.0
user (nuyoo.utm.mx(none)):igcast
331 password required for igcast
password:xxxx
230 user igcast logged in
ftp>binary
200 type set to I
ftp> put
(local-file): articulo.doc
(remote-file): articulo.doc
200 port command successful
150 binary data connection for articulo.doc (192.100.170.42,1133)
226 transfer complete
24 bytes sent in 1 second (24000kb/second)
ftp>close
221 googbye
ftp>quit
c:\
```

Fig. V.12. Acceso a un servidor mediante ftp vía CLI

Otra manera de conectarse a un servidor es vía GUI, una típica es *winscr,* cuyo ejemplo se muestra en la figura V.13. Otra interfaz típica es *filezilla;* ambas se pueden obtener gratuitamente en internet.

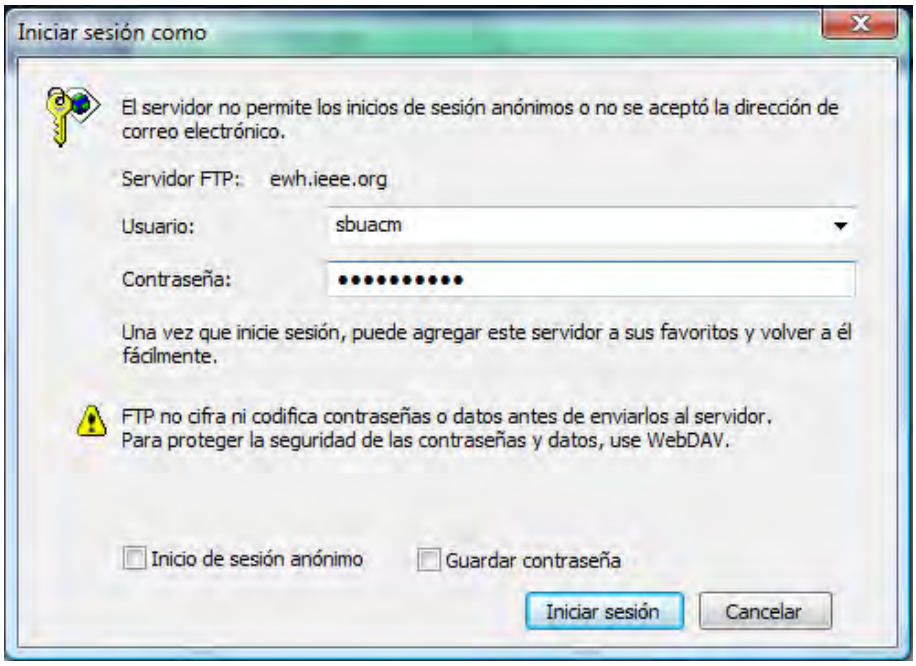


Fig. V.13. Respuesta a solicitud de conexión a un servidor empleando una GUI.

V.3.1. Resolución de nombres de dominios

En la sección anterior se observaron las direcciones IP y sus nombres de dominio correspondientes para un determinado servidor. Una herramienta útil que viene con el sistema operativo es "*nslookup"*, la cual sirve para encontrar la correspondencia entre la dirección IP asignada a un servidor y su correspondiente nombre de dominio. Por ejemplo, si se desea conocer la dirección IP asignada a www.telcel.com se deberá usar el comando "nslookup" vía CLI como se indica en la figura V.14 presentando su correspondiente dirección IP. Es probable que cuando lo intente haya cambiado la dirección asignada.

```
C:>\nslookup www.telcel.com
Respuesta no autoritativa:
Nombre: telcel.com
Address: 128.241.121.56
Aliases: www.telcel.com
```

Fig. V.14. Uso de "nslookup".

También se puede buscar el nombre de dominio a partir de una dirección de IP, "C:>\nslookup 128.241.121.56", en cuyo caso se obtendrá la correspondiente nombre de dominio. La información de un servidor DNS constituye una BD distribuida, cuya información tiene asociados nombres de dominio asociados a direcciones de IP.

Si se usa "nslookup" y se obtiene por ejemplo, para el caso de los servidores de la UACM sobre los que se probó anteriormente, una respuesta "FwCiscoE3.uacm.edu.mx**"** y una dirección "172.17.104.1"**,** entonces, se estará haciendo referencia a un servidor del tipo *firewall* ya sea *software* o *hardware*.

En este punto cabe preguntar al lector:

1. ¿Qué protocolos se emplearon?
2. ¿A qué capa corresponden en el modelo ISO/OSI?

PRÁCTICA 5: El objetivo es que el lector verifique que cuenta con la conectividad con un determinado host, computadora o servidor, y que puede obtener su correspondiente nombre de dominio y dirección IP.

Actividad 1- Acceda al CLI de su sistema operativo para emplear el comando "ping" que le permitirá verificar si existe conectividad con un determinado servidor. Básicamente debe resolver la pregunta: ¿el servidor esta alcanzable?

Repita lo indicado en la figura V.15, y emplee 10 direcciones IP para realizar la verificación correspondiente. Observe el número de paquetes enviados, recibidos y perdidos en función de IPv4.

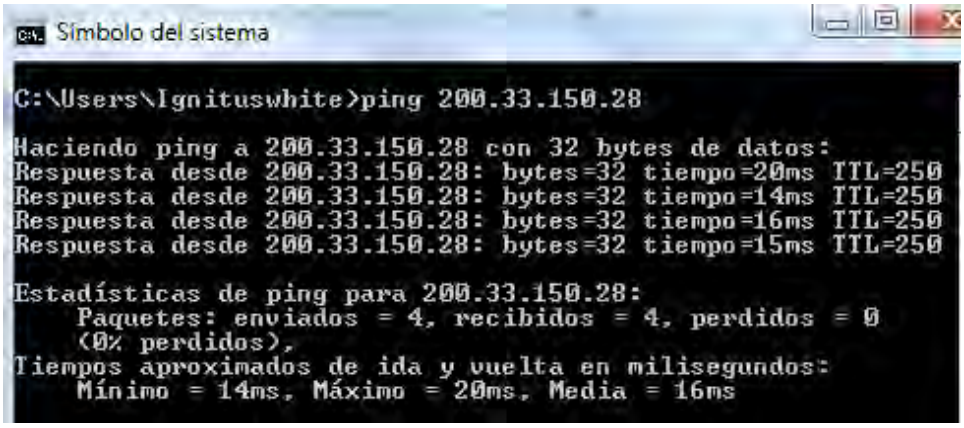


Fig. V.15 Empleo de "ping".

En este punto, el lector podría preguntarse: ¿cuál es el motivo por el que se envían 4 paquetes?, y también está en condiciones de responder correctamente.

Actividad 2- Acceda al CLI de su sistema operativo para emplear el comando "nslookup" para que dadas 10 direcciones IP obtenga sus correspondientes nombres de dominio.

Actividad 3- Acceda al CLI de su sistema operativo para emplear el comando "nslookup" para que dados 10 nombres de dominio obtenga sus correspondientes direcciones IP.

Actividad 4- Acceda al CLI de su sistema operativo para emplear el comando "hostname" para que dados 10 nombres de dominio obtenga sus correspondientes nombres.

V.3.2 Conexión a servidores web

PRÁCTICA 6: El objetivo es que el lector emplee una computadora para comunicarse con un servidor, de manera consciente, usando nombres de dominio y direcciones IP. También se busca que identifique el tipo de servidor al que se accede o intenta acceder.

Actividad 1- Acceda a un servidor web si se le proporciona su "nombre de dominio". Emplee 10 diferentes nombres de dominio y también obtenga en una tabla, sus direcciones IP.

Actividad 2- Acceda a un servidor si se le proporciona su "dirección IP". Emplee las 10 diferentes direcciones IP indicadas en la tabla V.2.

IP	URL correspondiente (tal y como lo resuelve el DNS)	Tipo de servidor
140.233.138.8		
132.248.10.44		
148.204.103.161		
148.206.159.21		
148.228.1.20		
148.237.3.162		
148.239.220.110		
200.23.113.36		
200.52.255.181		
200.56.248.23		
148.228.1.1		

Tabla V.2

Actividad 3- Acceda a la página web de Prodigy, colocando en el URL de sus nombre de dominio http://prodigy.msn.com. Ahora acceda a la página web de PRODIGY usando la siguiente dirección IP: http://200.33.150.28, observe los resultados. Ahora use la tabla V.2 y repita este ejercicio con cada uno de los 10 casos.

¿Qué puerto se empleó, en capa 4?, ¿en qué casos se empleó el servidor DNS?

V.3.3. Conexión a servidores ftp

PRÁCTICA 7: El objetivo es que el lector emplee una computadora para comunicarse con un servidor ftp, de manera consciente, vía CLI y GUI mediante un browser, usando nombres de dominio y direcciones IP.

Actividad 1- Acceda vía CLI del sistema operativo de su computadora, tableta o teléfono celular, al menos a los servidores "ftp" listados a continuación, para obtener su árbol de directorios, de modo que indique 5 directorios ligados al directorio raíz y el árbol presente tres niveles de profundidad indicando al menos 3 archivos por directorio.

1. ftp.uv.es
2. ftp.iij.ad.jp
3. ftp.esat.net
4. ftp.terra.es
5. ftp.microsoft.com

Actividad 2- Acceda a un servidor ftp vía GUI mediante un browser en su computadora, tableta o teléfono celular, como se indica en la siguiente figura. Verifique y valide la estructura de árbol que obtuvo en la actividad 1.

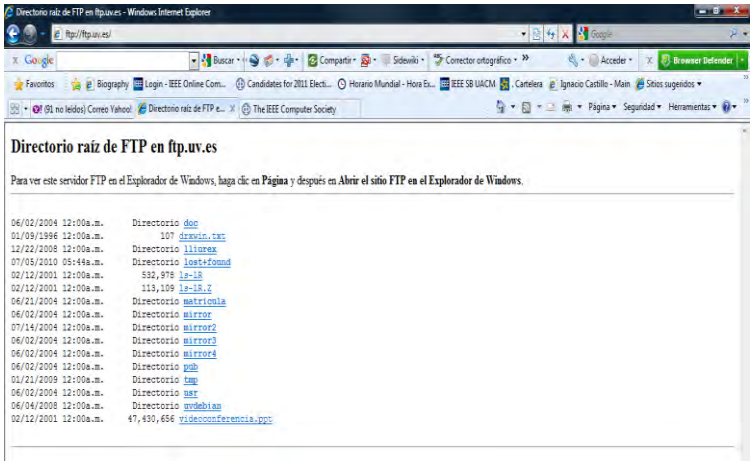


Fig. V.16 Ingreso al servidor FTP vía *web browser*

Actividad 3- Acceda a un servidor ftp vía GUI mediante un visor que le proporciona el sistema operativo en su computadora, tableta o teléfono celular. Verifique y valide la estructura de árbol que obtuvo en la actividad 1.

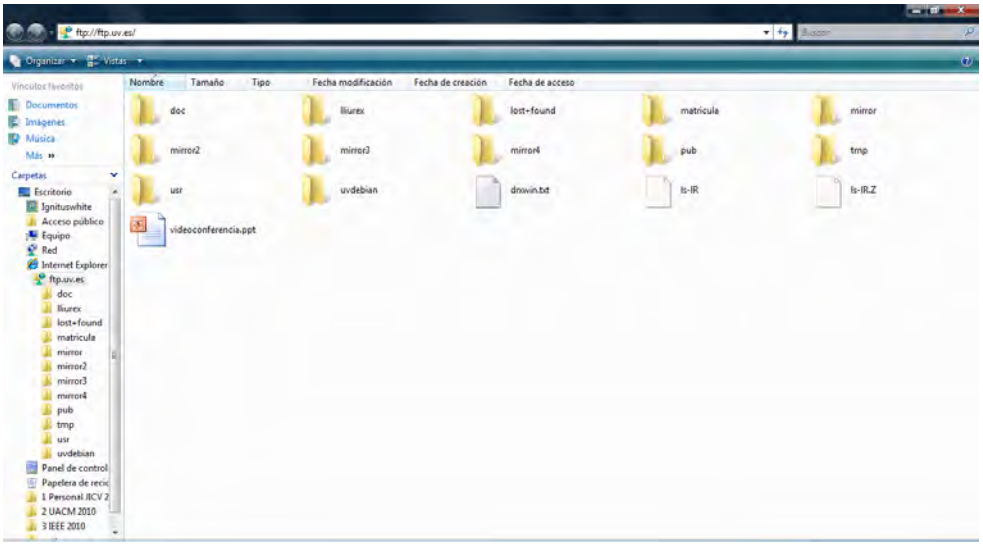


Fig. V.17 Ingreso al servidor FTP vía windows explorer

Actividad 4- Por cualesquiera vía intente crear un subdirectorio nuevo y obtendrá lo indicado por la figura V.18, reproduzca y explique el motivo.

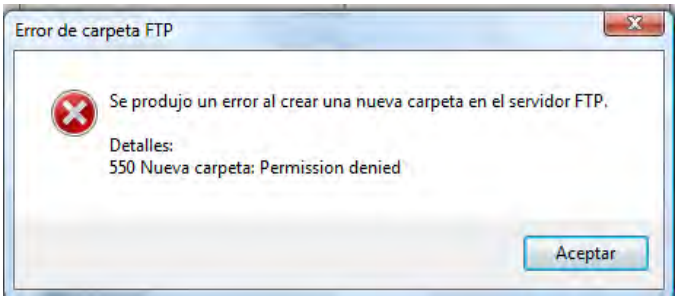


Fig. V.18 Mensaje de error ya que no se cuenta con permisos de escritura al ingresar como anonymous.

Por cualesquiera vía intente copiar un archivo desde su computadora hacia el servidor y obtendrá lo indicado en la figura V.19, reproduzca y explique el motivo.

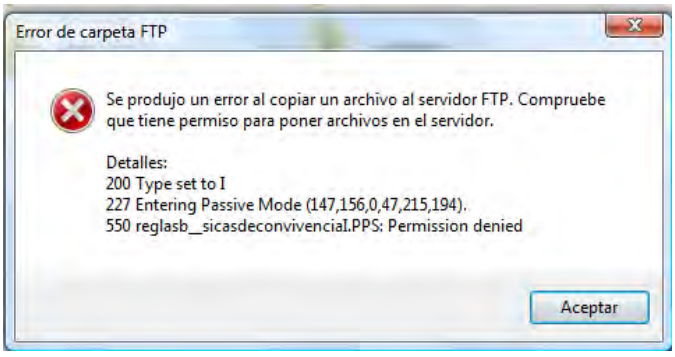


Fig. V.19 Mensaje de error ya que no se cuenta con permisos de escritura.

Actividad 5- Acceda a un servidor ftp vía una "aplicación cliente GUI". Verifique y valide su estructura de árbol, observe los ejemplos de V.20 y V. 21.

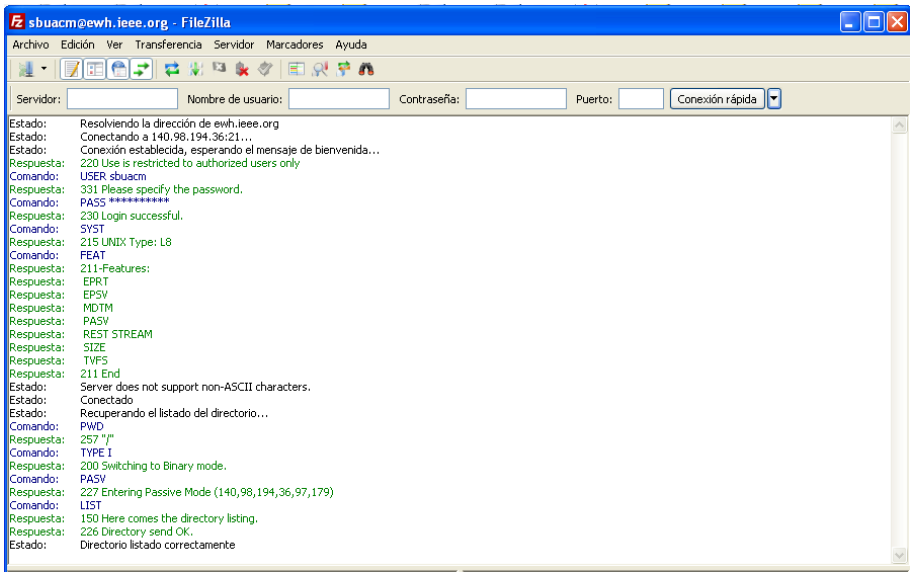


Fig. V.20 Conexión a servidor FTP usando FileZilla. Observe los códigos 150, 220, 211, 215, 226, 230, 257 y 331 para dar su adecuada interpretación.

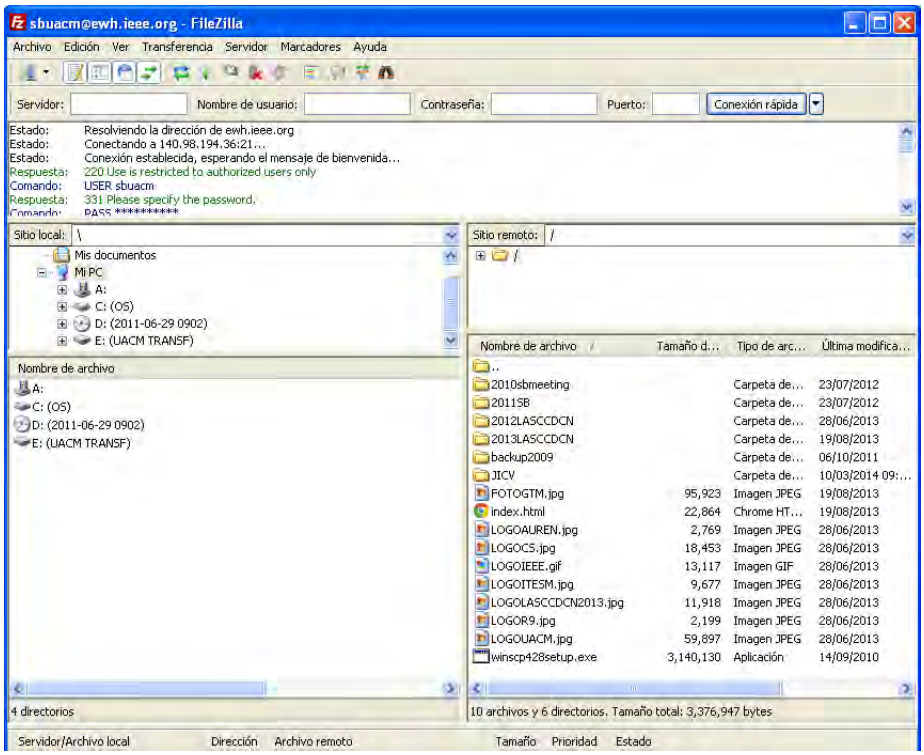


Fig. V.21 Conexión a servidor FTP usando FileZilla. Observe la información que presenta la interfaz completa conformada por 3 áreas: diálogo entre host y servidor, directorio del host y directorio del servidor.

V.4. Instalación de un servidor web

Una práctica común para las aplicaciones en internet es dar de alta servidores, así como mantener al servidor operando adecuadamente, para lo cual se realizan actividades que den soporte a la operación del mismo. A continuación se indica como instalar, probar y administrar servidores web mediante APACHE y MS-IIS en un servidor de máquina real [88].

V.4.1 Instalación del servidor MS-IIS

Considerando que es relativamente fácil contar con un equipo que cuente con el sistema operativo "Windows", instalaremos un servidor para emplear el *localhost*, es decir, el host en el que se convierte mi computadora, para poder ejecutar mis programas e incluso me permite dejar todo listo para darlos de alta en un web host y proveer un servicio profesional. Para instalar el "*Internet Information Server*" (IIS) de Windows es necesario agregar programas, componentes o características de Windows como en la figura V.22. Observe los detalles.

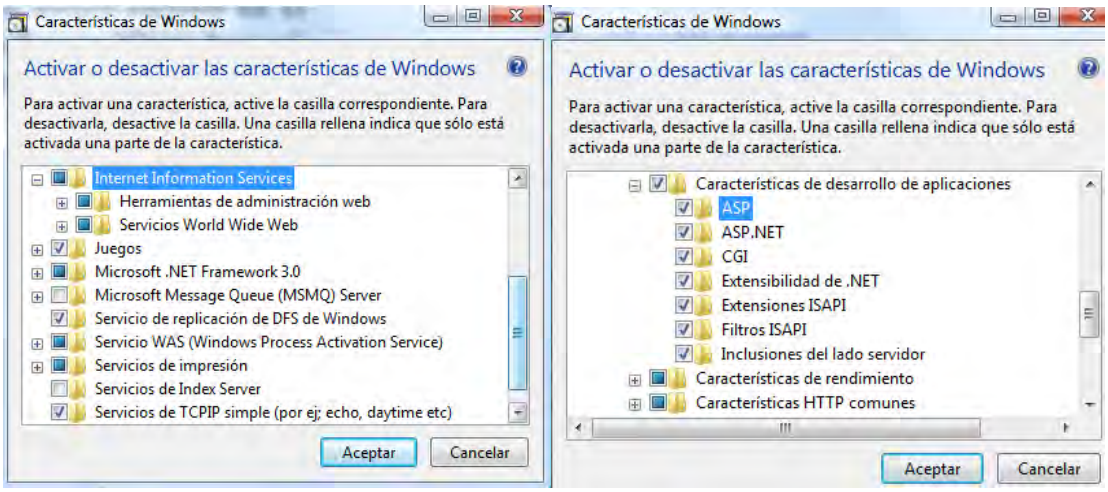


Fig. V.22 Instalación de componentes del IIS de Windows.

Ahora active las características de diagnóstico, seguridad y HTTP como se indica en la figura V.23.

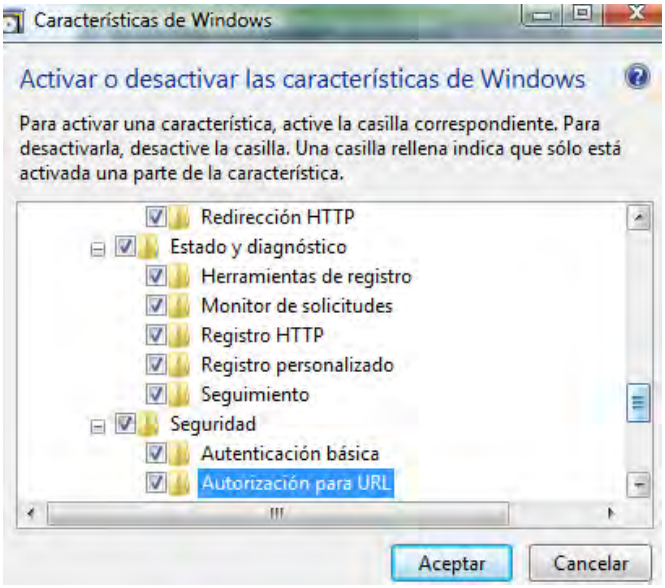


Fig. V.23 Instalación de características de diagnóstico y seguridad.

Una vez que ha quedado instalado el IIS V7, el *localhost* tiene como directorio o subdirectorio "C:\Inetpub\wwwroot\" el cual es el "directorio web raíz" o lo que correspondería al "directorio de conexión" en una página web. La figura V.24 muestra el contenido de subdirectorio en cuestión.

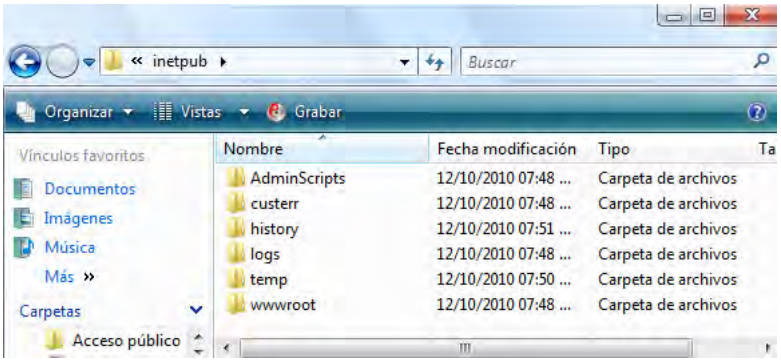


Fig. V.24 Contenido del subdirectorio C:\Inetpub\

Para comprobar que el servidor en **localhost** funciona, se abre el browser preferido, evite *explorer*, y en el URL se debe indicar, por ejemplo, http://localhost/WPJICV2010.html, para obtener la figura V.25, en cuyo caso, es claro que la instalación del servidor ha sido exitosa y es posible ejecutar mis desarrollos web.

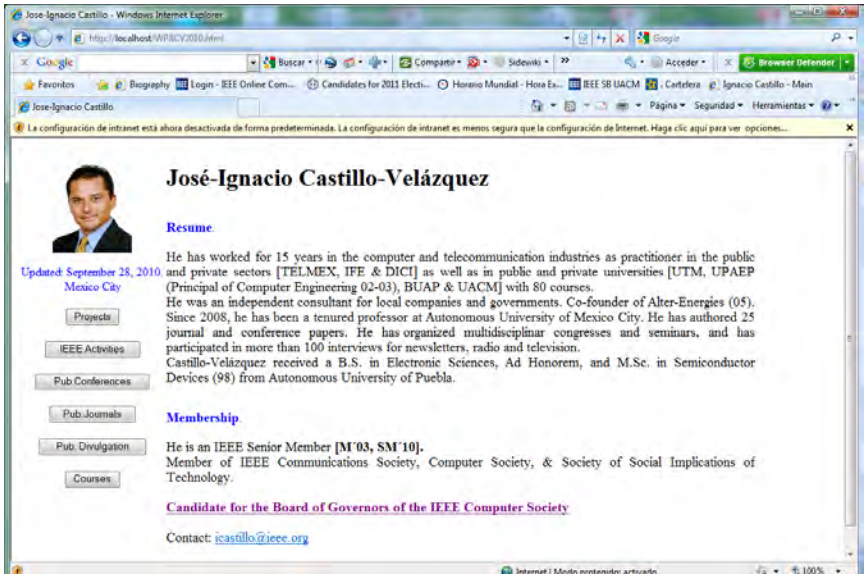


Fig. V.25 Página web distribuida desde mi servidor *localhost.*

V.4.2 La administración en un servidor IIS

La administración de un servidor consiste en realizar tareas como la lectura e interpretación de los **logs** del servidor y de los mensajes de error, así como de apagar o encender el servidor adecuadamente.

A. Logs**:** Son archivos de texto que sirven para registrar toda actividad en el servidor y con ello monitorear al mismo; se ubican en "C:\Inetpub\wwwroot\logs\LogFiles\W3SVC1". La figura V.26, ejemplifica el contenido de un LOG.

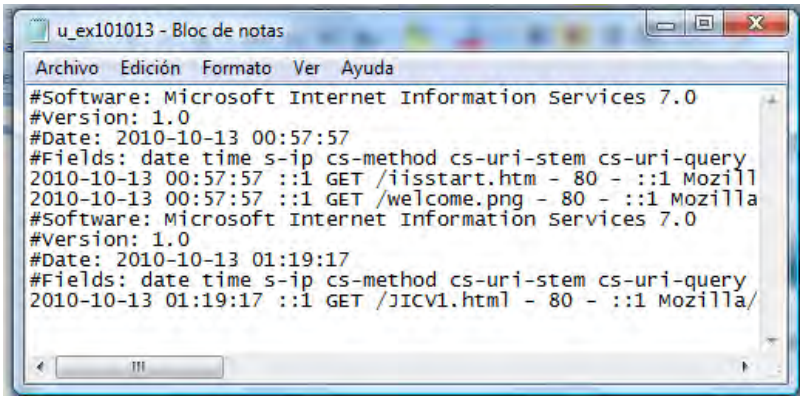


Fig. V.26 Ejemplo del log "W3SVC1".

B. Mensajes de error: Un administrador de servidores también debe poder interpretar correctamente los mensajes de error; algunos de los mensajes de error comunes son el

404 y el 500 como se indican en las siguientes figuras V.27 y V.28. Los mensajes de error que puede indicar el servidor *localhost* se encuentran como páginas HTML en la ruta "C:\Inetpub\wwwroot\custerr\es-Es**".**

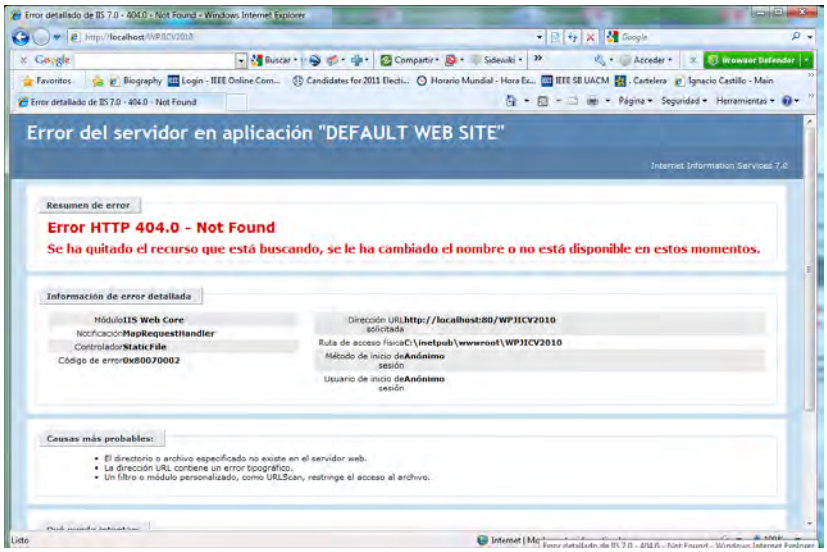


Fig. V.27 Mensaje de error 404 generado al indicar el nombre del archivo de la página web incompleta, falta la extensión del archivo.

Observe también que se indica la versión del servidor IIS V7 en la parte superior izquierda de cada pantalla de error.

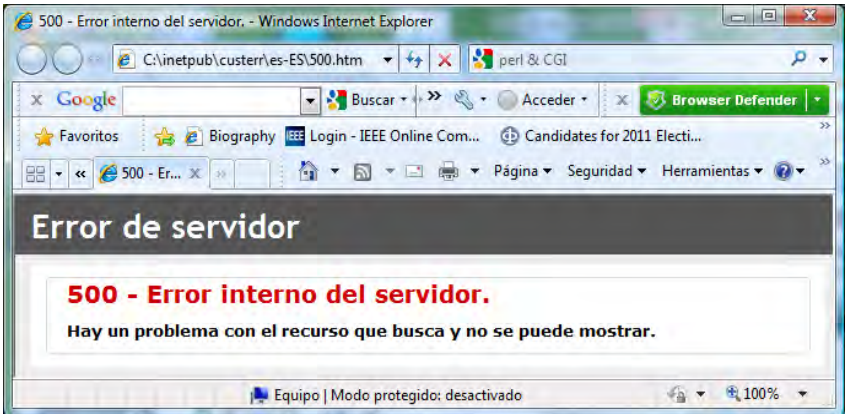


Fig. V.28. Error 500

En términos de seguridad se debe considerar que de manera recurrente habrá un conjunto de subdirectorios para los cuales les aparecerá la siguiente leyenda. Razón por la cual habrá que indicar que cuenta con los permisos para poder acceder a ella. Como recomendación, si no sabe para qué

sirven los archivos indicados en una determinada carpeta no acceda, sea muy cuidadoso ya que puede provocar serios errores en su servidor [88].

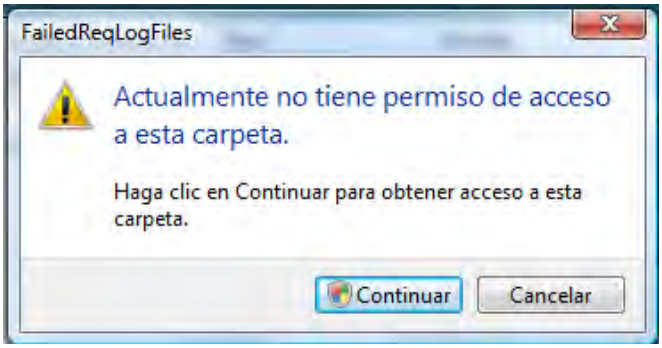


Fig. V.29. Cuadro de dialogo relativo a permisos

Cada vez que usted copie archivos o realice modificaciones en el *localhost* le aparecerá la advertencia indicada en la figura V.30, la cual permitirá comprobar sus permisos de administrador.

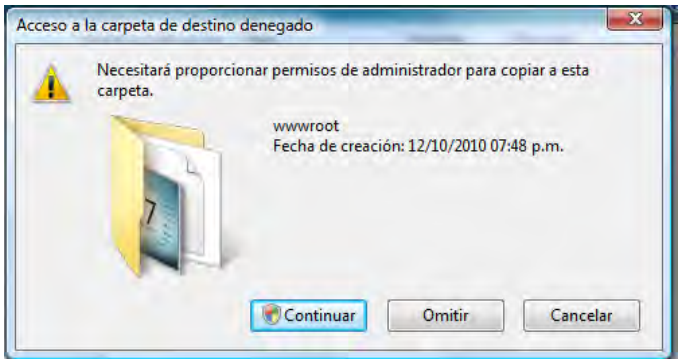


Fig. V. 30. Complemento de caja de diálogo sobre permisos en el directorio raíz del *localhost*.

V.4.3 Instalación del servidor Apache

Apache es un servidor HTTP desarrollado por *Apache Software Foundation*, el cual se obtiene desde el siguiente nombre de dominio: http://httpd.apache.org/. Todo servidor en internet se compara siempre contra un servidor Apache dado que los servidores Apache en Unix son los más empleados en la internet. Recomiendo bajar una versión estable. Una vez que se baja a mi computadora el software de instalación httpd-2.2.17-win32-x86-no_ssl con un peso de casi 6MB, se ejecuta y se obtienen los mensajes importantes como en la en la figura V.31 [88].

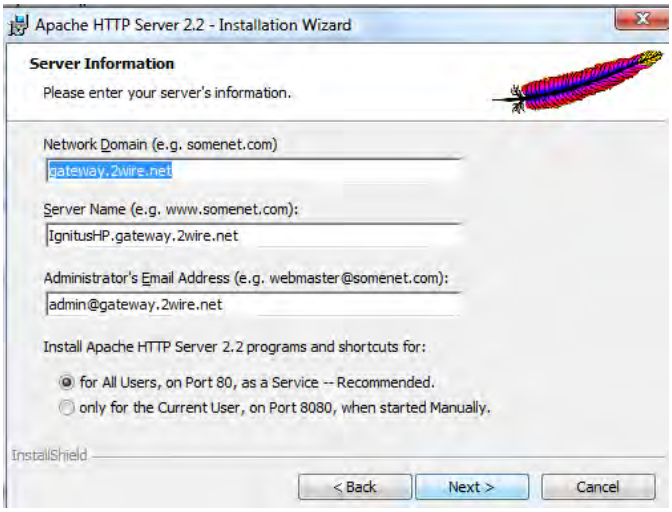


Fig. V.31 Instalación de Apache para Windows.

Observe que "IgnitusHP.gateway.2wire.net" es equivalente al *localhost*. En la figura V.32, se observan algunos elementos que se instalan, por ejemplo, en el caso de una instalación "típica"

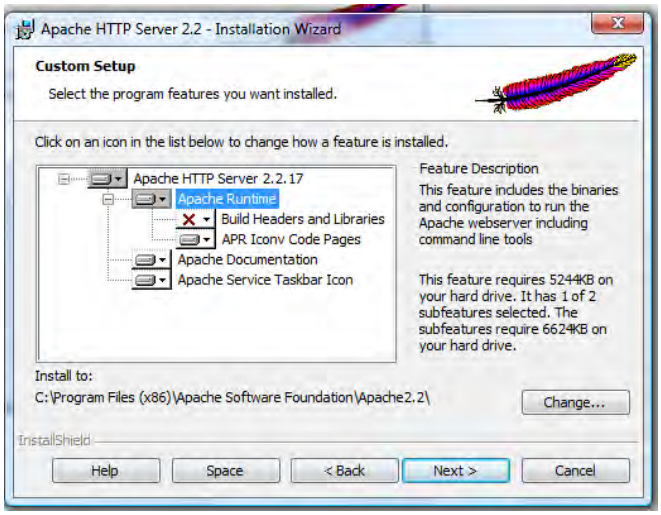


Fig. V.32 Elementos que se instalan.

Una vez que ha quedado instalado el servidor Apache, es conveniente observar el contenido del directorio de Apache, así como se analizó el caso del IIS. Para el caso de Apache, el *localhost* tiene como directorio o subdirectorio "C:\...\Apache2.2\htdocs\" el cual es el "directorio web raíz" o lo que correspondería al directorio de conexión en una página web, para colocar archivos o documentos HTML o equivalentes. En el caso de apache se habla de *ServerRoot* ubicado en, por ejemplo, **"**C:/Program Files (x86)/Apache Software Foundation/Apache2.2". Una vez instalado Apache debe poder localizar el subdirectorio, como se indica en la figura V.33. También es posible obtener la estructura del árbol del subdirectorio indicado.

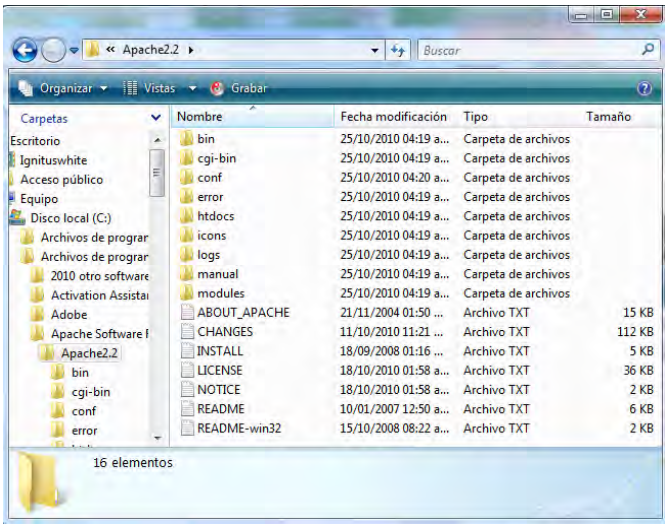


Fig. V.33. Contenido del subdirectorio "C:\Program Files (x86)\Apache Software Foundation\Apache2.2"

Para comprobar que funciona el servidor en **localhost** se abre el browser preferido y en el URL se indica http://localhost/ para obtener la figura V.34. La figura indica que la instalación del servidor ha sido exitosa y que el servidor se encuentra listo para ejecutar los desarrollos web.

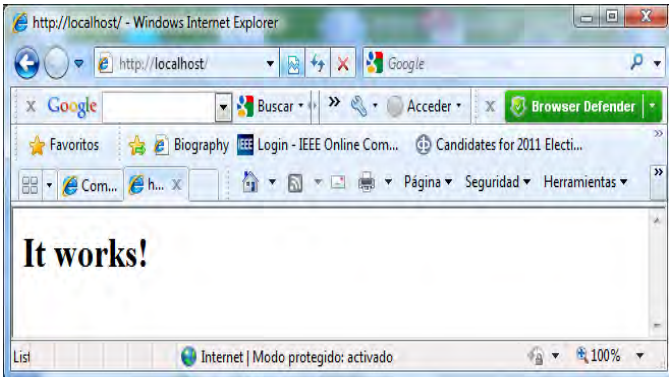


Fig. V.34. Página web distribuida desde mi servidor *localhost*.

También puede probar con "http://127.0.0.1" y se obtendrá el mismo resultado. Una vez instalado el servidor Apache, este se inicializa, lo cual se puede hacer mediante el monitor del servicio del servidor Apache (Apache Service Monitor). La figura V.35 muestra que le servidor Apache se encuentra detenido o apagado, por lo que para iniciarlo se debe usar la opción "Start" [88]. Una manera alternativa de encontrarlo es buscando la aplicación "apachemonitor.exe"

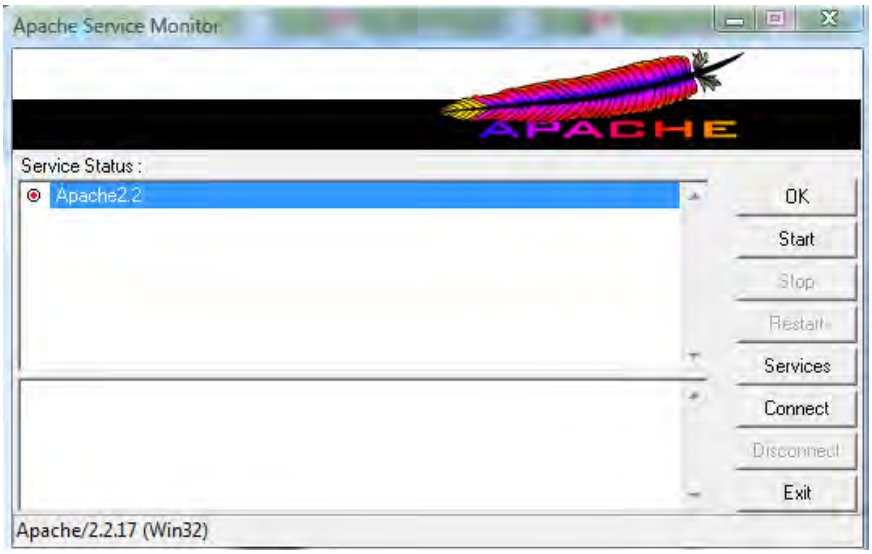
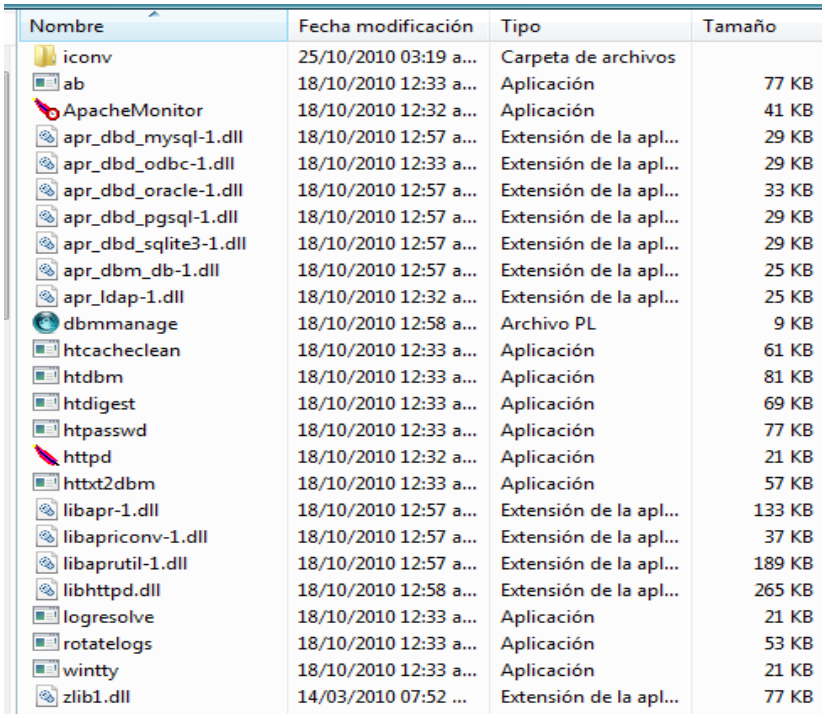


Fig. V.35 Monitor de Servicio de Apache.

Considere que Apache no puede compartir el puerto 8080 con otras aplicaciones *web*, por lo que es preciso desactivar otras aplicaciones que estén empleando tal puerto para iniciar Apache y viceversa. Algunas aplicaciones WWW con las que podría haber conflicto son por ejemplo, con IIS o implementaciones de *firewall*. En el caso de Apache, las aplicaciones en HTML para servidor web, se deben colocar en "C:\...\Apache2.2\htdocs".

V.4.4 La administración en un servidor Apache

Las aplicaciones principales “httpd” y “Apache monitor” se encuentran en el subdirectorio “bin” como se indica en la figura V.36.



Nombre	Fecha modificación	Tipo	Tamaño
iconv	25/10/2010 03:19 a...	Carpeta de archivos	
ab	18/10/2010 12:33 a...	Aplicación	77 KB
ApacheMonitor	18/10/2010 12:32 a...	Aplicación	41 KB
apr_dbd_mysql-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	29 KB
apr_dbd_odbc-1.dll	18/10/2010 12:33 a...	Extensión de la apl...	29 KB
apr_dbd_oracle-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	33 KB
apr_dbd_pgsql-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	29 KB
apr_dbd_sqlite3-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	29 KB
apr_dbm_db-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	25 KB
apr_ldap-1.dll	18/10/2010 12:32 a...	Extensión de la apl...	25 KB
dbmmanage	18/10/2010 12:58 a...	Archivo PL	9 KB
htcacheclean	18/10/2010 12:33 a...	Aplicación	61 KB
htdbm	18/10/2010 12:33 a...	Aplicación	81 KB
htdigest	18/10/2010 12:33 a...	Aplicación	69 KB
htpasswd	18/10/2010 12:33 a...	Aplicación	77 KB
httpd	18/10/2010 12:32 a...	Aplicación	21 KB
httxt2dbm	18/10/2010 12:33 a...	Aplicación	57 KB
libapr-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	133 KB
libapriconv-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	37 KB
libaprutil-1.dll	18/10/2010 12:57 a...	Extensión de la apl...	189 KB
libhttpd.dll	18/10/2010 12:58 a...	Extensión de la apl...	265 KB
logresolve	18/10/2010 12:33 a...	Aplicación	21 KB
rotatelogs	18/10/2010 12:33 a...	Aplicación	53 KB
wintty	18/10/2010 12:33 a...	Aplicación	21 KB
zlib1.dll	14/03/2010 07:52 ...	Extensión de la apl...	77 KB

Fig. V.36. Comandos principales: “httpd” y “Apache monitor”.

A. Los logs en Apache, son de tres tipos: de instalación [install.log], de acceso [access.log] y de error [error.log]; todos ellos archivos de tipo texto, mismos que se ubican en el subdirectorio “C:\...\Apache2.2\logs”**.** La figura V.37 muestra el contenido de un archivo “install.log”, indicándose el subdirectorio en el que se depositan los archivos de instalación [88].

```
Installing Apache HTTP 2.0 server with
 DomainName =    gateway.2wire.net
 ServerName =    IgnitusHP.gateway.2wire.net
 ServerAdmin =   ignacio_castillo_2005@yahoo.com.mx
 ServerPort =    80
 ServerSslPort = 80
 ServerRoot =    C:/Program Files (x86)/Apache Software Foundation/Apache2.2
Rewrote C:/Program Files (x86)/Apache Software Foundation/Apache2.2/conf/original/extra/httpd-autoindex.conf.in
 to C:/Program Files (x86)/Apache Software Foundation/Apache2.2/conf/original/extra/httpd-autoindex.conf
Successfully removed C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\original\extra\httpd-
autoindex.conf.in
Rewrote C:/Program Files (x86)/Apache Software Foundation/Apache2.2/conf/original/extra/httpd-vhosts.conf.in
 to C:/Program Files (x86)/Apache Software Foundation/Apache2.2/conf/original/extra/httpd-vhosts.conf
```

Fig. V.37. Contenido parcial del archivo “install.log”

La figura V.38 muestra en ejecución el comando "get", para solicitar páginas web. En el caso de que se realizaran cargas de archivos, se podría observar el empleo del comando "put". También se observan los códigos de éxito o error al entregar o recibir las páginas web por parte del servidor.

```
127.0.0.1 - - [25/Oct/2010:04:45:58 -0500] "GET / HTTP/1.1" 200 44
127.0.0.1 - - [25/Oct/2010:04:50:41 -0500] "GET /test.pl HTTP/1.1" 404 205
127.0.0.1 - - [25/Oct/2010:04:57:27 -0500] "GET /cgi-bin/test.pl HTTP/1.1" 500 554
127.0.0.1 - - [25/Oct/2010:05:01:17 -0500] "GET /cgi-bin/test.cgi HTTP/1.1" 500 554
127.0.0.1 - - [25/Oct/2010:05:07:35 -0500] "GET /cgi-bin/test.cgi HTTP/1.1" 500 554
127.0.0.1 - - [25/Oct/2010:05:07:51 -0500] "GET /cgi-bin/printenv.pl HTTP/1.1" 200 1464
127.0.0.1 - - [25/Oct/2010:05:08:10 -0500] "GET /cgi-bin/printenv.cgi HTTP/1.1" 404 218
127.0.0.1 - - [25/Oct/2010:10:53:01 -0500] "GET /test.pl HTTP/1.1" 404 205
169.254.77.162 - - [25/Oct/2010:15:51:39 -0500] "OPTIONS //::%7B2227a280-3aea-1069-a2de-08002b30309d%7D/
HTTP/1.1" 403 243
169.254.77.162 - - [25/Oct/2010:15:51:39 -0500] "OPTIONS //::%7B2227a280-3aea-1069-a2de-08002b30309d%7D/
HTTP/1.1" 403 243
127.0.0.1 - - [27/Oct/2010:10:31:01 -0500] "GET / HTTP/1.1" 304 -
127.0.0.1 - - [27/Oct/2010:10:33:34 -0500] "GET / HTTP/1.1" 200 44
127.0.0.1 - - [02/Nov/2010:23:35:11 -0600] "GET / HTTP/1.1" 200 44
127.0.0.1 - - [02/Nov/2010:23:40:59 -0600] "GET / HTTP/1.1" 304 -
127.0.0.1 - - [02/Nov/2010:23:41:08 -0600] "GET /PERL1.html HTTP/1.1" 200 292
127.0.0.1 - - [03/Nov/2010:01:36:20 -0600] "GET /test.pl HTTP/1.1" 404 205
127.0.0.1 - - [03/Nov/2010:02:05:06 -0600] "GET /cgi-bin/first.pl HTTP/1.1" 200 13
127.0.0.1 -[03/Nov/2010:02:20:42 -0600] "GET /cgi-bin/primero.pl HTTP/1.1" 200 13
```

Fig. V.38. Contenido parcial del archivo "access.log".

La figura V.39 muestra el contenido de un archivo "error.log".

```
httpd.exe: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
[Tue Nov 02 22:24:28 2010] [notice] Child 1820: Child process is running
[Tue Nov 02 22:24:28 2010] [notice] Child 1820: Acquired the start mutex.
[Tue Nov 02 22:24:28 2010] [notice] Child 1820: Starting 64 worker threads.
[Tue Nov 02 22:24:28 2010] [notice] Child 1820: Starting thread to listen on port 80.
[Wed Nov 03 01:36:20 2010] [error] [client 127.0.0.1] File does not exist: C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/htdocs/test.pl
[Wed Nov 03 01:47:36 2010] [error] [client 127.0.0.1] File does not exist: C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/htdocs/test.pl
[Wed Nov 03 01:47:43 2010] [error] [client 127.0.0.1] File does not exist: C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/htdocs/uno.pl
[Wed Nov 03 02:01:39 2010] [error] [client 127.0.0.1] File does not exist: C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/htdocs/first.pl
[Wed Nov 03 02:04:03 2010] [error] [client 127.0.0.1] File does not exist: C:/Program Files (x86)/Apache Software
Foundation/Apache2.2/htdocs/first.pl
```

Fig. V.39. Contenido parcial del archivo "error.log".

B. Mensajes de error: En Apache, éstos se encuentran como páginas HTML en la ruta "C:\...\Apache2.2\error". La figura V.40 muestra un mensaje de error en el que un sitio web determinado emplea una aplicación en lenguaje "Perl" y genera un mensaje muy interesante, el cual pocas veces veremos en los servidores de la internet [105, 106].

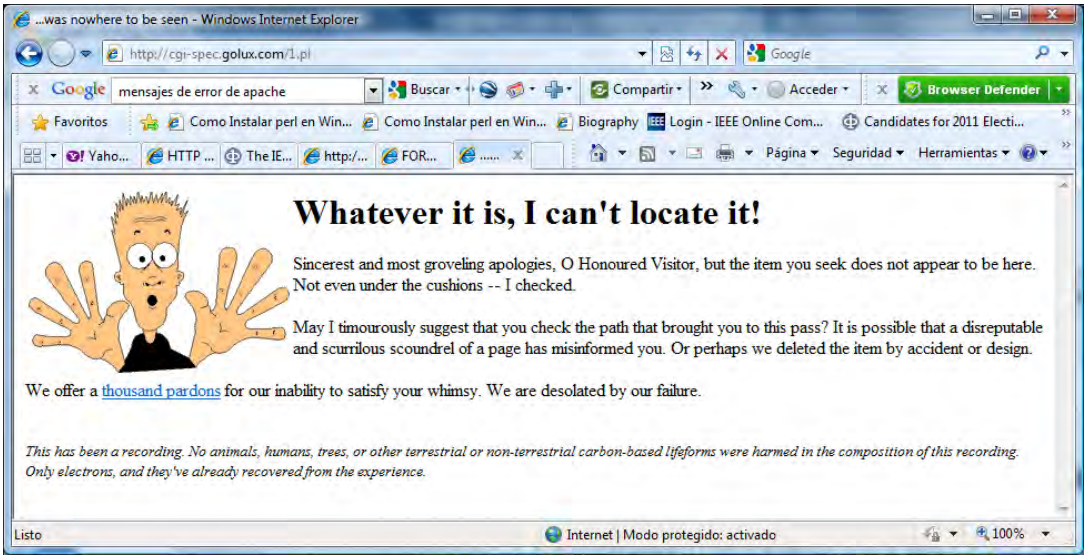


Fig. V.40 Mensaje de error 404 de apache para un archivo no encontrado.

El mensaje anterior nos lleva a http://cgi-spec.golux.com/1000p.cgi el cual es un programa en CGI que nos indica que el archivo CGI no se encuentra, es decir, al interpretarlo, nos percatamos de que en realidad no es un error del servidor Apache. Observe las mensajes de las figuras V.41 y V.42.

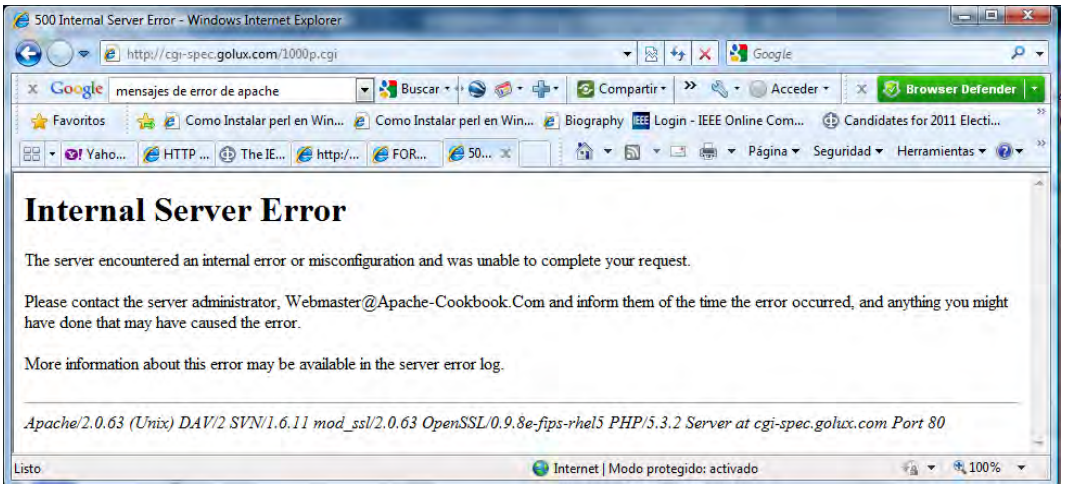


Fig. V.41. Mensaje de error 500 típico de un servidor Apache en Unix.

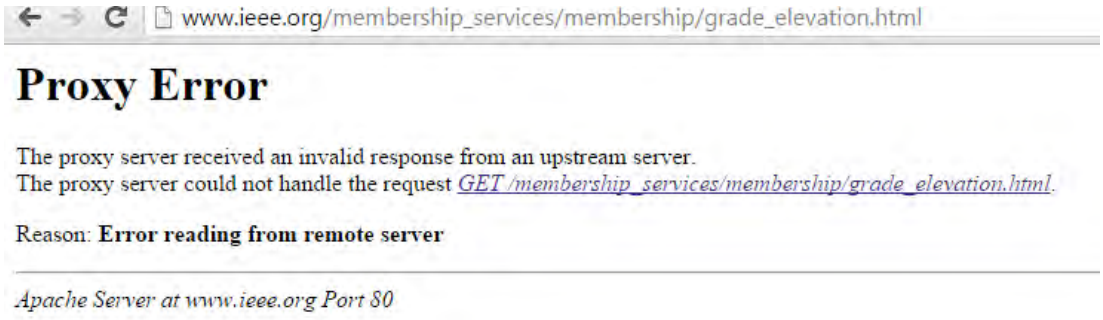


Fig. V.42. Mensaje de error 502, "Proxy error", en un servidor Apache en Unix.

V.4.5 Configuración en un servidor Apache

Una vez finalizada la instalación de Apache y comprobada la ejecución básica, Apache se configura con los archivos de configuración ubicados en "C:\...\Apache2.2\conf". El archivo configuración principal es el "httpd.conf", el cual es un archivo de texto, tal y como en los tradicionales y antiguos "autoexec.bat" y "config.sys" [105,106].

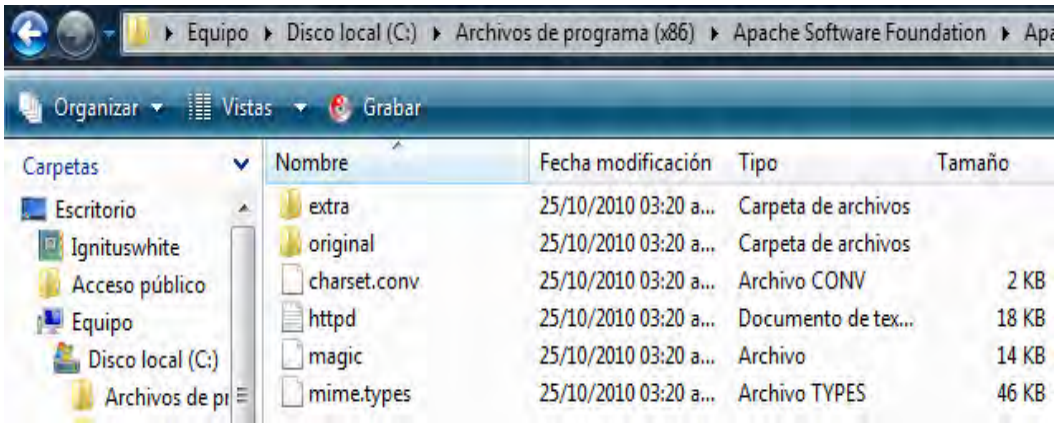


Fig. V.43. Archivos de configuración.

Con la finalidad de permitir la ejecución de programas CGI, se debe configurar Apache para ejecutar scripts CGI. La manera estándar es indicar en la configuración, la "directiva ScriptAlias", la cual le indica al servidor Apache, el directorio donde se encuentran todos los programas CGI, por lo que el servidor tratará de ejecutarlo cada vez que un cliente lo requiera. Para ello se consulta el archivo de configuración buscando se encuentre "ScriptAlias" o se incluye en el archivo, como se indica en la figura V.44.

```
# ServerRoot: The top of the directory tree under which the server's configuration, error, and log files are kept.
ServerRoot "C:/Program Files (x86)/Apache Software Foundation/Apache2.2"
# Listen: Allows you to bind Apache to specific IP addresses and/or # ports, instead of the default. See also the
<VirtualHost> directive.
Listen 80
# ScriptAlias: This controls which directories contain server scripts. ScriptAliases are essentially the same as Aliases,
except that documents in the target directory are treated as applications and run by the server when requested rather than
as documents sent to the client.  The same rules about trailing "/" apply to ScriptAlias directives as to Alias.
ScriptAlias /cgi-bin/ "C:/Program Files (x86)/Apache Software Foundation/Apache2.2/cgi-bin/"
```

Fig. V.44. Contenido parcial del archivo de configuración "httpd.conf"

En el caso de que se esté ejecutando en un servidor diferente al *localhosts*, sea por ejemplo, http://www.mipagina.com/cgi-bin/prueba.pl, entonces Apache tratará de ejecutar el archivo "C:/Program Files (x86)/Apache Software Foundation/Apache2.2/cgi-bin/prueba.pl" en el servidor, y regresará la salida del mismo al cliente solicitante. Los programas CGI se ubican en el directorio "cgi-bin" por cuestiones de seguridad, pero Apache se puede configurar para poder ejecutar los programas CGI en otro directorio, incluso en el propio directorio raíz de conexión [105, 106].

V.5 Implementación y administración de servidores

PRÁCTICA 8: El objetivo es que el lector instale un servidor web mediante APACHE y MS-IIS en un servidor de máquina real, pruebe la instalación y se familiarice con el gestor del servidor. También debe familiarizarse con la estructura de directorios, logs y mensajes de error del servidor.

Actividad 1. Instalar, probar y administrar un servidor MS-IIS como se ha indicado en las secciones anteriores.

Actividad 2. Localice el subdirectorio indicado en su equipo, como se indica en la figura correspondiente y obtenga la estructura del árbol del subdirectorio de conexión.

Actividad 3. Busque, lea e interprete los *logs*; también genere los errores que le permitan reproducir la aparición de los mensajes de error 401, 404 y 500. El error 502 se indica en la figura V.45 con la finalidad de que familiarice con otro de los mensajes de error más comunes que aparecen en un servidor.

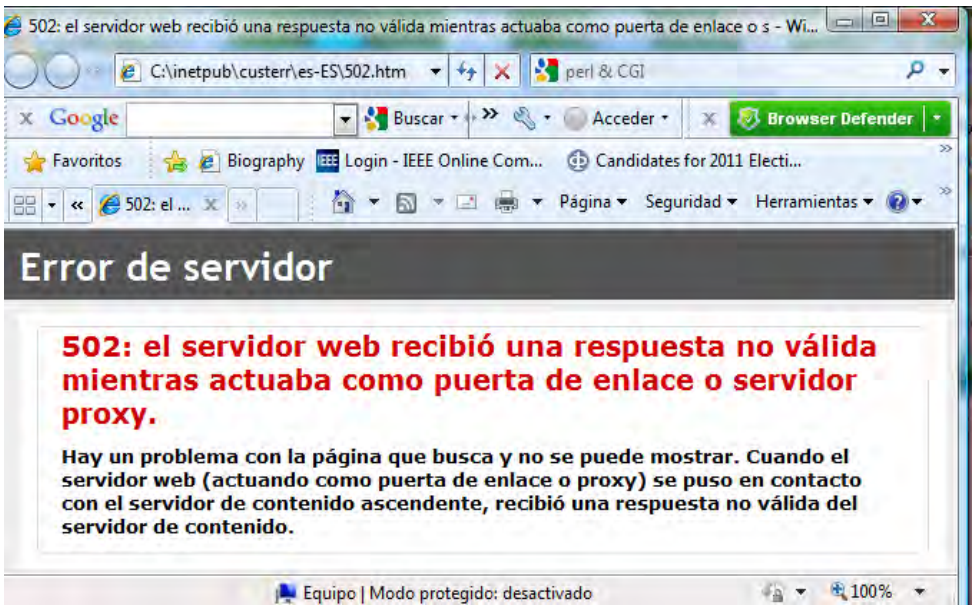


Fig V.45. Error 502

Actividad 4. Realice las actividades 1, 2 y 3 con un servidor APACHE como indicó en las secciones anteriores.

V.6 Vulnerabilidades de la arquitectura cliente servidor

La arquitectura cliente servidor es vulnerable al Ataque DoS (Denial-of-Sevice - Denegación de servicio) o DDoS (Distributed Denial-of-service / Denegación distribuida de Servicio). La DoS es un intento por hacer que un host (generalmente un servidor) o red quede como no disponible para los usuarios objetivo, lo cual se logra ya sea: al sobrecargar o saturar a los servidores o por disminuir de manera drástica el ancho de banda de la conexión. Algunas causas raíz de DoS son: "Envío de ping"; "ping de la muerte", cuando se envían pings mal formados; "envío de malware" y "Botnet (Ro**bot-Net**work)", el cual explota vulnerabilidades de un *browser* para colectar computadoras zombies con la finalidad de ejecutar software malicioso.

Como recomendación de seguridad, se debe instalar la versión de java más recente en terminales y servidores, accdiendo con cierta frecuencia a https://www.java.com/es/download/, con la finalidad de varificar que cuenta con la versión más reciente de java para su browser y en caso de tener versiones obsoletas desinstalarlas, en su intento aparecerá un gráfico como el indicado en la figura V.46.

Fig. V.46. Actualización de Java para los browsers.

V.7 Autoevaluación para el capítulo V

1. Como ejercicio para diagramas UML de casos de uso, obtenga el diagrama de casos de uso para una memoria flash.
2. Como ejercicio para diagramas UML de casos de uso, obtenga el diagrama de casos de uso para una cámara fotográfica antigua
3. Como ejercicio para diagramas UML de casos de uso, obtenga el diagrama de casos de uso para una cámara fotográfica moderna.
4. ¿A qué refiere un DBMS?
5. ¿A qué refiere MySQL?
6. Describa el procedimiento de instalación de MySQL

PARTE III: LA CUARTA REVOLUCIÓN INDUSTRIAL

El progreso es imposible sin el cambio, y aquellos quienes no pueden cambiar su mente nada pueden cambiar.

George Bernard Shaw (1856-1950), Irlandes

Premio Nobel de literatura 1925

CAPÍTULO VI: LAS TIC EN EL SIGLO XXI

VI. Aplicaciones de las TIC en el siglo XXI

Toda tecnología creada busca resolver problemas de una sociedad, el actual mundo interconectado busca resolver sus problemas empleando todas las herramientas disponibles, nos encontramos en una época en la que se emplea todo el conocimiento de distintas áreas apoyadas en las TI. Es por ello que las computadoras, las comunicaciones, las personas y cosas dejan de concebirse como entes separados, las ciencias de la vida, las fuentes de energía y prácticamente toda área del conocimiento y tecnologías se integran. En este capítulo se hace una revisión general de las tecnologías que están en pleno auge desarrollándose para gestar la "cuarta revolución industrial", tales como: las ciudades inteligentes (*Smart Cities*), las redes eléctricas inteligentes (*Smart Grids*), el internet de las cosas (*Internet of Things* - IoT), los grandes datos (*Big data)*, la computación la nube (C*loud computing),* los centros de datos (*data centers)* y la seguridad cibernética (cyber security), como algunas de las principales tendencias en tecnologías de la información y las comunicaciones. Las tecnologías citadas conforman lo que llamo "el ecosistema del futuro tecnológico en las TIC" que impactará también buena parte del futuro de la humanidad, en el que las ciudades inteligentes son el gran integrador de las TIC, lo cual resumo en la figura VI.1. Cabe mencionar que IEEE mantiene 6 iniciativas de las 7 indicadas anteriormente.

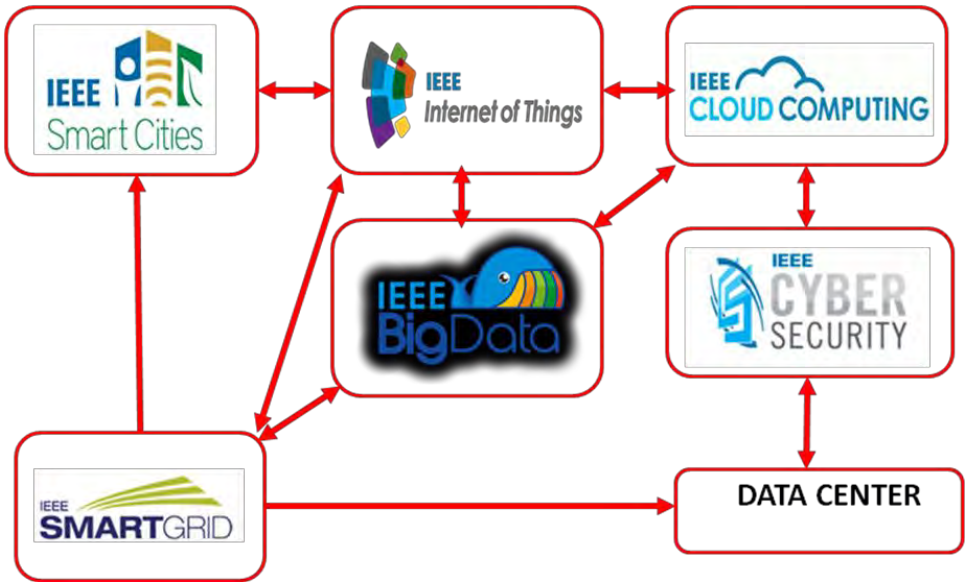


Fig. VI.1. Ecosistema tecnológico para la humanidad en el siglo XXI. (Used by permission of the IEEE Computer Society. All rigths reserved)

VI.1 La computación en la nube

La primera ola de la computación se originó desde que estuvieron disponibles las primeras computadoras comerciales del tipo mainframe en 1950 y durante el desarrollo de las midicomputadoras, minicomputadoras, estaciones de trabajo y hasta finales de la década de los 70.

La segunda gran ola de la computación se originó en la década de los años 80, con la llegada de las computadoras personales, cuando las redes de computadoras se hicieron masivas gracias a la miniaturización, el bajo costo de los circuitos integrados de alta escala de integración, los sistemas operativos y lenguajes de programación, los cuales eran más fáciles de manejar. En aquella época se popularizó la arquitectura "cliente-servidor", en la que varias computadoras personales o estaciones de trabajo se conectaban a servidores, gracias a los módems, inventados en los 70 para usar las líneas telefónicas PSTN. La arquitectura cliente-servidor permitió compartir archivos, los cuales eran distribuidos desde servidores específicos, de modo que se mejoró el rendimiento de los equipos, concentrando la información y evitando así realizar copias que involucraran movimientos de archivos de un lugar a otro físicamente. Los servidores más populares de la época fueron los de correo electrónico y los de transferencias de archivos. En 1990 se popularizaron los servidores web, más tarde los exploradores o "browsers" como "explorer" o "chrome" que facilitan mucho la navegación en internet, la cual tuvo un crecimiento exponencial hasta el punto que desapareció ARPANET y las redes que lo constituían se desintegraron. En 1995 nace formalmente el internet comercial y el mundo deseaba conectarse a internet; la gente compraba una computadora y compraba el software, el cual venía en discos y empaquetado en una caja. Por su parte las empresas tenían departamentos de informática o computación, compraban grandes cantidades de computadoras, software, garantías, servicio y soporte técnico; a esta se le llamó la tercera era de la informática. Internet había experimentado un gran crecimiento, había servidores por todas partes, sin embargo, se desperdiciaba memoria de trabajo o RAM, procesador, disco duro, energía, etc. En 1999, ya se encontraba madura la "virtualización" de la memoria, procesadores y discos, en general había madurado la "virtualización de servidores" y con ello creció de manera exponencial el número de servidores virtualizados conectados a internet, con lo cual nació la tercera ola de la computación. Con la virtualización, se redujeron enormemente los tiempos muertos que tenían los recursos de las computadoras, se elevó la eficiencia en la transferencia de la información y en el consuno de energía. Con la virtualización de servidores varias aplicaciones de software podrían emplear

físicamente un mismo servidor o distintos servidores haciendo la ejecución de las aplicaciones web mucho más rápidas y eficientes.

La cuarta gran ola de la computación, lo constituye la computación en la nube, la cual se da como una consecuencia lógica de la virtualización a gran escala, pero sobretodo por una tendencia mundial en la que todo ya se terciarizaba (outsourcing). En este siglo se hizo una práctica común que las empresas contratan de manera externa los servicios de limpieza, comida, servicios profesionales, internet, nómina, mantenimiento, autos, casas, bodegas, educación, entretenimiento, etc., "todo como un servicio" (E*verything As A Service*). Así las empresas de diferentes rubros que durante las décadas de los años 80 y 90 habían creado nuevos departamentos y posiciones para telecomunicaciones y computación, para la primera de cada de 2000 se fueron transformando, "modernizándose" en los citados rubros hacia la terciarización como en el resto de los servicios. La crisis económica para las empresas "punto com" del año 2002 aceleró el hecho de que la tendencia mundial de terciarizar alcanzara a la computación y las telecomunicaciones, con lo que se llegaba las TIC como un servicio. Como consecuencia de maximizar la eficiencia en el uso de servidores, se popularizaron los grandes centros de datos, verdaderos bunkers diseñados para albergar miles de servidores con "toda" la seguridad, para soportar de manera natural la computación en la nube. La figura VI.2 muestra una de las representaciones abstractas de la computación en la nube.

Fig. VI.2. Representación abstracta de "Computación en la nube" (archivo del autor)

La figura VI.3 muestra un diagrama que incluye las 4 olas de la computación.

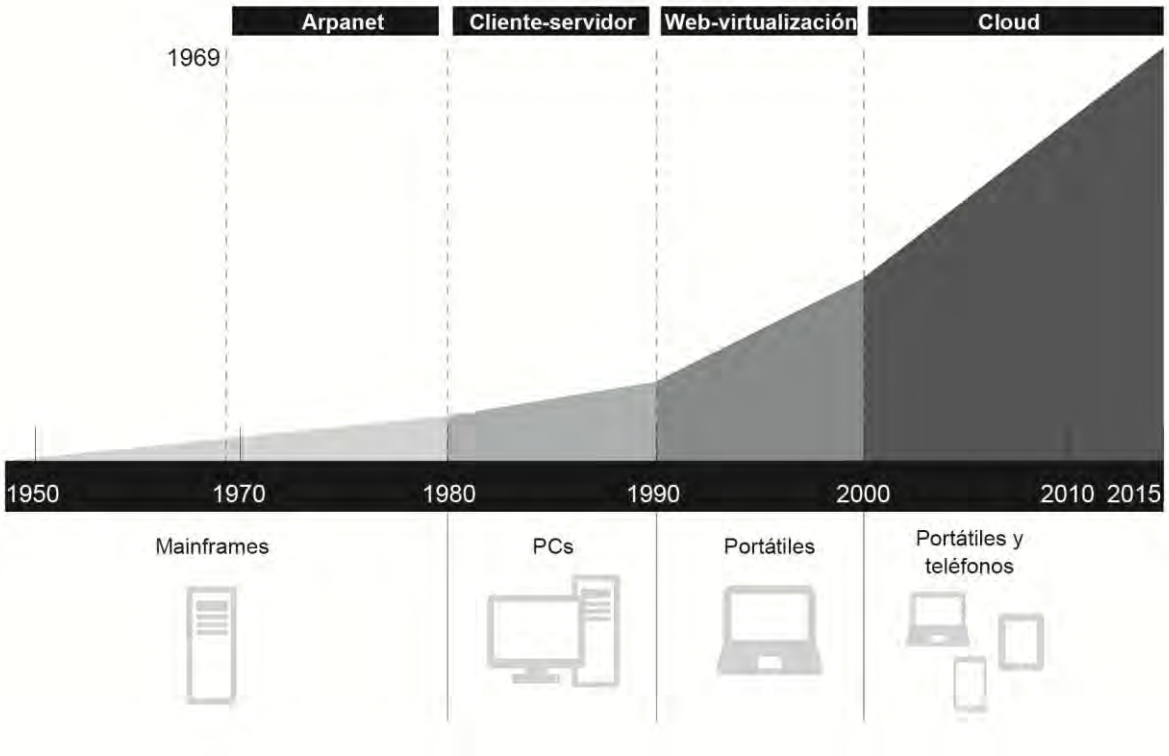


Fig. VI.3. Las 4 olas de la computación, una aproximación en el tiempo.

El Instituto Nacional de Normalización y Tecnología de EEUU (NIST) define computación en la nube como "un modelo de las tecnologías de la información que permite proveer servicios de computación bajo demanda y a bajo costo". VMware, pionera de la virtualización y la computación en la nube, define computación en la nube como un enfoque de computación que libera servicios eficientemente bajo demanda, son autoadministrados y con infraestructura virtual.

Con la computación en la nube, tanto el *software* como el *hardware* se venden como un servicio, de modo que ya no es necesario comparar una licencia de software, basta con conectarse a internet, usar software y pagar sólo por el tiempo que se use. Por ejemplo, Google, así como otras compañías, provee el correo electrónico y varias aplicaciones de *software* como calendario, hojas de cálculo, traductores, etc. desde la nube, es decir, las aplicaciones corren en los servidores y no necesitan instalarse en la computadora del usuario.

La computación en la nube pretende ofrecer todos los servicios de computación bajo un determinado modelo de servicio, por ejemplo, el modelo software como un servicio (SaaS), provee las aplicaciones de software para usuarios finales, como correo electrónico (gmail), software ofimático (google docs), almacenamiento de archivos (drive, icloud, dropbox, skydrive), etc. vía internet. Del mismo modo el modelo plataforma como un servicio (PaaS) provee las plataformas

para el desarrollo de software como lenguajes de programación, sistemas operativos y sus bibliotecas vía internet para que no tengan que instalarse en la computadora cliente, va dirigido a desarrolladores de aplicaciones. El modelo infraestructura como un servicio (IaaS) provee la infraestructura física que permita a su vez soportar PaaS y SaaS como servidores físicos, redes, switches, routers y laboratorios de computadoras vía internet, este servicio es muy atractivo para las instituciones dado lo caro que resulta montar laboratorios por la acelerada obsolescencia de los equipos electrónicos, aunado a la consecuente generación de residuos a partir de "equipos eléctricos y electrónicos" (WEEE- Waste of Electrical And Electronic Equipments) [107]. La IaaS va dirigida a administradores de servidores redes y sistemas, en este caso el consumidor no administra o controla la infraestructura que lo soporta, pero tiene control sobre todos los sistemas operativos, almacenamiento y las aplicaciones.

Por su parte el NIST define a la IaaS "como la capacidad proveída a un consumidor de recursos de cómputo para procesar, almacenar información, proveer redes y otros recursos donde el consumidor es capaz de ejecutar software que incluye sistemas operativos y aplicaciones; el consumidor no tiene control sobre la infraestructura de la nube, pero si sobre el SO, las aplicaciones, el almacenamiento y algunos componentes de red como servidores y firewalls".

Existen otros modelos de servicios de computación en la nube para servicios de las TIC, todos soportados por centros de datos. Algunas de las principales empresas que proveen los servicios de nubes IaaS son Amazon Web Services, VMware, Skytap, Bluelock.

Sin duda la virtualización es necesaria para la computación en la nube, ya que la virtualización es la que ofrece la computación elástica para proveer la escalabilidad, también es la que permite compartir recursos, el balanceo de cargas, la portabilidad y la alta disponibilidad. En el año 2009, la computación en la nube dio un salto histórico, muchas compañías públicas y privadas usan la nube, en alguna de sus tres modalidades ya sea usando nubes públicas o nubes privadas o hibridas. Ya en la actualidad varias instituciones y gobiernos usan alguna de las tres modalidades.

La nube permite que las instituciones de educación en todos los niveles y centros de investigación dejen de hacer grandes inversiones en equipos que pronto se hacen obsoletos, haciendo uso de software, plataformas o la infraestructura en su caso. Un ejemplo claro en la transformación de las bibliotecas se dio en universidades de los EEUU, principalmente en la universidad de la defensa de los EEUU, donde en lugar de proveer a los estudiantes de libros físicos, se les proveía desde la inscripción a sus cursos los lectores de libros *Kindle*, los cuales ya podrían contener cientos de libros precargados o incluso conectarse a la nube para descargar otros en tiempo

real. Cada estudiante de la citada universidad recibe un libro electrónico con todos los libros electrónicos indicados en los temarios, tanto los textos principales como los complementarios y sugeridos. Mediante el uso de los libros electrónicos, un estudiante no tiene necesidad de acudir a biblioteca alguna, esto también permite a las instituciones reducir sus inversiones en instalaciones de bibliotecas y permite otorgar un servicio mucho más dinámico, lo cual implica un ahorro de tiempo de transportación, energía y por ende contribuye a una menor contaminación por emisiones de carbono.

Una aplicación típica en la nube es el servicio de videoconferencia que ofrece Cisco mediante la aplicación *WebEx*, una pantalla sobre la aplicación se muestra en la figura VI.4. En la parte superior derecha se ubica el área de participantes.

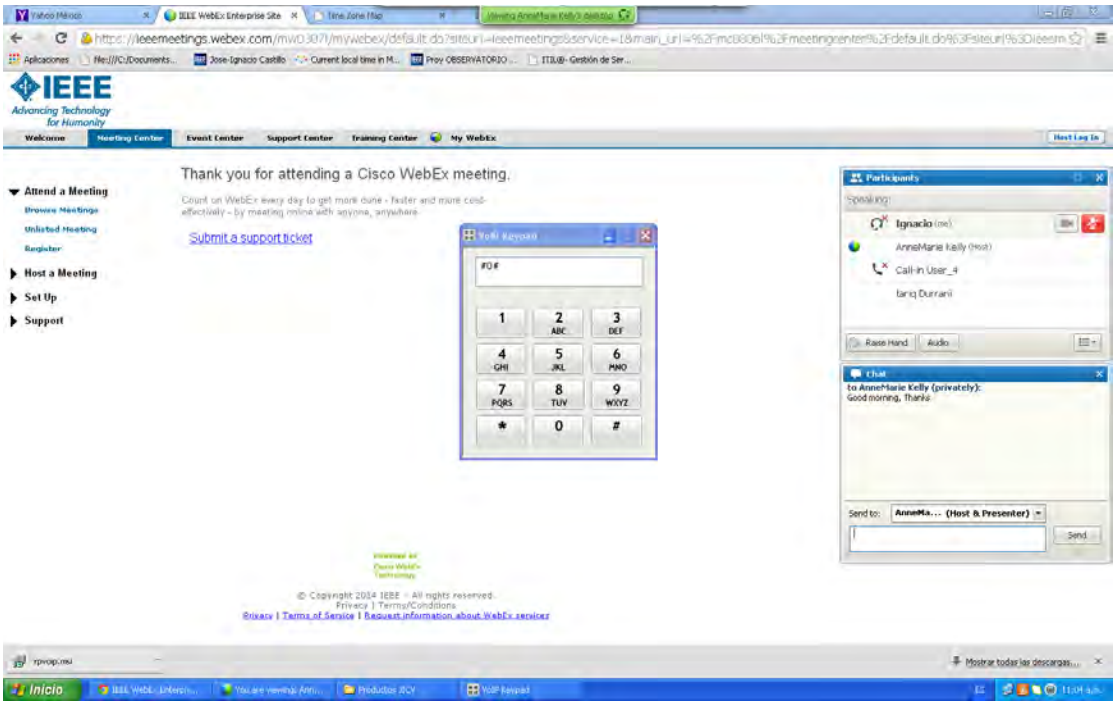


Fig. VI.4. Uso de Webex en una conferencia a distancia de IEEE.

Por otro lado, desde el nacimiento de las computadoras las interfaces comunes fueron las tarjetas perforadas, después las CLI facilitaron la popularidad de las computadoras, pero sobretodo las GUI que se popularizaron con los *browsers* que empleamos en la internet. Al final de la primera década de 2000, en la plena cuarta ola de la computación aparecen ya maduras las interfaces naturales de usuario (*Natural User Interface*-NUI), misma que para el año 2014 se encuentran a punto de iniciar algo más que solamente una moda [108].

En México, algunas escuelas primarias, secundarias y preparatorias ya se emplean soluciones *Cloud* para no invertir en los tradicionales laboratorios de computación. Por su parte, algunas universidades ya usan sus sistemas de correo con Google en lugar de contar con su propia infraestructura. Por su parte el gobierno de México, en 2013, planeó contar con su propia nube privada, y para el caso de la modernización de CFE también se contempló una reestructuración mediante la migración de sus centros de datos hacia una nube privada. Una de las primeras aplicaciones de los servicios que proveía el gobierno de México vía computación en la nube fue para 2014, el servicio de pago de impuestos vía el SAT, la oficina de recaudación de impuestos, desafortunadamente el servicio fue bastante irregular, el gobierno prometió el reintegro del importe deducible en 5 días, en realidad el promedio fue de aproximadamente 31 días, sólo dentro del DF. Algo similar sucede con la mayoría de las compañías proveedoras de servicios "cloud", la madurez todavía está por llegar.

VI.1.1 La iniciativa IEEE Cloud Computing

Por su parte la iniciativa "IEEE Cloud Computing" impulsa el desarrollo de la computación en la nube a nivel mundial [109]. Evidentemente aunque la computación en la nube presenta muchas ventajas reales y potenciales, también está siempre presente el gran inhibidor al crecimiento acelerado de la computación en la nube, la seguridad cibernética, todo un tema aparte, razón por la que en una posterior sección se abordará el tema de seguridad en la información [110]. Para mayor información visite su web site cloudcomputing.ieee.org

VI.2 El internet de las cosas

Desde el nacimiento de las redes de datos, pasando por su estandarización para obtener la interoperabilidad hasta su uso generalizado se experimentó con redes de extensión pequeñas como las redes PAN (*Personal Area Network*), medianas como LAN (*Local Area Network*), grandes como MAN (*Metropolitan Area Network*) y grandes como WAN (*Wide Area network*). Si nos preguntamos qué tan pequeñas pueden ser esas redes, llegamos al año 2000, para poder contar con redes de computadoras integradas por computadoras de 1mm cúbico, cada una de ellas integrada por sensores, actuadores y medios de comunicación inalámbrica, conocidas como el polvo inteligente (*Smart Dust*). La miniaturización también se llevó a los satélites y en la misma década se lanzaron satélites de $1cm^3$. Si nos preguntamos qué tan grandes pueden ser esas redes, es claro que el mundo está interconectado por la Internet, pero desde 2010 se encuentra en desarrollo el internet interplanetario, primero se conectó a la Estación Espacial Internacional con la tierra, Marte está conectada con la tierra, aunque no como se concibe la interconexión comercial en la tierra, esa tarea debe completarse antes de colonizarla.

Pero qué estará conectado a internet, sencillamente todo. Todo objeto se conecta a internet y se llama el internet de las cosas, para el año 2025 se espera que más de 50 billones de objetos se encuentren conectados a internet y una gran cantidad de compañías se encuentran mirando en esa dirección, el internet de las cosas [111]. De acuerdo con Gartner en 2015 hay alrededor de 4.9 mil millones de cosas conectadas a internet y para 2020 se espera que hayan 25 mil millones de estas, por ello se insiste en que todas estas tecnologías indicadas en este capítulo están generando lo que llamamos la 4ta revolución industrial.

VI.2.1 La iniciativa IEEE Internet of things

IEEE cuenta con una iniciativa llamada “IEEE Internet of Things” [112]. Para mayor información visite su página web **iot.ieee.org**

VI.3 Centros de datos

Los centros de datos (Data Centers) son la infraestructura que soporta la computación en la nube, los centros de datos son construcciones físicas que tienen las instalaciones adecuadas de energía eléctrica, enfriamiento, seguridad física y salas para servidores y telecomunicaciones que permiten contener toda la infraestructura de tecnologías de la información. Por lo general para contar con centros de datos se requiere de fuertes inversiones por lo cual o se tiene un centro de datos propio o se renta, en este caso los centros de datos del tipo "colo" o "colocation" son unos de los preferidos para la computación en la nube. Los centros de datos del tipo colocation son aquellos en los que el dueño del data center provee las instalaciones físicas, los sistemas de enfriamiento, seguridad física, energía eléctrica, telecomunicaciones, racks para servidores, y algunos servicios de administración, mientras que el cliente que renta parcialmente espacios en el centro de datos pone los servidores y los equipos para almacenamiento.

VI.3.1 CENTROS DE DATOS TIPO COLOCATION

Para mediados de 2015 se estiman cerca de 3557 centros de datos del tipo "colocation" en 104 países, bajo una disposición aproximada a la mostrada en la figura VI.5.

Fig. VI.5. Mapa Google de los Centros de Datos del tipo "colo" en el mundo.

La distribución en América está liderada evidentemente por EEUU, el cual cuenta con 1,447 cuya densidad más alta está en California (193) luego Texas (144) y Nueva York (98). Por su parte

Canadá cuenta con 117, cuya alta densidad esta en Vancouver, Toronto (31), Montreal (27). En la figura VI.6 se muestran las distribuciones aproximadas de los centros de datos tipo colocation en EEUU y Canadá [113].

Fig. VI.6. Mapa Google de los Centros de Datos del tipo "colo" en EEUU y Canadá.

Por su parte España cuenta con 51 Centros de Datos ubicados principalmente en Madrid (17), Barcelona (13) y Valencia (5), mientras que Portugal cuenta con 25 ubicados en Lisboa (11) Porto (7) y Alentejo (2). Y para el caso de Latinoamérica se resume en la tabla VI.1.

País	Total	Ciudad de ubicación
Brasil	31	Sao Paolo (11), Rio de Janeiro (6)
México	11	DF (5), GDL(2), MTY=QRO (1)
Argentina	9	BA(8), Córdoba(1)
Costa Rica	7	San José (6), Alajuela (1)
Colombia	6	Bogotá (3), Medellín (2), Cali (1)
Chile	6	Santiago (4), Los Andes (2)
Uruguay	5	MTV (4), Maldonado (1)
Panamá	3	Panamá (3)
Bolivia / Venezuela	2	
Guatemala / Puerto Rico	1	

Tabla VI.1 Centros de datos tipo "Colo" en Latinoamérica

Por otro lado Google puso en funcionamiento su primer centro de datos en Latinoamérica en Quilicura, Chile. Google cuenta con un total de 13 centros de datos en el mundo; en América en Carolina del Sur, Carolina del Norte, Iowa, Georia, Oklahoma, Oregón y Chile; en Europa en Finlandia, Bélgica e Irlanda; en Asia en Hong King, Taiwán y Singapur (http://www.google.com/about/datacenters/inside/locations).

Se estima que en el mundo existen aproximadamente 1,300 centros de datos, de los cuales aproximadamente el 7% de ellos se encuentra en Latinoamérica. Google, por ejemplo, cuenta con 13 centros de datos repartidos en América, Europa y Asia. Aun cuando los centros de datos de las grandes corporaciones pueden ser de miles de metros cuadrados, como el de T-Systems en Brasil de 4,000m^2, la mayoría de los centros de datos en el mundo son de alrededor de 80m^2. En México desde el año 2000 se crearon centros de datos para empresas como Triara-Telmex (3 en Apodaca, NL y Querétaro), KIO Networks (3 en Querétaro, Santa Fe DF), RedIT (4 en Santa Fe DF y el Edo. de México). Alestra (5 en Guadalajara-01, Monterrey-08 y Querétaro-13), Axtel (3), Digital Reality (Querétaro), 1 para Produval, por citar algunos.

VI.3.2 CERTIFICACIONES PARA LOS CENTROS DE DATOS

La construcción y la operación de los centros de datos se rigen por certificaciones, tales como UPTIME e ICREA. UPTIME se rige por 4 niveles, que van de "TIER I" a "TIER IV", donde este último es el que presenta la máxima seguridad y disponibilidad. Por su parte ICREA tiene la norma ICREA-STD-131-2013, la cual cubre los métodos y procedimientos para el diseño y la construcción de las instalaciones que contienen los servidores y medios de almacenamiento, los sistemas de comunicaciones y la infraestructura asociada para operar un centro de datos. La norma de ICREA considera los aspectos eléctrico, de climatización, seguridad, las comunicaciones que debe considerar tanto el NOC (*Network Operation Center*) como el SOC (*Security Operations Center*) y la construcción física la que llama ámbito. ICREA usa 5 niveles para indicar el grado de redundancia con la que cuenta una infraestructura para proveer desde el 95% de disponibilidad en el nivel 1, conocido como el *Quality Assurance Datacenter* (QADC) hasta el nivel 5 para proveer una disponibilidad del 99.999%, el cual es conocido como *High Security, High Availiable World Class Quality Assurance* (HSHA-WCQA). En el rubro de universidades, la Universidad Autónoma de Nuevo León es la única universidad en México cuyo centro de datos cuenta con una certificación ICREA [114].

VI.3.3 CENTROS DE DATOS PARA APLICACIONES ESPECIALES

Entre los centros de datos para aplicaciones especiales podemos tener centros de datos para aplicaciones espaciales y para aplicaciones científicas especificas. En la figura X se muestra el centro de datos donde se reciben y tratan parcialmente datos del HAWC y el GTM en Puebla México. El centro de datos (figura VI.7) se ubica a la misma altura que el HAWC (figura VI.8a) es decir a 4,100 metros sobre el nivel del mar (msnm), mientras que el GTM se encuentra a 4,600 metros sobre el nivel del mar (figura VI.8b).

Fig. VI.7. Site a 4,100 mts. usados por los proyectos HAWC y GTM (archivo del autor).

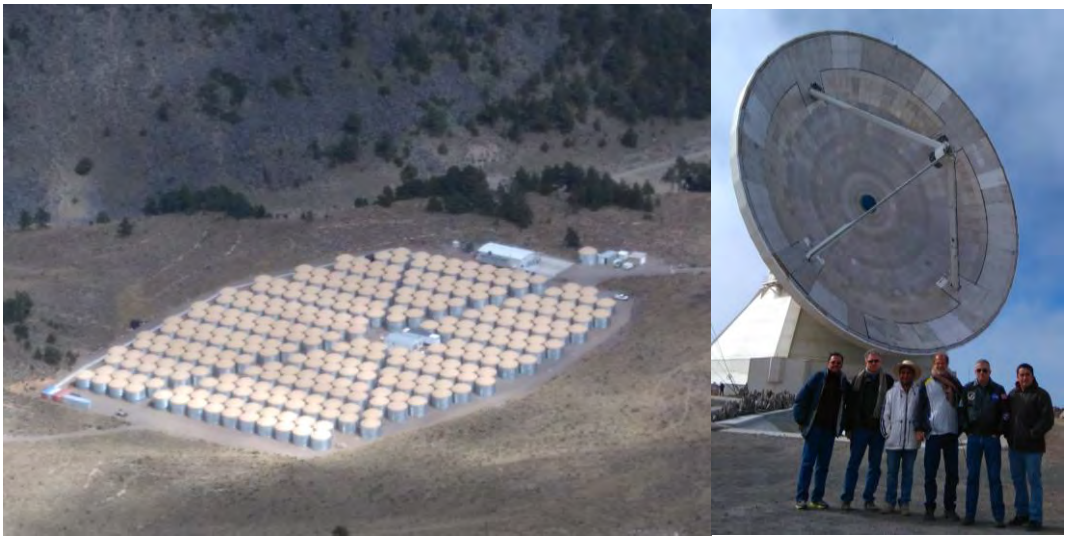


Fig. VI.8. (a) HAWC a 4,100 msnm. (b) GTM a 4,600 msnm (archivo del autor).

VI.3.3 Redes programables

Con la internet osificación mundial el manejo de las infraestructuras de internet se va haciendo día a día más compleja de modo que surgió la idea de la programación de redes con la finalidad de facilitar la evolución de internet. Bajo ese entendido las redes definidas por software (SDN-Software Defined Networks) constituyen un paradigma de red que permite desacoplar el hardware de las decisiones de control, con lo cual se pretende simplificar dramáticamente la administración de las redes. Es decir, así como los programadores han simplificado el almacenamiento y el desempeño de computación, lo hagan con las redes. Entonces en SDN se pretende dejar la inteligencia de red lógicamente centralizada en los *controladores con base en software*, lo que se llama el *plano del control*, mientras que los *equipos de red* se convierten en reenviadores de paquetes, lo que se llama el *plano de los datos*, mismos que se pueden programar vía una interfaz [115]. Luego entonces esto se hace muy llamativo para los interesados en el tema tanto que se ha creado la *Open Network Foundation*, una organización dirigida por la industria que promueve la estandarización del protocolo *OpenFlow*, esto muy en la línea del *Open Software Foundation* [116]. Por su parte en el lado académico *Open Networking Research Center* se dirige exclusivamente a investigación [117]. Para desarrollar servicios y protocolos con base en SDN se han desarrollado varia herramientas entre las cuales están aquellas para emulación y simulación como “mininet” y “ns-3”. Por su parte en términos de aplicaciones SDN están aquellas para redes empresariales, para centros de datos, redes de accesos inalámbricos dentro del contexto de conectividad ubicua incluyendo las redes celulares y las WiFi, las redes ópticas (SDON-Software Defined Optical Network) y las redes para hogares y negocios pequeños. Los servicios de la computación en la nube quedan soportados por data centers, todo dirigido hacia una alta eficiencia por el lado de la virtualización la eficiencia energética y la alta seguridad en las redes. Para los proveedores de servicios productos y los operadores de las redes, las redes definidas por software son una opción viable en términos de tecnología y de precio, sin embargo todavía se deben enfrentar algunos retos en términos de desempeño, escalabilidad, seguridad e interoperabilidad [118]. Por el lado de la virtualización y los servicios cloud existe aplicaciones como FlowVisor y AutoSlice, los cuales crean recursos de red, de modo que esto alienta la creación de centros de datos en la nube (cloud data centers) para proveer la infraestructura como un servicio.

VI.4 Redes de energía eléctrica inteligentes

Nuestra sociedad se apoya en distinta medida en tecnología, pero toda ella se fundamenta en la energía eléctrica, sin embargo, existen fugas, pérdidas y robos de energía, de modo que para hacer más eficiente la operación de las redes de energía eléctrica, se dota a ellas de cierto grado de inteligencia. Las redes eléctricas inteligentes son las redes de energía eléctrica a las que se les ha integrado una red de telecomunicaciones con la finalidad de que los operadores puedan colectar y analizar información acerca de la generación transmisión, distribución y consumo de la energía eléctrica para realizar la conexión y desconexión pertinente que le permita a la red eléctrica operar de una manera eficiente. Alrededor del mundo se van colocando medidores inteligentes y también paneles solares que permitan cierta autonomía a la iluminación ene carreteras, parques, jardines en las ciudades, las cuales tienen actualmente un novel reducido de inteligencia pero sobre las que poco a poco irá agregándose inteligencia en sus sistemas de control. La figura VI:9 muestra un caso típico en Bogotá Colombia, pero puede encontrarse prácticamente en todas las grandes ciudades del mundo.

Fig. VI.9. Instalaciones para aprovechar energía solar en Colombia.

La red eléctrica inteligente probablemente permita que se genere una red similar a la "internet" pero por su especificidad sería considerada una "ENERNET"[119].

Los sistemas que gobiernan a las subestaciones emplean sistemas SCADA (*Supervisor Control and Data Acquisition*), los cuales deben integrar protocolos y estándares que permitan la interoperabilidad entre los distintos equipos sensores y actuadores de diferentes fabricantes, para lo cual se han desarrollado estándares como los indicados en la tabla VI.2.

Estándar	Aplicación
IEC 61850	Sistemas y redes de comunicación (switches Ethernet en subestaciones) Para automatizar el suministro de energía eléctrica.
IEC 62351:	Seguridad en la comunicación de datos NERC-CIP.
IEC 61968	Interfaces de aplicación para la administración de la energía.
IEC 61400-25:	Comunicación y control para plantas de energía eólica.
IEC 1686	Seguridad para dispositivos electrónicos de interfaz en las subestaciones
IEEE 2030 **IEEE 1901/ IEEE 1547**	Para el almacenamiento y la distribución de la energía solar y eólica.

Tabla VI.2. Estándares empleados para redes eléctricas inteligentes

En México, la Comisión Federal de Electricidad (CFE-1937) es la empresa paraestatal dominante que cuenta con alrededor de 51,000 MW (2007) para 36 millones de clientes con incrementos anuales de casi un millón. En México la política energética busca el desarrollo de las redes eléctricas inteligentes, la meta es tener para 2025 una generación de energía con base en recursos fósiles máxima del 65% y el 35% con base en energía renovable. México ingresó al ámbito de las redes eléctricas inteligentes en 2007, cuando implementó los protocolos IEC 61850 y DNP3 (*Distributed Network Protocol* - protocolo de red distribuida) para sus sistemas SCADA del lado de las subestaciones, logrando con esto algunas subestaciones inteligentes. El protocolo IEC 61850 permite la interoperabilidad entre dispositivos Electrónicos Inteligentes IED (*Intelligent Electronic Devices*) de diferentes fabricantes.

Con la finalidad de implementar estrategias en *Smart Grid* se han realizado ya algunos programas pilotos desde 2012, por parte del área de generación ha habido proyectos de modernización y por parte de transmisión la modernización se centra en las "unidades de medición de fasorial" (PMU - *Phasor Measurement Units*). Por parte de distribución se han realizado básicamente 2 grandes proyectos para *Smart Grid* en medidores inteligentes, uno en la colonia Polanco de la ciudad de México donde se instalaron más de 26,000 medidores AMI y el otro proyecto se realizó en Acapulco, en el estado de Guerrero. La primera compra de medidores inteligentes de CFE se realizó en 2011, la siguiente fue en 2013. En 2013 y 2014 los medidores CFE-IUSA se han implementado como medidores digitales en varias Ciudades de México, los cuales permiten que una tarjeta de prepago o "tarjeta inteligente" registre el consumo mensual (el

cual se ha cobrado por décadas de manera bimestral) y con ello se permite la modalidad de pago programado mensual, de modo que la desconexión es automática en caso de falta de pago y la reconexión también es automática, sin embargo, este tipo de servicio no ha sido bien recibido [120, 121]. Sin embargo, el gobierno federal de México planeó en su PND (Plan Nacional de Desarrollo) de 2014, la inversión por 1 millón de nuevos medidores inteligentes AMI. En Centro América la organización que coordina la interconexión regional de los 6 países que la conforman es el Sistema de Interconexión Eléctrica para América Central (SIEPAC), cuya extensión de líneas de transmisión es de aproximadamente 18,000 kilómetros. Por su parte Costa Rica cuenta con el Instituto Costarricense de Electricidad (ICE) la empresa paraestatal dominante en el sector eléctrico, cuya capacidad instalada es de aproximadamente 2,700 MW cuya producción energética con base en energías renovables es del 69% (60% hidroeléctrica y 9% eólica). Costa Rica ingresó al *Smart Grid* desde 2010 y a la fecha presentan avances concretos en distribución, en términos de la implementación de medidores inteligentes. Por su parte Guatemala cuenta con el Instituto Nacional de Electrificación (INDE) como empresa paraestatal y el sector privado, juntos cuentan con una capacidad instalada de aproximadamente 2,200 MW (50% hidroeléctrica, 36 térmica, 11% biomasa y 3% geotérmica). Actualmente CFE de México le vende energía a Guatemala, directamente al INDE por más de 400 KW (vía 153 torres en 103 Km de líneas de transmisión). En El Salvador la Superintendencia de Energía y Comunicaciones (SIGET) es la paraestatal que suministra la mayoría de la energía pero la iniciativa privada participa en la generación y distribución, cuya capacidad instalada es de 1,400MW (47% térmica, 53% geotérmica e hidroeléctrica). El mayor riesgo al implementar *Smart Grid* está en dedicar muy poco a la planeación, de modo que emplear las TICS a las redes eléctricas sin verdadera inteligencia podría generar un monstruo con un punto único de fallo (PUF) [122].

VI.4 La iniciativa IEEE Smart Grid

Por su parte IEEE cuenta con la iniciativa "IEEE Smart Grid" desde 2009 [123]. Para mayor información visite su página web: **smartgrid.ieee.org**

La iniciativa IEEE Smart Grid cuenta con la colaboración de 12 de las 39 sociedades de IEEE, algunas de ellas Computer Society, Communication Society y Power and Energy Society. Esto ya que la colaboración transdisciplinar y multidisciplinar es necesaria dada la complejidad del Smart Grid, básicamente por 2 factores, uno es la interdependencia entre la infraestructuras heterogéneas (diferentes fuentes energéticas con sus propias variables y dependencias) y el otro es lo distribuido que se encuentran las funciones de monitoreo y control [124].

Aún cuando Smart Grid es de interés mundial, IEEE Smart Grid ha tomado el modelo conceptual del framework 3.0 de NIST Smart Grid, el cual consta de dominios o agentes participantes (generación, distribución, transmisión, proveedores de servicios, mercados, los usuarios y la operación) y de flujos tanto de energía eléctrica como de comunicación segura [125].

VI.5 Ciudades inteligentes

Cada día la población mundial en las ciudades aumenta de manera acelerada, por lo cual hay que resolver los problemas de infraestructura necesaria para proveer bienes y servicios para la alimentación, vivienda, salud, educación, transporte, energía, agua, recolección de residuos, seguridad, recreación, etc. Dado el rápido crecimiento poblacional y las crisis globales por los recursos, la idea de las ciudades que fuesen amables con el medio ambiente se hizo popular el término "ciudades sustentables", para lo cual ha sido necesario un cambio de mentalidad en la manera como nos relacionamos con el planeta. En términos prácticos, ya que cada ciudad en el mundo tiene sus propios problemas e intereses, cada una decide cómo usar su capital financiero y humano, para atender uno o varios de los rubros mencionados con el apoyo de la tecnología, principalmente con base en las TIC. Lo que se busca con estas tecnologías es proveer distintos grados de inteligencia a la gestión de servicios e infraestructura de una ciudad, lo que permitiría llamar a una ciudad, ciudad inteligente.

Podemos definir a una ciudad como una gran máquina económica y social, la cual cuenta con muchos retos para mantenerse saludable. Naciones Unidas estima que para 2030 más de 5,000 millones de personas vivirán en las ciudades y los problemas a las que se enfrentan actualmente las ciudades es diferente a los retos que enfrentaban hace 100, 50 o 10 años. Sin duda el mayor de los problemas en las ciudades es la distribución de la riqueza, hace 100 años, en 1914, Pareto midió la distribución de la riqueza en Italia y encontró que el 20 % de la población tenía el 80 % de la riqueza, esta es una relación llamada 20/80 con muchas aplicaciones principalmente en economía pero que alcanza casi todos campo de conocimiento. En 2014 se estima que el 1% de la población tiene el 99% de la riqueza, una medición de mayo indica que el 0.18% de la población mundial tiene el 48%, esta ridícula proporción será sin duda el principal obstáculo para la democratización en el uso de las tecnologías, además de considerar que actualmente el 70 % de las emisiones de carbono se generan en las ciudades. Es entonces que las ciudades deben readaptarse y reconstruirse o construirse nuevas ciudades con un enfoque y una visión holística que contemple todos los problemas urbanos; es por ello que una ciudad inteligente busca que una ciudad fusione las tecnologías tradicionales con las TIC para usar de manera más eficiente todos los recursos quede los que se alimenta para mantenerse como una ciudad viva; una "ciudad inteligente debe ser una ciudad económica social y ambientalmente sostenible". Sin embargo, existen corrientes que son todavía más completas y que buscan generar lo que llama "ciencias de la ciudad", en la que abarcan a las

ciudades inteligentes que a su vez se basan en las TIC, pero también incluyen diseño urbano y aspectos sociológicos [126].

La idea de las ciudades inteligentes inició alrededor de 1995 con el proyecto VENUS [127]. Ahora hablamos de ciudades inteligentes con gran soltura y extrapolando las realidades podemos partir de lo micro a lo macro, podemos pensar en las cosas de internet en la que se añade cierta inteligencia las cosas con computadoras de 1mm cúbico o más pequeñas que en suma ayudarían a contar con objetos inteligentes, casas inteligentes, edificios inteligentes, ciudades inteligentes, países inteligentes, continentes inteligentes, planeta inteligente, planetas inteligentes, etc. En todos y cada uno de esas aproximaciones están todos los elementos enunciados al inicio del capítulo, y basta con recordar que como una rama del futuro de internet contamos ya con el proyecto del internet interplanetario que busca conectar la Tierra, Luna y Marte vía internet, para que los futuros habitantes de Marte cuenten con internet antes de sus llegada y colonización.

En Europa existen al menos 70 proyectos de ciudades inteligentes de tamaño medio, entre 100,000 y 500,000 habitantes, para las que se usan 6 características y 74 indicadores, de modo que la ciudad de Luxemburgo en Luxemburgo ocupa la posición número 1 y Ruse en Bulgaria, la posición número 70. Las características que permiten definir el grado de avance que tiene una ciudad inteligente son: Economía inteligente, gente inteligente, vida inteligente, ambiente inteligente, movilidad inteligente y gobierno inteligente. Las TIC controlan: sistemas de distribución de agua, energía eléctrica, transporte, seguridad, manejo de residuos, alumbrado público, salud, educación, entre otros [128].

Algunos ejemplos de ciudades inteligentes que ya presentan excelentes avances son Masdar en los Emiratos Árabes Unidos, Barcelona en España, Songdo en Corea del Sur, Rio de Janeiro en Brasil; la mayoría de estos proyectos iniciaron en la primera década del siglo y deberían terminar en la segunda pero la crisis económica global ha forzado a que los proyectos se recalendaricen para la tercera década. Cabe resaltar que las empresas que tradicionalmente trabajaban en el área de telecomunicaciones como Cisco, Siemens e IBM, cuentan con sus programas de ciudades inteligentes que buscan la integración de una ciudad o parte de ella, y en particular Songdo es básicamente apoyada por Cisco, el sistema de transporte metropolitano de Nueva York en EEUU por Siemens y Rio de Janeiro por IBM [129-133]. Varias organizaciones empujan iniciativas relacionadas con las ciudades inteligentes, por su parte IEEE activó la Iniciativa "IEEE *Smart Cities"* desde 2013 [134]**.**

Para el caso de los sistemas de seguridad y vigilancia, ya son muchas las ciudades que cuentan con sistemas de vigilancia por cámaras. Para este tipo de sistemas existen fuertes

cuestionamientos por parte de grupos ONG, preocupados por el uso que se puede hacer de las imágenes, ya que si es cierto que la policía puede usar las imágenes para combatir el crimen, pero un dictador podría usarlo para combatir a sus disidentes [135].

En el caso de México el ritmo de crecimiento es de 1 millón de habitantes por año, por lo que para 2030 se estima que se necesitarán al menos 10 nuevas ciudades, las cuales deben ser planeadas, además del crecimiento que tendrán las tradicionales grandes urbes. Quizá en lo que algunas ciudades de México se encuentran más avanzadas es en seguridad. Por ejemplo, la Ciudad de México cuenta con un Centro de atención a emergencias y protección Ciudadana de la Ciudad de México (CAEPCCM), el cual cuenta con 4 Centros de Comando y Control (C2) y un Centro de Comando Control Comunicaciones Cómputo (C4), desde tales centros se monitorean las más de 8,088 cámaras de vigilancia llamados Sistemas Tecnológicos de Video Vigilancia (STVV), las cuales cuentan a su vez con una cámara, bocinas y botón de activación; algunas de las cámaras las portan drones [136, 137].

En la ciudad de Puebla se cuenta con un Centro de Emergencias y Respuesta Inmediatas (CERI), en Guadalajara y Monterrey se tienen centros equivalentes para respuesta a emergencias [138]. Además se usa conectividad a internet gratuita en el Zócalo de la Ciudad de Puebla, así como en el Zócalo y Alameda central de la Ciudad de México, por citar solo un par. En Tuxtla Gutiérrez Chiapas, entre 2009 y 2013 funcionó un programa llamado taxi vigilante, en el cual alrededor de 3,500 taxistas reportaban vía mensajes SMS y fotos, anomalías a un centro de gobierno vía teléfonos celulares cuyo servicio lo proveía la compañía Iusacell. Existen en otras ciudades esfuerzos aislados no coordinados que formalmente no constituyen ciudades inteligentes, pero que son una muestra de la necesidad de que una ciudad opere de una manera más eficiente [139,140].

Fig. VI.10. "Smart conectivity" aplicada en la Ciudad de Puebla, la Ciudad de México, así como en la mayoría de las ciudades con más de 1 millón de habitantes en el mundo desde el año 2015(archivo del autor).

Uno de los más importantes objetivos de emplear simuladores de ciudades con modelos cada vez más cercanos a la realidad es el de evitar o predecir la caída de ciudades. Tradicionalmente la caída de los imperios se relacionaba directamente con las ciudades que les hicieron grandes. Si damos un vistazo a la historia de Cleveland, Ohio, EEUU, en 1920 era la 5ta ciudad más grande de los EEUU impulsada por el monopolio petrolero en EEUU desde 1890, cuyo dueño fue John Davison Rockefeller, el emprendedor estadounidense por excelencia del siglo XIX. Sin embargo, con el tiempo la importancia de Cleveland fue cayendo, de manera dramática en las décadas de los 50 y de los 70 y 80, cuando el epicentro del empredurismo se movió a Silicon Valley en California con la industria electrónica. En 2013 Cleveland se ubica en el lugar número 47 de las ciudades más grandes y dentro de las 10 ciudades más peligrosas de EEUU. Otro ejemplo emblemático de ciudades que se desploman en EEUU es Detroit, Michigan, ciudad donde se fundó la Ford Motor company a principios del siglo XX, en 1903, inventando la producción en masa vía las líneas de producción, siendo en 1920 la cuarta ciudad más poblada de EEUU; en 2013 la ciudad de Detroit se declaró en bancarrota y en los últimos años es la ciudad más peligrosa de aquel país, y como estos ejemplos cualquier número en ciudades de todo el mundo en tan sólo casi 100 años.

VI.5 La iniciativa IEEE Smart Cities

Por su parte IEEE cuenta con la iniciativa “IEEE Smart Cities” desde 2014. El autor forma parte del comité evaluador. Para mayor información visite su página web: **smartcities.ieee.org** [134]

VI. 6 Seguridad cibernética

Toda nuestra sociedad actual se apoya en distinta medida en tecnología, dependiendo del país del que se trate, y ésta a su vez en la internet, desde las relaciones humanas y laborales vía las redes sociales, pasando por los servicios de salud, de educación, financieros, gubernamentales, de transporte, de seguridad en todos sus ámbitos, las redes de energía eléctricas inteligentes y las ciudades inteligentes, incluyendo las guerras, por eso, la seguridad de la información y el ciberespacio son los temas más delicados para toda institución o empresa pública y privada. Alrededor del mundo se generan sistemas que permiten gestionar la información y otros que se ocupan de la seguridad de la información, por lo que se trabaja en generar estándares internacionales. Y bien demos una mirada hacia el origen y evolución de lo que nació llamándose seguridad de la información, y que al crecer en el ámbito de internet ahora llamamos seguridad cibernética.

VI.6.1 Antecedentes

Si bien recordamos la carrera de las primeras computadoras comerciales de propósito general inició en 1950 en Alemania. En la década de los 60 se hicieron muy populares las *mainframes* y posteriormente nacieron las primeras redes de computadoras en EEUU y el Reino Unido. Para 1965 las computadoras de la tercera generación, aquéllas hechas completamente con circuitos integrados, eran ya muy populares, así como en cierta medida la compatibilidad del software. En 1968 con el desarrollo de varios programas, incluyendo el espacial de EEUU, los proyectos de desarrollo de software ya mostraban un patrón, no se entregaban en tiempo y forma, y estaban fuera de presupuesto, por lo que se acuñó el término "crisis del software", la cual incluía ya problemas en la seguridad de la información. Para 1969 nació formalmente ARPANET y en 1971 se creó “creeper”, un programa informático que se copiaba y propagaba dentro de las mainframes de ARPANET, particularmente ejecutándose en equipos DEC-PDP-10; sin embargo, fue hasta la década de los 80 que se acuñó el término “virus informático”, cuando las computadoras personales se usaron masivamente [141, 142].

Dada la complejidad de los sistemas informáticos, para 1984 el gobierno del Reino Unido creó un modelo de mejores prácticas para la gestión de la información: ITIL (*Information Technology Infrastructure Library*) y dada su calidad, la empresa HP la adoptó en la década de los 90, ayudando a su vez a que ITIL se hiciera popular por su énfasis en las mejores prácticas. En esa misma década se hizo popular el término "seguridad informática" [143].

VI.6.2 Propiedades de la información

Para el año 1995, el tema de la seguridad de software cobró gran importancia, ya que los EEUU liberaron el control de internet y para 1997 *Charles Plefeer* generó una clasificación de las propiedades de la seguridad de la información, en la que indicó que éstas son: confidencialidad, integridad y disponibilidad (CID).

En 2001 Peltier definió a la seguridad como "el uso de controles de acceso a los datos físicos y lógicos para asegurar el uso apropiado de datos y prohibir la modificación, destrucción, pérdida o accesos no autorizado a los archivos o registros manuales o automáticos de maneras no autorizadas o accidentales, así como la pérdida o daño o uso incorrecto de la información", esta es una definición bastante completa aunque muy general.

En 2003 Matt Bishop publica su libro *Computer Security; Art & Science*, en la que provee una de las definiciones más formales de seguridad informática como "una colección de atributos que capturan muchas dimensiones de seguridad, por lo que para medir la seguridad se deben usar varias métricas, que contemplen metas, audiencias y propósitos"; de esta manera toda medición tiene dos propósitos: la evaluación y la predicción, ambas necesitan modelos y estándares.

En 2006 Flavian y Guinal definieron a la seguridad como "la garantía técnica para el cumplimiento de los requerimientos legales y las mejores prácticas", dando un giro muy al estilo de las normas ISO y otros estándares internacionales, dejando listo el terreno de estándares más globales para generar definiciones y prácticas más adecuadas con los retos que se presentarían en años posteriores. La tabla VI.3 muestra algunas propiedades básicas y extendidas de la seguridad de la información y las vías con las que se asegura su cumplimiento.

Propiedades	Vías (el cómo)
1. La **confidencialidad** impide la divulgación de información a personas o sistemas no autorizados. ***Sólo personal autorizado accede a la información***.	El cifrado de los datos durante una transferencia electrónica. La NSA viola la confidencialidad con las puertas traseras de los estándares de cifrados.
2. La **integridad** busca mantener los datos libres de modificaciones no autorizadas. La integridad de la información se asegura ***solo si el personal autorizado modifica la información.***	Vía la firma digital durante la transferencias electrónicas.
La **autentificación** se da si el usuario es quien dice ser, es decir no existe suplantación de identidad.	Claves y métodos de ingreso a un sistema
No repudio: [ISO-7498-2] Quien envía no puede decir "yo no lo envie" y quien recibe no puede decir "yo no lo recibi".	Enviando notificaciones de envío y recepción tanto para quien envía como para quien recibe. Ej. servicio SMS
3. La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad se asegura cuando ***el personal autorizado dispone de la información en cualquier momento.***	Alta disponibilidad, vía SLA y que no exista denegación del servicio.

Tabla VI.3. Estándares empleados para redes eléctricas inteligentes

VI.6.3 Administración de la seguridad informática

Con base en las necesidades de empresas públicas y privadas se generaron estándares relacionados con la administración de los servicios de la tecnología de la información, como ISO/IEC 20000 o ITIL (Information Technology Infrastructure Library), en las que se plantean las mejores prácticas para la administración de servicios de las tecnologías de la información (TI) mediante el alineamiento de los servicios de TI a las necesidades del negocio. ITIL nace en 1984 desde el gobierno del Reino Unido y dada su calidad, la empresa HP la adopta en la década de los 90, ayudando a su vez a que ITIL se hiciera popular por sus énfasis en las mejores prácticas, incluso en su versión de 2007. La versión de ITIL para 2011 agregó características de *cloud computing* y la parte medular de gestión de servicios de TI quedó como una buena base del estándar ISO 20000.

En 2005 se creó la familia de estándares ISO/IEC 27000 para los sistemas de gestión de la seguridad de la información. ISO/IEC 27000 se compone de varios estándares, entre ellos el 27000, el cual provee la introducción y generalidades en similitud al ISO 9000; el 27001 indica los requerimientos para un sistema de gestión de seguridad de la información (SGSI), el 27002 como un código de prácticas para los SGS. Por su parte el 27011 (2008) es una guía para la implementación de SGSI para telecomunicaciones, el 27033 sobre la seguridad en redes y particularmente el 27032 (2010) trata sobre la seguridad cibernética. Tanto ISO/IEC 20000 como ITIL e ISO/IEC 27000 cuentan con especificaciones, mejores prácticas y aspectos de implementación.

VI.6.4 Seguridad cibernética y espacio cibernético

El término *seguridad cibernética* nació de la ficción científica en la década de los 1980 y se popularizó a principios de los 2000, mientras que *cibernética* es un término acuñado por Norbert Wiener en la década de los años 40 para dar cabida a las "teorías de control" dentro de un marco de estudios más generales e interdisciplinarios llamado la "teoría general de sistemas".

A. ITU-2008

En 2008 la Unión Internacional de Telecomunicaciones de la ONU generó el estándar ITU-T X.1205, como "Redes de datos para la comunicación de sistemas abiertos y la seguridad de las telecomunicaciones". En el estándar ITU-TX.1205 se define a la *seguridad cibernética* como "un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, guías, la administración del riesgo, las acciones, mejores prácticas y tecnologías que se puedan usar para proteger los bienes de una organización y el uso del ciber espacio" [144]. Esta fue la primera vez que de manera formal se consideraron los términos "seguridad cibernética" y "espacio cibernético".

B. ISO/IEC 27032-2010

En 2010 el estándar ISO/IEC 27032 incluyó una guía general para la *seguridad cibernética*, tanto para los proveedores de servicios de comunicaciones, como para los usuarios de internet con tal de que se reduzca el *spam*, los ataques de virus y las malas prácticas. La norma define *seguridad cibernética* como "la preservación de la confidencialidad, integridad y la disponibilidad (CID) de la información en el espacio cibernético"; razón por la cual también definió *espacio cibernético* como "el ambiente complejo resultante de la interacción de la gente, el software y los servicios de internet, soportado por equipos tecnológicos y redes interconectadas, las cuales no existen en forma física". El estándar también definió 4 tipos de amenazas al *espacio cibernético*: las amenazas a los bienes de las personas, a los bienes de las organizaciones, a los bienes virtuales y a las infraestructuras [145].

Este estándar que se encuentra en desarrollo, lo realiza el grupo de trabajo JTC 1/SC27, donde participan 47 países, 18 de los cuales tienen la categoría de observadores, México entre ellos. El JTC 1/SC27 se divide en 5 grupos de trabajo: el WG1 se enfoca en los Sistemas de Gestión de la Seguridad de la Información (ISMS-Information Security Management System); el WG2 en los mecanismos de seguridad y criptografía; el WG3 en los criterios para la evaluación de la seguridad; el WG4 en los servicios y controles de seguridad y el WG5 identifica las tecnologías de gestión y privacidad. A manera de resumen, la figura VI.11 muestra una línea de tiempo que incluye 12 hitos de la seguridad de la información, también se puede observar la trasformación desde la seguridad informática hasta la seguridad cibernética.

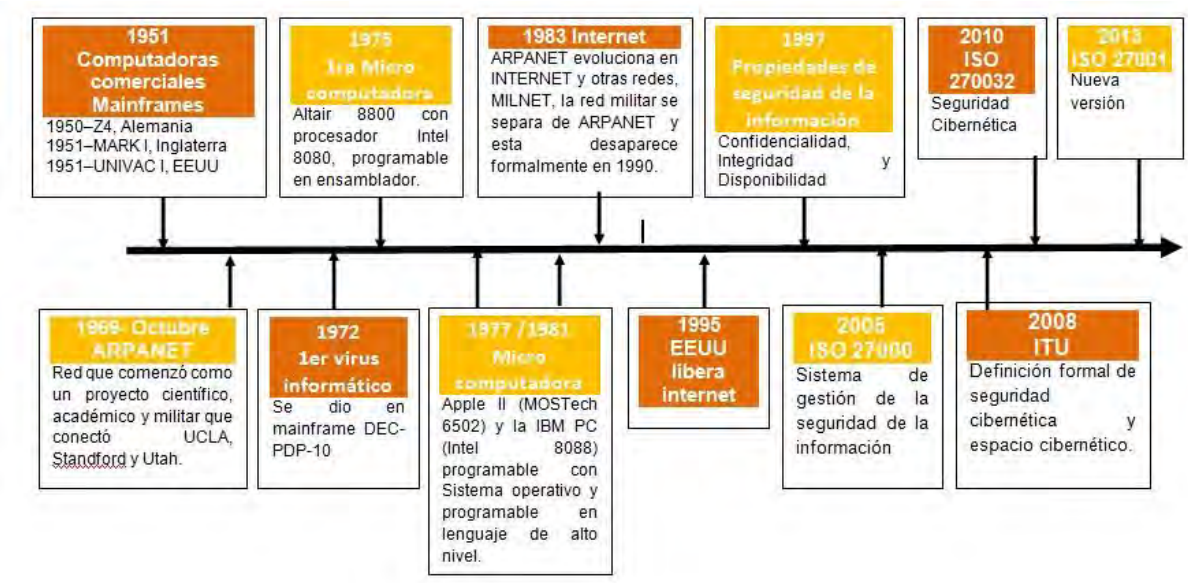


Fig. VI.11 Hitos de la seguridad de la información.

C. Gobierno de EEUU-2010

Desde el año 2010 la seguridad cibernética y el espacio cibernético han ido refinando sus definiciones, incluso el gobierno de los EEUU cuenta con sus propias definiciones. Para el 6 de diciembre de 2011 el gobierno de los EEUU generó el ***Trustworthy cyberspace: strategic plan for the federal cyber security research and development program***, documento en el que se imprime su propia definición de *espacio cibernético* y lo que el gobierno de EEUU considera necesario para mantenerlo a salvo, así como las acciones a emprender. Veamos pues la definición de seguridad cibernética del gobierno de los EEUU de diciembre de 2011 y sus áreas de acción generales:

A) Espacio cibernético: Es la infraestructura de la información interconectada globalmente, incluyendo internet, las redes de telecomunicaciones, los sistemas de computadoras y los sistema de control industrial. Entonces se destaca que: *"para mantener el orden público y el bienestar de la humanidad, el espacio cibernético debe ser protegido del malware, por lo cual el gobierno de los EEUU es responsable de encarar las vulnerabilidades estratégicas del espacio cibernético, para proteger a la nación y asegurar que sus ciudadanos puedan liberar todo el potencial que se da con la revolución de las tecnologías de la información".*

B) Las áreas de acción son las redes de energía, los servicios de salud, los servicios financieros, la defensa nacional y educación en seguridad cibernética, el transporte y la identidad cibernética.

En 2012 los EEUU lideran una amplia discusión sobre si es pertinente ejercer un control mucho más severo sobre internet [146].

VI.6.5 Ataques al espacio cibernético

En casi todo país, las instituciones públicas y privadas, gubernamentales o no, han sido atacadas por algún tipo de grupo inconforme, quizá el más conocido es el ataque del tipo "Denegación de Servicio del tipo Distribuido (DDoS-Distributed Denial of Service) realizado por "Anonymous". En México desde 2010 la caída de las páginas del gobierno se va haciendo costumbre vía este tipo de ataques, particularmente en el mes septiembre, por ejemplo, el ataque DDoS del 15 de septiembre de 2011 y duró al menos hasta el 20 de septiembre como se indica en la figura VI.12. Sin embargo, este tipo de ataques no tienen un impacto real sobre algún tipo de infraestructura.

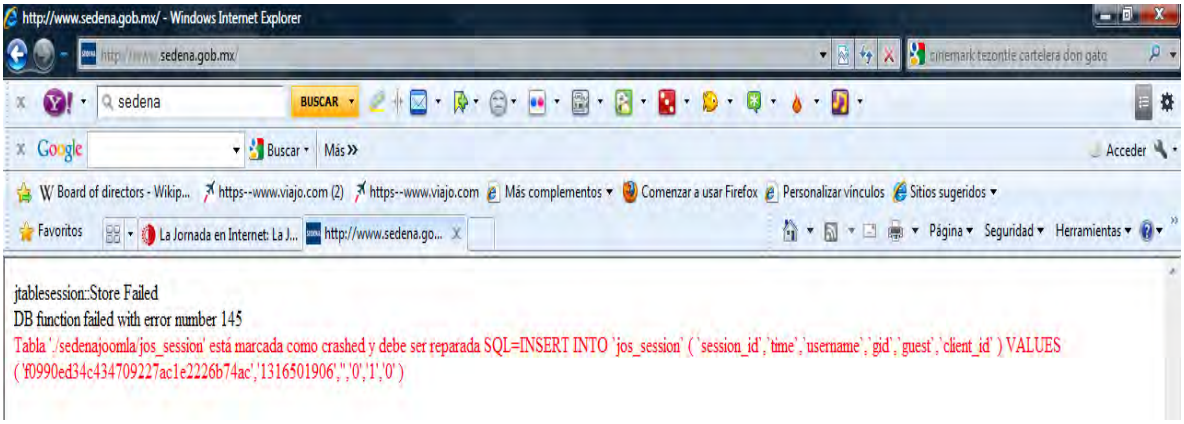


Fig. VI.12 . Caída de una página debido a un DDoS.

Ya que lo que nos interesa es mostrar cómo se encuentra el estado de los ataques cibernéticos sobre las infraestructuras críticas nos centraremos en el caso de EEUU, sin ser exhaustivos. Un problema mundial es pues el ataque cibernético o "ciber" ataques, que al menos desde el año 2011 llegaron a un punto crítico, año en el que se reconocieron ataques que lograron penetrar a 72 organizaciones alrededor del mundo, incluyendo los ataques a las infraestructuras críticas. Entre las organizaciones atacadas están la ONU, el FMI, y particularmente en EEUU, el Senado, la CIA, el Departamento de la Defensa (DoD) y el Departamento de Seguridad Nacional (DHS). En este punto cabe destacar 2 aspectos que preocupan al gobierno de los EEUU, y que deberían preocupar a cualesquier gobierno: uno es la vulnerabilidad de las redes de comunicaciones y el otro es el riesgo de ataque a las infraestructuras críticas. La red es vulnerable ya que el DoD cuenta con más de 15,000 redes y más de 7 millones de equipos conectados a éstas y todas están

conectadas a la internet; y el riesgo de ataque a sus infraestructuras críticas es que el 100% de éstas se encuentran conectadas a la internet, más aún, aproximadamente el 85% se encuentran controladas por empresas privadas y el 15% por el estado. También en 2011, el DoD estimaba que se requerirían de 250,000 expertos en seguridad cibernética desde ese momento y hasta el 2015, el problema es que urgen expertos y no hay todavía una masa crítica de ellos, lo cual representa un verdadero "Washington we have a problem"; "Where are the experts now?". Como parte de la estrategia para cubrir el requerimiento, la Universidad de la Defensa Nacional, en sus diferentes campus, el MIT Lincon Lab y la Universidad de West Virginia, entre otros, apoyarían con la preparación de futuros egresados para nutrir la CIA, el DOD y DHS, sin embargo, el senado todavía no había aprobado las inversiones requeridas incluso hasta el tercer cuarto de 2012. La gente capacitada iría a incrementar las filas de los más de 1000 expertos en seguridad para la División de Seguridad Cibernética (NCSD-National Ciber Security Division) de la DHS creada en 2003, y para cubrir las necesidades de las Divisiones de seguridad cibernética del DoD, NSA (National Security Agency) y la CIA. El DHS usa al US-CERT (Computer Emergency Readiness Team) para coordinar el Sistema de protección de seguridad cibernética nacional (NCPS-National Cibersecurity Proteccion System). Para octubre de 2011 se presentó en EEUU una iniciativa de antipiratería, particularmente el acta o ley del cese a la piratería en línea (SOPA-Stop Online Anti Piracy Act), la cual se encuentra en estado de espera. Antes de que se discutieran los últimos avances de SOPA, incluso sin haberse aprobado, el 19 de enero de 2012, el gobierno de los EEUU confiscó los bienes de Megaupload y en el lugar de su página web (www.megaupload.com) aparece el anuncio del gobierno de EEUU, mostrado en la figura VI.13. Megaupload ofrecía películas piratas, por la que generaron ganancias superiores a los mil millones de dólares.

Fig. VI.13. Estado de la página web de "megaupload" desde 19 enero de 2012

VI.6.6 Ataques cibernéticos a las infraestructuras críticas

Todo mundo es testigo de las diferencias entre el Oriente y Occidente pero particularmente con Medio Oriente. Para junio de 2010 se detectó un ataque cibernético de Israel hacia Irán, particularmente sobre una granja de centrifugadoras para generar uranio enriquecido; se calcula que se dañaron al 33% de las centrifugadoras en Natanz, Irán, lo cual aplazó el programa nuclear de Irán. Este ataque cibernético no tuvo precedentes, la *ciber arma* ***Stuxnet*** *no atacó a la información sino a la infraestructura*. Este hecho pone en alerta a todos los responsables de infraestructuras y se pone de moda nuevamente el sistema SCADA (Supervisory Control And Data Acquisition) más que nunca, tratando de combinar con sistemas de bastionado al puro estilo medieval. En este punto la informática forense en internet se hace muy interesante, al analizar el malware, las vulnerabilidades de los sistemas operativos y en particular los procesadores PLC MC7 de Siemens con los que contaban los controladores de las centrifugadoras atacadas. En términos generales **Stuxnet** buscó los controladores industriales de siemens números 315 y 417, introdujo un código de ataque vía los drivers de IRQ, tomó el control como si fuera el código original y ejecutó su propio código vía las interfaces de entrada y salida.

Para noviembre de 2010 se detectó un ataque sobre EEUU, alguien le atacó con DDoS siendo éste el más largo y grande ataque, que duró 7 días y 20 hrs, se reporta que fue detectado y rechazado. Para abril de 2011, Israel liberó a la ciber arma Duqu, la evolución de Stuxnet, su objetivo fueron las instalaciones militares de Alghadir Bidganeh en Irán; el principal daño fue la explosión de un misil Sejil-2 durante las pruebas, matando a científicos, ingenieros y militares de alto rango, 16 en total. Sin embargo, el hecho que aceleró el documento del gobierno de los EEUU del 6 de diciembre de 2011, fue el ataque que sufrió EEUU, en noviembre de 2011, con una arma cibernética que afectó las bombas de agua en Springfield Massachusetts, las cuales fueron encendidas y apagadas constantemente hasta que se dañaron. La dirección IP desde la cual se recibió el ataque fue de Rusia pero no se pudo determinar con precisión el origen ni a sus responsables. La tabla VI.4 muestra qué es y qué no es un arma cibernética; en ese contexto una guerra cibernética es diferente de una guerra convencional ya que no tiene fronteras.

Las ciber armas son	Las ciber armas NO son
Armas para destruir o afectar objetivos físicos militares o industriales estratégicos	**Armas de espionaje industrial**
Armas que actúan sobre controladores para los cuales no existen antivirus.	**Dedicadas a robar o borrar información**

Tabla VI.4. Qué son y qué no son las armas cibernéticas

Las ciber armas conocidas hasta hoy son 5: Stuxnet, Duqu, Flame, Gauss y Mahdi, de ellas las 4 primeras pertenecen a la misma familia. La primer ciber arma fue Stuxnet, Duqu fue una versión mejorada y todavía más Flame, la cual se autodestruye para intentar no ser detectada. De acuerdo con los informers de ENISA (European Network Information Security Agency) EEUU através de la CIA y la NSA en colaboración con Israel crearon Flame para atacar infraestructura militar de Irán, quien lo detectó en mayo de 2012. Finalmente se presenta en la tabla VI.5 las armas cibernéticas conocidas hasta el momento [147].

Armas cibernéticas	Algunos datos
Stuxnet (creada entre 2008-2009)	Descubierta en junio de 2010, pero se presumen ataques desde 2009. Atacó a Irán, sobre sistemas operativos de los PLC de Siemens.
Duqu (creada entre 2007-2011)	Descubierta en 2011. Atacó a Irán y Sudán en 2011
Flame (creada entre 2006-2011)	Descubierta en mayo de 2012. Los ataques se registraron en 7 países en 2012, sobre el sistema operativo Windows
Mahdi	Ataques en 2012, en medio oriente, EEUU y Reino Unido.
Gauss	Ataques en 2012

Tabla VI.5. Armas cibernéticas y datos generales

La tabla VI.5 sólo muestra algunos datos sobre los primeros ataques pero cada gusano a la fecha ha atacado a cada caso a más de 10 países cada uno. Alrededor de este tema los medios como siempre sucede dan espacio para muchas especulaciones, por lo que se debe ser cuidadosos con las fuentes de información.

Los ataques cibernéticos en los aeropuertos son un ejemplo típico de la actividad en el ciberespacio, tan solo en 2011, el aeropuerto de Los Ángeles en EEUU recibió 2.9 millones de intentos de ataque, los cuales fueron bloqueados, sin embargo, algunos más no pudieron bloquearlos, incluyendo a los sistemas SCADA del aeropuerto. Por su parte el secretario de la defensa de EEUU consideraba el peligro de los ataques cibernéticos a los aeropuertos de su país haciendo analogías con los ataques a Pearl Harbor, pero también mostró su preocupación por los sistemas financieros, de servicios de gobierno, seguridad y sistemas de energía [148]. Existen varias aplicaciones de distintas compañías que muestran monitores de ataques cibernéticos en el mundo tanto para redes móviles como para redes de datos, incluyendo el caso de la denegación de servicio en servidores, actualmente nos encontramos en el rango de millones por día [149-151].

VI.6.7 La criptografía: una historia sin fin

Uno de los organismos más avanzados es el NICT (*National Institute for Information and Communications Technology*) de Japón, el cual ha desarrollado varios sistemas de alerta de ataques cibernéticos: Uno de los más exitosos es el sistema NICT Daedalus, inspirado en la historia griega de Dédalo quien creó el famoso laberinto, quien también pudo escapar de éste. Incluso más recientemente se creó el sistema Darknet Observation System, el cual es la evolución del NICT DAEDALUS, este es un sistema de visualización tridimensional en tiempo real [147]. La figura VI.14 presenta una pantalla demostrativa del sistema, cuyos elementos son: una gran esfera azul que equivale a internet, las pequeñas esferas representan a las redes monitoreadas y los tenues hilos que equivalen a las direcciones IP. El sistema completo vigila más de 190,000 direcciones IP donde se monitorean posibles ataques cibernéticos, indicados a la distancia en rojo.

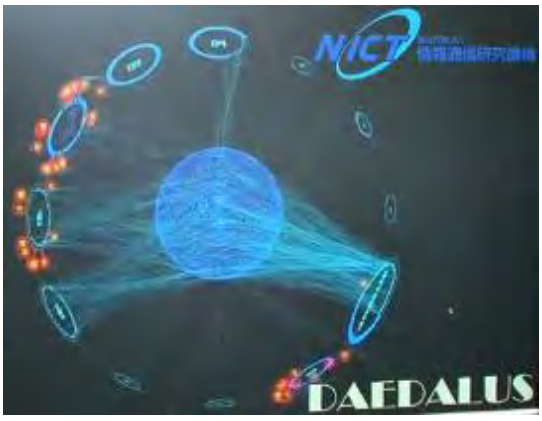


Fig. VI.14. Pantalla demostrativa del sistema Darknet Observation System-Daedalous

Cada red vigilada presenta la forma de un disco, cuya porción azul representa todas las direcciones IP monitoreadas usadas en la red y la porción oscura del disco las direcciones IP disponibles. En cuanto a su operación básica, se puede detectar a un virus cuando inicia su ataque a una red, entonces activa las alertas y muestra la IP fuente, así como los protocolos que se están utilizando. La figura VI.15 muestra a la red "50", la cual presenta varios ataques, mismos que evidentemente se presentan dentro de su área azul donde se tienen las direcciones IP asignadas

Fig. VI.15. Pantalla demostrativa de la red 50 dentro del sistema Darknet Observation System-Daedalous que muestra los ataques en amarillo.

VI.6.8 La seguridad física y la seguridad cibernética en el siglo XXI

Prácticamente el mundo cambio desde el 11 de septiembre de 2001, después de la caída de las torres gemelas en Nueva York, cualesquiera que haya sido el origen y motivo de tal suceso, fue la primera vez que al cambiar la seguridad en el mundo físico también afectó la seguridad en el mundo virtual, específicamente en la seguridad cibernética y el espacio cibernético. Como consecuencia del evento citado, la National Security Agency (NSA) se convirtió en una institución sumamente poderosa con un enorme presupuesto, para globalizar el espionaje que EEUU realizaba hacia todos los países extranjeros, generalizándolo incluso a sus propios ciudadanos. Desde entonces los ciudadanos de EEUU, así como en otros países han visto reducir sus libertades y privacidad en nombre de la seguridad, ha sido todo un cambio por diseño, así como en alguna época se implantó la obsolescencia programada para los productos en la economía de mercado. Fue desde 2001 que inició el diseño de las armas cibernéticas ya citadas y las conocidas consecuencias. La NSA creció tanto, implementado sistemas de vigilancia en masa que después de la crisis económica en EEUU coincidió con la revelación de evidencias y filtraciones por parte de miembros de CIA, FBI, NSA y

DoD, algunos casos fueron tan sonados que tuvieron eco mundial. En 2013 Edward Snowden fue uno de los que más evidencias aportó respecto de los programas de vigilancia y espionaje de la NSA, que se ha popularizado el término, "la era post Snowden". Sin duda la primera década del siglo XXI pasara a la historia como una evidencia más de que los imperios, incluso los dominantes caen desde adentro, como sucedió en occidente con Roma, España, Reino Unido en el pasado. Nos espera pues un interesante siglo XXI en términos de seguridad cibernética, en la que cualquier país que así se lo proponga, puede convertirse en una verdadera potencia.

VI.6.9 La iniciativa *IEEE Cyber Security*

Desde 2012 IEEE lanzó la iniciativa IEEE Cyber Security, misma con la cual se creó el IEEE Center for Secure Design (CSD), el cual busca cambiar el enfoque tradicional de encontrar "bugs", para cambian a un enfoque en el que se identifiquen fallas de diseño con la finalidad de que los arquitectos de software puedan aprender de los errores de otros. Para mayor información consultar la página principal.

http://cybersecurity.ieee.org

VI.6.9 Ataques vías cortinas de humo usando ingeniería social.

Por último cabe mencionar sobre la información, un hecho que acompaña al hombre desde siempre, la manipulación de la información, la mentira en el contenido de la misma para distintos fines, de allí el problema de la veracidad de la información que se alimenta a los sistemas que llegarían a bases de datos y a los "DataWare Houses" para poder proveer información tratada que permita la toma de decisiones. La manipulación de la información se da básicamente en la historia y la historia la escriben los vencedores, dando su versión de los hechos y parece que ningún pueblo en el planeta es inmune la manipulación de la información. La manipulación de la información es y ha sido un elemento importante en las guerras, es toda una estrategia para engañar al adversario o enemigo, cualquiera que este sea. La tergiversación de la información se dio en las guerras napoleónicas, entre Inglaterra y Francia, durante la primera guerra mundial para hacer que EEUU ingresara a la guerra vía la campaña del "miedo rojo", y qué decir de la segunda guerra mundial con la propaganda de la Alemania Nazi en Francia con lo que los doblegaron fácilmente. El engaño también permitió el arribo de las tropas de EEUU a Normandía en Francia, engañando esta vez al ejército Nazi. La propaganda falaz mediante slogans vacios, se usó en las guerras de Vietnam, Corea, Afganistán, Irak, Ucrania y todas las revueltas sociales y revoluciones. También es bien conocido el caso de la transmisión radiofónica de la adaptación de la guerra de los mundos en 1938 en EEUU lo que dejó patente la manera tan sencilla de "manipular al ciudadano promedio" llevándolo a la histeria colectiva, al grado de influir en una gran cantidad de programas de radio, televisión, libros sobre ovnis que se mantiene en nuestros días. Por su parte los estereotipos son alimentados por los medios, otro ejemplo típico de desinformación es la percepción que se tiene en EEUU acerca de que el día de la independencia de México es el 5 de mayo, por la Batalla de Puebla de 1862 contra la intervención francesa, cuyo origen también tuvo motivos políticos y así podríamos citar cientos, quizá miles de ejemplos de falacias y afirmaciones sin evidencias.

Todos los mitos alrededor de intereses políticos, religiosos, económicos y de control social, las llamadas leyendas urbanas, los distractores como las olimpiadas y los mundiales; las obras de Noam Chomsky sobre "el control de los medios de comunicación" da muchos ejemplos de casos y excelentes reflexiones para quienes deseen iniciarse en el tema. Chomsky también deja claro que no solo los ciudadanos promedio son manipulables también las élites intelectuales, el objetivo es

llevar a determinadas sociedades a la apatía, la obediencia y la pasividad es la forma de controlarles.

Casi todo tipo de información se encuentra en internet, la información es enorme, es válido decir que en los últimos 50 años se ha producido más información que en toda la historia de la humanidad, pero también es válido para los últimos 10 años o el último año. Desde que se liberó la internet comercial a más de 20 años, se ha integrado a esta una gran cantidad de información, mucha gente accede a ella a diario, y mucha toma decisiones con base en la información que encuentra en internet, la macrohistoria y la microhistoria se encuentra plagada de esas alteraciones a la realidad que toman formas distintas algunas son directamente dogmáticas otras son pseudocientíficas y algunos son conceptos erróneos; por el lado del conocimiento científico muchas verdades hoy aceptadas luego serán corregidas. En fin, internet es como un iceberg, difícil es saber cuanta información es falaz, el ciudadano promedio no verifica ni valida las fuentes de información, si una nota sale publicada de manera oficial, o se indica en radio o en televisión o en revistas, las toma como ciertas. Y cierto que con el crecimiento exponencial de la internet la cantidad de información puesta en internet desde 1995 a 2005 fue tal que se contaba con mucha información puesta a disposición de la gente bajo el concepto de web 1.0 o la web estática en la que el flujo de información fue unidireccional. Sin embargo, ya podríamos decir, que la sociedad que podía acceder a esta tecnología conformaba una sociedad de la información.

En 2002 una de las varias causas que llevaron a la crisis "punto com" fue que los inversionistas se preguntaron, si bien se tenía una sólida web 1.0 con muchísima información: ¿y qué hacemos con todo esto?, entonces se planteó la necesidad de un evolución en la web, la web semántica o web inteligente la cual se conceptualiza en 2001, pero en ese momento se estaba y lejos [152]. En 2005 se hace realidad una evolución que no llegó a web semántica, pero esa web2.0 daría posibilidades las páginas web de hacer bidireccional el flujo de la información, permitiendo al usuario interactuar y en algunos casos colaborar.

Lo que en verdad será interesante y muy útil será cuando llegue esa web semántica, la web inteligente o web 3.0 la cual se encuentra en desarrollo y que permitiría ayudar a separa la información sin verificación y validación entre otras cosas, buscando que la información colocada realmente agregue valor. También en el ciberespacio se han levantado la ciberdemocracia y el ciberfascismo, las posibilidades parecen infinitas y si bien en la ciberdemocracia todo es horizontal, un apersona que piense que "en internet hay toneladas de blogs superficiales e infantiles, como Andrew Keen en su libro "The cult of the amateur", tales declaraciones podrían considerarse fascistas [153]. Aunque en realidad las declaraciones anteriores podrían ser solo una

vista que no cubre los de 360 grados, ya que también podría darse un equilibrio al denunciar abusos de poder, pero también influir como herramienta en grandes manifestaciones sociales que acompañen transformaciones como la primavera árabe. El gran riesgo es que dentro de las ciber culturas, esa de la desinformación, de información basura impacte a las sociedades debilitando a determinadas sociedades desviándolas de lo que podríamos llamar civilizado, entonces internet no quedaría rápidamente tan lejos de los fenómenos que aparecieron en medios como radio y televisión. Una de las causas raíz del problema podría resumirse así:

"La gente demanda *libertad de expresión* como compensación por la *libertad de pensamiento* que rara vez ejerce"

Søren Kierkegaard (1813-1855)
Filosofo Danés, padre del Existencialismo

La solución estará en buscar buenos programas en internet como si existen buenos programas de radio, televisión o cine, el problema como sucede en esos caso es buscarlos y encontrarlos, pero la verdadera solución viene en la educación, y que esta se interiorice. En internet, en ese mundo virtual se encuentra un mundo paralelo al mundo real, y este tema del ciber anarquismo como extremos de la ciber democracia, sin duda también empujó el ciber espionaje incluso al nivel de ciber vigilancia ciudadano por ciudadano, bajo los programas que ya todos conocemos como PRISM de la NSA en EEUU y del resto de los programas similares en países industrializados. Esperemos pues que la web semántica, se haga una realidad, madure y sea alcanzable a la mayoría para gestionar los contenidos para resolver aunque sea parcialmente el problema de la confiabilidad de la información, cuando esta web semántica permita que las máquinas generen conocimiento estaremos en la sociedad del conocimiento, claro está, solo aquellas que tengan esta web a su alcance.

VI.7 Autoevaluación para el capítulo VI

1. Busque información relacionada con virus informáticos
2. Consulte "Honey Map" en **map.honeycloud.net** y describa ampliamente su objetivo y funciona, citando 3 ejemplos de su actividad.
3. ¿Cómo afecta a su institución la adecuada o inadecuada "seguridad cibernética"?.
4. ¿Conoce algún "data center"?
5. ¿Ud. vive en una ciudad inteligente?, explique.
6. ¿Conoce los medidores inteligentes AMI?, ¿ya cuenta con uno de ellos en casa? En su caso que nos puede decir al respecto.

CAPÍTULO VII: CONTEXTO SOCIAL Y SU IMPACTO EN LAS TICS.

Para poder predecir necesitamos contar con la mayor cantidad de información posible, que sea veraz y oportuna, mientras que los riesgos son la propaganda y la publicidad engañosa en todas sus formas. Los países, las instituciones, empresas y la gente en general, proporciona la información con la que cuenta, la cual puede ser cierta o falsa. En distintos grados los habitantes del planeta estamos sumergidos en un gran juego de propaganda, en función del país donde vivamos. Lo que vale la pena preguntarse a diario es, ¿qué tan cierta es la propaganda que reciben los ciudadanos de todo país a cada momento, vía radio televisión o la propia internet?

En uno de los proyectos que trabajé en la década pasada, sobre energía eólica en México con el Programa de Naciones Unidas para el Desarrollo (PNUD), el Instituto de Investigaciones Eléctricas (IIE) y la Benemérita Universidad Autónoma de Puebla (BUAP), sucedió que desde la década de los 80 se promovió el uso de energía eólica pero fue hasta 2005 que se introdujeron los primeros 99 aerogeneradores a gran escala en la Venta, Oaxaca. Hubiese tardado menos la introducción de esta tecnología que se compró a GAMESA, una empresa española, sin embargo, la gente del lugar donde se compraron las tierras para las granjas eólicas se opuso durante varios años, es decir, entre lo que se proyectó y la puesta en marcha pasaron varios años, y eso no fue considerado en el proyecto, el facto social, la aceptación de la sociedad. Con base en este caso práctico, pensemos ahora en términos de las TICS.

Fig. VII.1. Aerogenerador en México, bajo el control de CFE

Para considerar las redes de computadoras partimos de las computadoras y dado que estas surgen comercialmente después de la segunda guerra mundial, partiré de la revisión del estado que guardaba el mundo desde la segunda guerra mundial a nuestros días.

Durante la segunda mitad del siglo XX el capitalismo acumulaba riqueza de modo que la renta de la tierra rivalizaba con la renta tecnológica, mientras que en siglos XXI la renta tecnológica es la que mantiene el nuevo orden mundial. La segunda guerra mundial también terminó con el imperio británico y el surgimiento de dos superpotencias EEUU y Rusia. Quizá las invenciones tecnológicas electrónicas que cambiaron la historia de la segunda guerra mundial fueron el magnetrón para el radar y las computadoras tras una gran alianza entre gran Bretaña y EEUU, mientras que en términos de materias primas el control del petróleo dio la ventaja. En los 6 años de guerra, EEUU duplicó su Producto Interno Bruto (PIB), producía la mitad de los productos manufactureros del mundo, obtuvo el 66 % de las reservas de oro del mundo, poseía más de 30,000 bases miliares en todo el mundo con lo que se convirtió en la primera potencia militar, lo que le permitió acelerar el proceso de globalización a su modo. A continuación se revisa el entorno económico mundial con base en el Producto Interno Bruto (PIB), con base en el cual se realizan parcialmente las inversiones en investigación, desarrollo y TICs.

VII. 1 1945-1980: LA ÉPOCA DORADA

Después de la segunda guerra mundial, por cerca de 35 años el mundo vivió un gran crecimiento, al resto del mundo le llamó la atención "el sueño americano", el cual consistía en que dada una generación, la siguiente duplicaba su poder adquisitivo y nivel de vida. La crisis energética del 74 tardó un poco en extender su efecto, pero permitieron a algunos países a salir del subdesarrollo, mientras China inició una gran revolución cultural. En la década de los 70 Corea del sur e Israel, economías en ese entonces muy inferiores la mexicana, se convirtieron hoy en potencias tecnológica gracias a su inversión en electrónica. México tuvo una época en la que ocupó en la economía mundial número 10 (PIB), gracias a un crecimiento sostenido en un periodo denominado, el milagro mexicano. El crecimiento que tuvo la clase media por 35 años, tuvo su proceso inverso en los siguientes 35 años (1980- 2015). Mientras tanto Japón y Alemania se recuperaron de la guerra, Japón ya había desplazado a la industria automotriz de EEUU, los conceptos de calidad en toda industria dieron un giro que también significaba el inicio de la caída industrial de EEUU en la década de los 80. La tabla VII.1 muestra el PIB de potencias y países en desarrollo en 1980, centrándonos en las 10 primeras [154,155].

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	2,862,475	8	China	309,060
2	Japón	1,086,988	9	Argentina	249,941
3	Alemania	826,142	10	México	234,618
4	Francia	704,483	11	España	224,368
5	Reino Unido	542,452	12	India	181,416
6	Italia	470,040	13	Brasil	148,916
7	Canadá	274,370	14	Corea del Sur	67,802

Tabla VII.1. PIB en 1980 de potencias y países en desarrollo.

Para 1980, el G7, incluía a los 7 países con mayor PIB indicado en la tabla anterior, EEUU, Japón, Alemania, Francia, Reino Unido, Italia y Canadá.

VII. 2 1980-1990: EL DESPEGUE ASIÁTICO

Mientras los países asiáticos se aceleraban con el crecimiento espectacular de Japón y Corea del Sur; los occidentales crecían al doble, mientras que en América Latina, Brasil subía, México se desaceleró y Argentina salió del mapa estrepitosamente, como se indica en la tabla VII.2.

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	5,979,575	8	España	520,415
2	Japón	3,103,699	9	Brasil	465,006
3	Alemania	1,547,026	10	China	404,495
4	Francia	1,278,570	11	India	326,608
5	Italia	1,140,235	12	Australia	323,444
6	Reino Unido	1,024,550	13	México	298,037
7	Canadá	594,612	14	Corea del Sur	284,755

Tabla VII.2 PIB de potencias y países en desarrollo en 1990.

La disponibilidad monetaria determina los grados de inversión en tecnología de comunicaciones.

VII. 3 1990-2000: FIN DEL SIGLO XX

Desde aproximadamente 1980 a 2000, lo sectores primarios, secundarios y terciarios tuvieron severos cambios, en esas décadas la materias primas se abarataron. USA casi duplicó, Canadá creció, Japón, y el resto de las potencias occidentales se desaceleró fuertemente, el más desacelerado fue España, se cambiaron nuevamente Italia y reino Unido. China subió espectacularmente, casi 3 veces y se posicionó dentro de las 10 economías. El resumen se muestra en la tabla VII.3. En este contexto económico se libera la "internet comercial".

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	10,254,758	8	Canadá	739,451
2	Japón	4,731,199	9	México	683,650
3	Alemania	1,891,934	10	Brasil	644,734
4	Francia	1,372,452	11	España	582,098
5	Reino Unido	1,496,606	12	Corea del Sur	561,634
6	China	1,192,854	13	India	476,636
7	Italia	1,107,248	14	Rusia	259,702

Tabla VII.3. PIB de potencias y países en desarrollo en 2000.

En 1998 el G-7 se expande al G-8, con la admisión de Rusia, sin embargo, en 2014 Rusia quedó excluida la anexarse territorios de Ucrania. En 2000 China desplazó a Canadá de las 7 primeras economías y el G7 tuvo que cambiar más su connotación más política pro-occidente que puramente económica.

VII. 4 2000-2010: PRIMERA DÉCADA DEL SIGLO XXI

El caso de China fue particular, creciendo durante la primera década a más de 10% lo que lo llevó en 2010 a ser la segunda economía más grande del mundo.

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	14,964,400	8	Italia	2,059,188
2	China	5,949,648	9	India	1,708,541
3	Japón	5,495,387	10	Canadá	1,614,072
4	Alemania	3,310,600	11	Rusia	1,524,915
5	Francia	2,651,772	12	España	1,387,427
6	Reino Unido	2,296,930	13	Corea del Sur	1,094,496
7	Brasil	2,142,905	14	México	1,051,128

Tabla VII.4. PIB de potencias y países en desarrollo en 2010.

Sin duda la primera década del siglo fue la década BRIC (Brasil, Rusia, India, China) y asiática. China se colocó como el rey absoluto, creció casi 6 veces, anualmente creció a dos dígitos y en 2010 desplazo a Japón, quien ocupó la segunda posición durante 30 años. Rusia 5 veces, Corea del sur 3 veces, India 4 veces, Brasil más de 3 veces. Y mientras que Alemania de fortaleció; por otro lado se desaceleraron EEUU y Japón. En 2010 Brasil desplazó a Italia de las 7 primeras economías y el G7 tuvo en realidad tenia a solo 5 en los 7 primeros lugares consolidando más su connotación política pro-occidente que puramente económica. Es en este contexto que al principio de la década se globalizó el término TICs. En esta década los EEUU recibieron la dura lección de haber terciarizado hacia China principalmente gran parte de su industria manufacturera. Pese a las grandes crisis, como la de 2008, las élites nunca lo resienten. En 2011 cuando salió el reporte de que China se había colocado como la segunda potencia económica mundial y también tercera potencia militar, recordé que en la década de los 70, cuando mi abuelo había regresado de una gira por Asia, me comento: "no cabe duda, … en el futuro China pondrá en grandes aprietos a los EEUU, no lo dudes" y como dice la frase "qué razón tenía el abuelo".

VII. 5 LA PRIMERA GRAN CRISIS GLOBAL DEL SIGLO XXI

La segunda mayor crisis global de 2008, nació en 2007 en EEUU, estos como una consecuencia de las crisis económicas recurrentes de los 70, 80, 90 y 00, que llevaron al punto máximo de crisis en 2008 cuando queda completamente develado el fin del "sueño americano" en los Estados Unidos llamado así desde la visión eurocentrista. En 2007 más de 57 millones de estadounidense, (de una población de cerca de 300 millones) no contaban con seguro médico, mientras que para el colapso de 2008, más de 25 millones quedaron sin empleo [156, 157]. En realidad la caída ya venía, en 1995 se hablaba de la necesidad de un cambo en la economía y la realidad del capitalismo salvaje, nació el concepto de ciudades inteligentes y los eventos de 2001 en EEUU fueron la gota que derramo el vaso. Y si se consulta el historial de PIB per capita de EEUU, de 1920 inicio una gran época para EEUU y hasta 1a década de los 70, vivió una época dorada, pero desde esa década hasta 2013, se ha alcanzado casi el mismo nivel que en los 20. En realidad la prosperidad que obtuvo la clase media entre 1945 a 1975 se vio revertida en los 80, 90 y 2000. Claro está que las fechas indicadas aplican para EEUU, México sufrió los efectos buenos (50-80) con algún retardo y los malos casi inmediatamente (1990-2010). EEUU paso de ser un gran imperio de producción a un gran imperio de consumo y México siguió el mismo patrón pero de un peor modo. EEUU bajo mucho en su nivel educativo equivalente a primaria y secundaria como lo indica su posición de media tabla de acuerdo con la prueba PISA, pero lo mismo sucedió con su productividad y competitividad. Lo que le sucedió a EEUU lo podría resumir con una impresionante anécdota personal, la cual describiré brevemente a continuación: En 1981 en Cancún, QRoo. México, mi padre me dijo "en Cancún quien sabe inglés gana un dólar más", el tiempo pasó y en 2011, 30 años después, en Los Ángeles, California, EEUU, un joven taxista que me llevó al aeropuerto me dijo:

"señor, aun cuando no soy mexicano, yo hablo español ya que aquí en Los Ángeles, quien habla español gana un dólar más"; el "shock" fue impresionante, es claro que muchas cosas en el mundo pueden cambiar en 30 años.

VII. 6 2010-2015

Desde 2014 en varias universidades de EEUU hay colegas profesores que deben dar más horas que las que eran habituales (12 hrs por semana) debido que la educación universitaria es muy cara y EEUU está enfrentando serios problemas con sus matrículas, así como Europa lo enfrento alrededor de 2010, cuando con base en planes estratégicos fueron fusionando universidades, facultades y escuelas, donde el modelo del Reino Unido fue uno de los más exitosos en términos de recortes y fusiones relativamente paulatinas que implicaron la reinstalación geográfica de facultades y estudiantes. En medio de la crisis España llegó al 57% de desempleo en 2014, en general en Europa se habla de toda una generación perdida y habrá que ver si esto va más allá de Europa. Como respuesta el foro económico mundial promueve el empredurismo en Europa para jóvenes menores a los 30 años. A continuación se muestra el PIB de 2014 en la tabla VII.5.

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	17,416,253	8	Italia	2,129,276
2	China	10,355,350	9	Rusia	2,057,301
3	Japón	4,769,804	10	India	2,047,811
4	Alemania	3,820,464	11	Canadá	1,793,797
5	Francia	2,902,330	12	Corea del Sur	1,449,494
6	Reino Unido	2,897,604	13	España	1,400,483
7	Brasil	2,244,131	14	México	1,295,860

Tabla VII.5. PIB de potencias y países en desarrollo en 2014.

De 2010 a 2014 Brasil se estancó, Rusia e India se desaceleraron, China solo duplicó y Corea creció bien. Japón fue el único país que retrocedió de los primeros 14, sin duda las secuelas de Fukushima tuvieron una fuerte influencia.

# PIB	País	MDD	#PIB	País	MDD
1	EEUU	18,124,731	8	Brasil	1,903,934
2	China	11,211,928	9	Italia	1,842,835
3	Japón	4,210,363	10	Canadá	1,615,471
4	Alemania	3,413,483	11	Corea del Sur	1,435,076
5	Reino Unido	2,853,357	12	Australia	1,252,273
6	Francia	2,469,530	13	México	1,231,982
7	India	2,308,018	14	España	1,230,207

Tabla VII.6. PIB de potencias y países en desarrollo en 2015.

Reino unido y Francia intercambiaron lugares, las notas buenas las dan EEUU, China, India y Australia, mientras que el resto perdieron terreno y quizá la caída más dolorosa haya sido la de Brasil. Sin duda la desarticulación política global se va acentuando y el planeta se pone más tenso al final de 2015 y los tambores de guerras suenan más fuerte, mayor claridad se da con la revisión de números en rojo de 2015 o el gráfico VII.2 que indica la evolución del PIB de 1980 a 2014, con base en herramientas que otorga el Fondo Monetario Internacional. Cabe destacar en el gráfico a EEUU China y Japón.

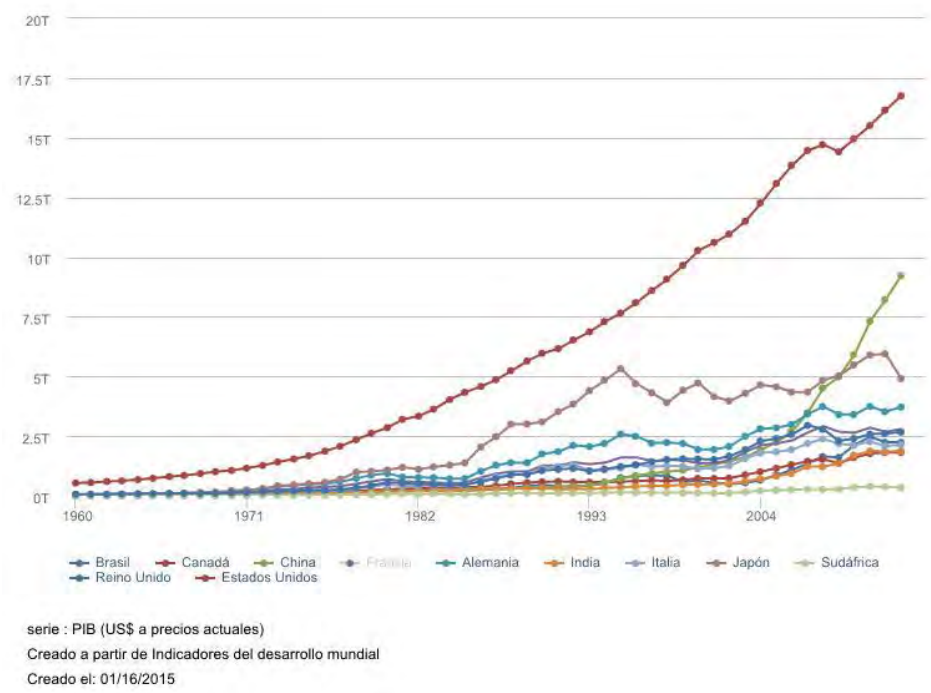


Figura VII.2. PIB de potencias y países en desarrollo de 1980 a 2014.

Revisando todos los datos duros presentados anteriormente, queda claro el qué, sin embargo, nada nos dice respecto del cómo, ¿Cómo logra cada país tales resultados económicos y cuál es el costo?

La cumbre del G20 fue crucial en 2009 al enfrentar una crisis que pegó a todos menos a China. Y por si hubiera gente que no lo tuviese claro, en la pasada reunión del G20 en 2014, se llegaron a cerca de 800 acuerdos en sólo una semana, en uno de ellos, se considerar a las infraestructuras críticas como globales, ya no solamente como nacionales, por aquello del efecto mariposa y el efecto dominó. Y basta decir, que para cerrar la pinza, el ejército de EEUU ha iniciado un plan para poder intervenir en las 20 mega ciudades del mundo (ciudades con más de 10 millones de habitantes), para evitar cualesquier inestabilidad, ya que la caía de una de esas ciudades podría colapsar la economía global. Las únicas 3 ciudades latinoamericanas incluidas entre las más grandes

urbes mundiales con las características mencionadas son: San Pablo y Rio de Janerio en Brasil y la Ciudad de México en México.

Respecto de México la figura VII.3 muestra la evolución del PIB en México de 1980 a 2014, en la que se muestran los 6 años deficitarios o de profunda crisis, 3 en la década de los 80 una en los 90 y otra en los 2000.

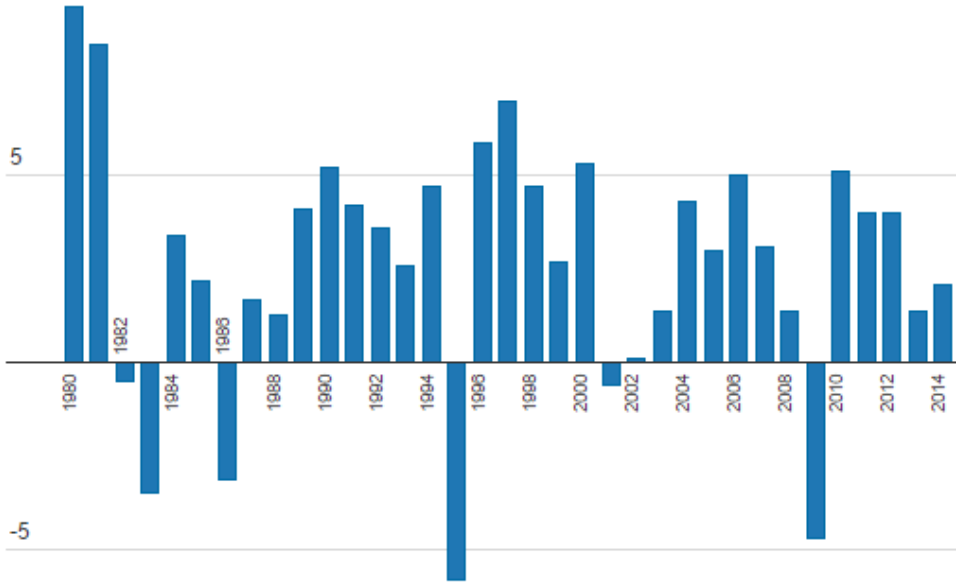


Figura VII.3. Evolución del PIB de México de 1980 a 2014.

Pese a que México se ha encontrado de 1980 a 2015 dentro de las 14 economías mundiales, el "PIB per cápita" de México es inferior al PIB per cápita de Trinidad y Tobago y de Puerto Rico, además de que la deuda externa acumulada es de casi un tercio del PIB. Además el desempleo, pero sobretodo el subempleo tienen un amplio impacto y por si fuera poco la balanza de pagos es fuertemente deficitaria.

Una vez que llegamos al final de esta obra espero que le lector haya encontrado lo que buscaba, no sin antes recordarle que aunque el conocimiento científico y tecnológico es valioso e importante, no debe olvidarse que una buena parte del conocimiento es arte, el cual sólo se gana a través de la experiencia. Ninguna tecnología nos dará por si sólo las respuestas de manera mágica. Y muy importante es preguntarse, sin importar en qué país del mundo vivas o te encuentres, si la información que un ciudadanos recibe a diario vía radio, tv o internet proviene de una fuente confiable y si aun así lo fuese, ¿es cierta o falsa?, ¿a qué intereses corresponde?, ¿se ha sacado de contexto? En un mundo donde todos juegan el juego de la propaganda, bienvenidos a un "mundo feliz".

VII.7 Autoevaluación para el capítulo VII

1. ¿Puede la calidad ser afectada sólo por la propaganda?
2. ¿Es posible que los fraudes como los de VW en la industria automotriz en 2015, en términos de contaminación ambiental se den en la industria de telecomunicaciones?
3. De conocer casos anómalos en la industria de telecomunicaciones lístelos y explique.
4. ¿El viaje del hombre a la Luna fue solo propaganda? Discuta si el hombre llegó a la Luna en 1969, en caso afirmativo o negativo proporcione argumentos.
5. Discuta sobre la obsolescencia programada en la industria de los teléfonos móviles

REFERENCIAS

Capítulo I

1. *IEEE Spectrum*, "*Patents Data"*, pp. 68, July 2011
2. "Benjamin Franklin, Book: Experiments and observations on electricity, 1751", *IEEE Milestones*, IEEE History Center, IEEE, 2009.
3. "Alessandro Volta´s Electrical battery invention, 1799", *IEEE Milestones*, IEEE History Center, IEEE, 2003.
4. "James Maxwell´s Equations, 1860-1871", *IEEE Milestones*, IEEE History Center, IEEE, 2009.
5. "Samuel Morse and Alfred Vail, Demonstration of practical telegraphy, 1833", *IEEE Milestones*, IEEE History Center, IEEE, 1988.
6. José Ignacio Castillo Velázquez*, "Curso Arquitectura de computadoras", EATI-Blackboard, Ingeniería en Computación, Departamento de TI, UPAEP, 1999-2005.*
7. INEGI (Instituto Nacional de Estadística y Geografía), México, 2014. [Disponible en: www.inegi.org.mx]
8. "Alexander Graham Bell,, First intelligible voice transmission over electric wire, 1876", IEEE Milestones, IEEE History Center, IEEE, 2006.
9. IEEE, Alexandre Graham Bell, "AIEE Edison Medal" por sus contribuciones a la telefonía, 1914, [Disponible en: http://www.ieee.org/about/awards/medals/medalofhonor.html]
10. "Thomas Alva Edison Historic Site At Menlo Park, 1876", IEEE Milestones, IEEE History Center, IEEE, 2006.
11. "Thomas Alva Edison, Pearl Street Generation Station, USA, 1882", IEEE Milestones, IEEE History Center, IEEE, 2011.
12. IEEE Communications Society, A brief history of communications, 2002. ISBN: 0-7803-9825-4.
13. Telecommunications Virtual Museum, *How phones work: the basic Science behind telephony.* [Disponible] http://www.telcomhistory.org/vm/sciencePhonesWork.shtml
14. "John Fleming, Fleming Valve, 1904", IEEE Milestones, IEEE History Center, IEEE, 2004.
15. IEEE, Lee, "AIEE Edison Medal" tríodo 1906, 1946, [Disponible]: http://www.ieee.org/about/awards/medals/medalofhonor.html.
16. Historia del teléfono; video, 2015, http://www.youtube.com/watch?v=gV9Ea2ylE3o#t=46
17. Bell Telephone System, The making of a telephone (433 parts), video, 2015 http://www.youtube.com/watch?v=MXS_14Jam1Q&list=PL1554957EA7223AE2
18. AT&T Now you can dial (1954): [7 numbers, 2 for central office name, 5 for telephone], video, 2015 http://www.youtube.com/watch?v=KSTOT7RBkNc&list=PL1554957EA7223AE2
19. AT&T, Mr Digit and the battle of bubbling brook, video, 2015 http://www.youtube.com/watch?v=EdW4FFMZrfU&list=PL1554957EA7223AE2
20. AT&T, "A story without End 1950", video, 2015 http://www.youtube.com/watch?v=QT7hLBpGxJs
21. AT&T, Operator 1969, 2011 http://www.youtube.com/watch?v=bAC4MvP_C-I
22. AT&T, The step by step switch (1951), video 2015, http://www.youtube.com/watch?v=xZePwin92cI&list=PL1554957EA7223AE2
23. *Herbert H. Warrick Jr Museum of Communications*, Seattle, Washington, EEUU. Mayor información en http://museumofcommunications.org, 2014.
24. AT&T, Good Bye Central, 1974, video 2015 http://www.youtube.com/watch?v=7qLU_urEYVE&list=PL1554957EA7223AE2
25. ITU-T, Q.700, 1998 [Disponible en] http://www.itu.int/rec/T-REC-Q.700-198811-S/en

26. Joel Álvarez de la Borda, *Crónica del petróleo en México, de 1863 a nuestros días*, Archivo Histórico de Petróleos Mexicanos, Pemex, 2006.
27. Telecommunications statistics for México, World Bank, 2015, http://databank.bancomundial.org/data/views/reports/chart.aspx?isshared=true

Capítulo II

28. Raul Rojas, *Konrad Zuse´s Legacy,* IEEE Annals of the History of Computing, Vol. 19, No. 2, pp 5-16, 1997.
29. John Alderman, Core Memory: 35 iconic machines, Computer History Museum, USA, pp 10-15, 2007. ISBN: 0-8118-5442-6.
30. "Sillicon Valley, Manufacture of Transistors, 1951", IEEE Milestones, IEEE History Center, IEEE, 1998.
31. Transistor, IEEE Global History Networks, IEEE History Center, IEEE, 2015 [Disponible] http://www.ieeeghn.org/wiki/index.php/The_Transistor_and_Portable_Electronics
32. Ferranti, An Introduction to the Ferranti Mecury Computer, England, 1956
33. Rand, An Introduction to the UNIVAC File Computer, USA, 1951
34. IBM 709, 2014. [Disponible en] http://www.columbia.edu/cu/computinghistory/ibm709.html
35. David A. Patterson and John Hennessy, *Computer Organization & Design: the hardware and software interface, 2nd Ed. Morgan Kaufmann, Chapter 1*, 1998. ISBN: 1-55860-428-6
36. Rand, Universal Automatic Computer Model II UNIVAC II, 1958
37. Jorge Aguirre y Raúl Camota, Historia de la informática en Latinoamérica y el Caribe: investigaciones y testimonios, Universidad nacional de rio Cuarto, Argentina, 2009, ISBN: 978-950-665-573-0 [Disponible en] http://www.slideshare.net/msavio/historia-da-informtica-na-amrica-latina
38. IBM, IBM 650, Fact Sheet, 1953, 2015 [Disponible en] http://www-03.ibm.com/ibm/history/exhibits/650/650_ch1.html
39. "First Semiconductor integrated Circuit (IC), 1958", IEEE Milestones, IEEE History Center, IEEE, 2009.
40. "Semiconductor Planar Process and Integrated Circuit, 1959", IEEE Milestones, IEEE History Center, IEEE, 2009
41. "Apollo Guidance Computer, 1962-1972", IEEE Milestones, IEEE History Center, IEEE, 2002
42. Electrológica, Electrológica X1 1958, Holanda 2015. [Disponible en] http://www.electrologica.nl/historie/electrologica.html
43. Stantec, Zebra, Electronic Digital Computer, Brief specification, EEUU, 1958
44. RCA, All new transistors, RCA 501, EEUU, 1958
45. DEC, Digital Equipment corporation, Nineteen Fifty seven to the present, EEUU, 1978. [Disponible] http://www.faqs.org/faqs/dec-faq/pdp8/
46. Computer Museum, Bendix G15, 2014 [Disponible en] http://www.computermuseum.li/Testpage/Bendix-G15-1950s.htm
47. IBM, IBM 360 model 40. [Disponible en] http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP2040.html
48. "Pioneering work on the quartz electronic wristwatch, 1962-1967", IEEE Milestones, IEEE History Center, IEEE, 2011
49. "Pioneering work on electronic calculators, 1964-1973", IEEE Milestones, IEEE History Center, IEEE, 2005
50. Computer History Museum, *Selling the computer revolution, 2015, [Disponible en]* http://www.computerhistory.org/brochures/decades.php?decade=thm-42b982c022233
51. IBM, IBM 360 Series, 2015 [Disponible en] http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_FS360.html
52. Xerox, Sigma 7 Computer Reference Manual, USA, 1973

53. DEC, Digital Equipment corporation, PDP-10, 1970, EEUU, 2014. [Disponible] http://bitsavers.informatik.uni-stuttgart.de/pdf/dec/pdp10/1970_PDP-10_Ref/
54. Fujitsu, FACOM, 2014, [Disponible en] http://museum.ipsj.or.jp/en/computer/personal/index.html
55. Gerardo Cisneros, La computación en México y la influencia de HV McIntosh en su desarrollo, 1991, 2015 [Disponible en] http://delta.cs.cinvestav.mx/~mcintosh/comun/gto91/gto91.pdf
56. IBM, IBM en Brasil, 2014 [Disponible en] http://www-03.ibm.com/ibm/history/exhibits/brazil/brazil_ch2.html
57. A. Licona et al, La computación en el Instituto de Ciencias de la UAP, 1985, 2015 [Disponible en] http://delta.cs.cinvestav.mx/~mcintosh/comun/historiaw/historia.pdf
58. EPROM, 2014, [Disponible en] http://www.computerhistory.org/semiconductor/timeline/1971-EPROM.html
59. David A. Patterson, *Reduced Instruction Set Computers,* Communications of ACM, V28, No 1, pp 8-21, 1985.
60. Andrew Tanenbaum, Organización de computadoras: un enfoque estructurado, 4ta Ed. Pearson, Capítulos 1 y 2, 2000. ISBN: 970-17-0399-5.
61. *Computer World, BENCHMARK, 2014, http://www.cpu-world.com/CPUs/CPU.html*
62. Weizenbaum, Last resume, [Disponible en] http://eecs-newsletter.mit.edu/articles/2008-fall/joseph-weizenbaum-1923-2008

Capítulo III

63. IEEE Communications Society, A brief history of communications, 2002. ISBN:0-7803-9825-4
64. UCLA, “Birthplace of the Internet, 1969”, IEEE Milestones, IEEE History Center, IEEE, 2009
65. SRI, “Inception of the ARPANET, 1969”, IEEE Milestones, IEEE History Center, IEEE, 2009
66. DARPA, RFC 15, Network Subsystem for Time Sharing Host, Sep. 1969
67. DARPA, RFC 354, *File Transfer Protocol*, 1972.
68. Cerf, V., and R. Kahn, "A Protocol for Packet Network Intercommunication," IEEE Transactions on Communications, Vol. COM-22, No. 5, pp 637-648, May 1974.
69. DARPA, RFC 739, *Assigned Numbers*, 1977.
70. *ISO/TC97/SC16 "Provisional model of open systems architecture", Doc N34, March 1978.*
71. *ISO/TC97/SC16, "Reference model of open systems interconnection," Doc N227, June 1979.*
72. DARPA, RFC 755, *ARPANET Protocol Handbook*, 1979.
73. DARPA, RFC 760, *DoD Standard Internet Protocol*, Jan. 1980.
74. DARPA, RFC 761, *Transmission Control Protocol*, Jan. 1980
75. DARPA, RFC 765, *A File Transfer Protocol,* 1980.
76. DARPA, RFC 762, *Assigned Numbers*, Jan. 1980
77. DARPA, RFC 770, *Assigned Numbers*, Sep. 1980
78. DEC-INTEL-XEROX, *The Ethernet, a Local Area Network Data Link Layer and Physical Layer Specifications Version 1.0*, USA, Sep. 1980. Available [http://ethernethistory.typepad.com/papers/EthernetSpec.pdf]
79. DARPA, RFC 776, *Assigned Numbers*, Jan. 1981
80. DARPA, RFC 777, *Internet Control Message Protocol*, Apr. 1981
81. DARPA, RFC 793, *Transmission Control Protocol: DARPA Internet Program Protocol Specification*, Sep. 1981
82. DEC-INTEL-XEROX, *The Ethernet, a Local Area Network Data Link Layer and Physical Layer Specifications Version 2.0*, USA, Nov. 1982. Available: [http://decnet.ipv7.net/docs/dundas/aa-k759b-tk.pdf]
83. Shoch J.F. Dalal Y.K., Redel D. D., Crane R.C., *Evolution of the Ethernet Local Computer Network*, IEEE Computer Aug. 1982, pp.10-26. Available [http://ethernethistory.typepad.com/papers/EthernetEvolution.pdf]

84. DARPA, RFC 826, *An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware,* Nov. 1982. Available: [http://tools.ietf.org/pdf/rfc826.pdf]

85. IEEE Std 802.3, IEEE standards for LAN & WAN: Overview and architecture, 2002.

86. DARPA, RFC 854, Telnet Protocol Specification, Feb. 1983.

87. *ISO 7498:1984 Open Systems Interconnection – Basic Reference Model: The basic Model, 1984.*

88. *José Ignacio Castillo Velázquez, Redes de datos: Contexto y evolución, Samsara, México, 2014.*

89. *ISO 7498-2:1989 Information Processing Systems – Open Systems Interconnection – Basic Reference Model- Part 2: Security Architecture, 1989. Available: [http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=14256*

90. National Science Foundation, Internet Projects, 2015, Available [http://www.nsf.gov/about/history/nsf0050/internet/launch.htm]

91. DARPA, RFC 1436, *The Internet Gopher Protocol a distributed document search and retrieval protocol*, *March*, 1993.

92. DARPA, RFC 2616, *Hypertext Transfer protocol- HTTP/1.1*, Jun., 1999.

93. *ISO/IEC 7498-1:1994 Information Technology – Open Systems Interconnection – Basic Reference Model: The basic Model, 1994. Available: [*http://www.iso.org/iso/catalogue_detail.htm?csnumber=20269*]*

94. DARPA, RFC 1716, *ATowards requirements for IP routers,* 1994. Available: [http://tools.ietf.org/pdf/rfc1716.pdf]

Capítulo IV (70-94)

95. *ISO/IEC 7498-3:1997 Information Technology – Open Systems Interconnection – Basic Reference Model: Naming and Addressing, 1997. Available: [*http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=25022*]*

96. IEEE Milestones, IEEE History Center, IEEE, 2015.

97. *USB Implementers Forum, 2015. Available: [www.usb.org]*

98. DARPA, RFC 791, *IPv4*, 1981.

Capítulo V

99. IEEE Std 729, IEEE standards for software, 1993.

100. Andrew Tanenbaum, *Sistemas operativos: diseño e implementación*, 1ra Ed. Pearson, cap. 1, 1988, ISBN: 968-880-153-4.

101. Andrew Tanenbaum, *Sistemas operativos distribuidos*, 4ta Ed. Pearson, 1996, ISBN: 968-880-627-7.

102. Andrew Tanenbaum, *Sistemas operativos modernos*, 1ra Ed. Pearson, 1993, ISBN: 968-880-323-5.

103. Amir Afzal, *Introducción a UNIX: un enfoque práctico*, 1ra Ed. Prentice Hall, cap. 2 y cap. 5, 1997, ISBN:84-8322-001-6.

104. Paul Kimel, *Manual de UML*, Ed. MC Graw Hill, 2007, ISBN:970-10-5899-2.

105. Apache Configuration, [Available at: http://httpd.apache.org/docs/2.0/es/howto/cgi.html#configuring , Jun., 2015]

106. Apache cookbook [Available at: http://cgi-spec.golux.com/, Jun. 2015]

Capítulo VI

107. Castillo-Velázquez J. I. and Ismael Daza, 3er Congreso Nal. de Ciencias de la Computación, "The IEEE Std. 1625 Portable Computing; Assesing Environmental Impact", Puebla Mexico, Nov. 2005.

108. G. Goth, Brave NUI World, ACM Communications, Vol. 54. No. 12, 2011

109. IEEE Cloud computing initiative, [última consulta en diciembre de 2015 http://cloudcomputing.ieee.org/].

110. Francisco et al, *The final frontier: Confidentiality and privacy in the cloud*, IEEE Computer, September 2011, pp 44-50

111. SAP-Internet of things [http://global.sap.com/campaigns/digitalhub-internet-of-things/index.html#section_0]

112. IEEE IoT initiative, [última consulta en diciembre de 2015 http://iot.ieee.org/].

113. Colocation datacenter MAP, www.datacentermap.com [última consulta en diciembre de 2015 http://iot.ieee.org/].

114. ICREA, Norma Internacional para la construcción de centros de procesamiento de datos, ICREA STD-131-2013.

115. Bruno Astuto, A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, *A survey of Software-Defined Networking: past, present and Future of Programmable Networks*, IEEE Communications Surveys and tutorials, Vol. 16, no. 3 July 2014, pp 1618-1633.

116. Open Networking Foundation https://www.opennetworking.org

117. Open Networking Research Center https://www.onrc.net

118. Sakir Sezer, Sandra Scott-Hayward, Pushpinder Kaur Chouhan, Barbara Fraser, David Lake, JimFinnegan Niel Vilijoen, Marc Miller and Navneet Rao. *Are we ready for SDN? Implementation Challenges for Software Defined Networks*, IEEE Communications magazine, vol. 51, no. 7 July 2013, pp 118-138.

119. José Ignacio Castillo Velázquez, Estado de Smart Grid 2010-2014, notas de curso, 2014

120. John D ambrosia, *Defining the Next Generation of Ethernet*, IEEE Communications, Vol. 45, No 11, Nov. 2007, p 38.

121. J. I. Castillo-Velázquez, *Consideraciones para dirigir industrias energéticas hacia las TICS verdes, JIT 2011*, Hidalgo, Mex. Nov. 2011.

122. J. I. Castillo-Velázquez, *Cyber security as a strategic-tactical critical infrastructure of Mexico*, PCIC-Mexico 2013, DF., México, July. 2013.

123. IEEE Smart Grid initiative, [última consulta en diciembre de 2015 http://smartgrid.ieee.org/].

124. Antonello Monti and Ferdinanda Ponci, "The complexity of smartgrid", IEEE Smart Grid Newsletter Compendium, pp, 68, 2015.

125. Ebrahim Vaahedi, Hossein Pakravan, Angelique Rajski and Massoud Amini, "Smart Grid: the next decade", IEEE Smart Grid Newsletter Compendium 2015, pp, 4-5, 2015.

126. City Sciences, 2014, http://www.citysciences.com], última consulta en diciembre de 2015.

127. Venus Project 1995 - 2013http://www.thevenusproject.com/technology/city-systems], última consulta en diciembre de 2015.

128. European smart cities, 2013, [Disponible en http://www.smart-cities.eu/], última consulta en Julio de 2014.

129. Masdar City, 2013, http://www.masdarcity.ae/en/

130. Cisco, Cities of the future: Songdo, South Corea, [Disponible en http://newsroom.cisco.com/songdo], última consulta en Julio de 2014.

131. Cisco, Cities [Disponible en *http://thenetwork.cisco.com/],* última consulta en Julio de 2015.

132. IBM Smart planet 2013, [Disponible en http://www.ibm.com/smarterplanet/uk/en/smarter_cities/examples/index.html], última consulta en Julio de 2015.

133. R. Y. Clarke, *Smart Cities and the internet of everything: the foundation for delivering next-generation citizen services*, IDC, 2013, [Disponible en

http://www.cisco.com/web/strategy/docs/scc/ioe_citizen_svcs_white_paper_idc_2013.pdf], última consulta en Julio de 2015.

134. IEEE Smart Cities Initiative [Disponible en http://www.smartcities.ieee.org], última consulta en Julio de 2015.

135. A. Marshal, *Big data big questions*, Mag. Metropoli, Feb. 2014, [Disponible en http://www.songdo.com/Uploads/FileManager/Metropolis%20Magazine%202.2014.pdf], última consulta en Julio de 2015.

136. Centro de Emergencias DF [Disponible en http://www.caepccm.df.gob.mx/], última consulta en Julio de 2015.

137. CAEPCCM [Disponible en http://www.caepccm.df.gob.mx/], última consulta en Julio de 2015.

138. Centro de Emergencias y Respuesta Inmediata [Disponible es https://twitter.com/CERI_PUEBLA] última consulta en Julio de 2015.

139. Alerta sísmica DF y aplicación para celulares [Disponible en http://www.alertasismica-df.com/], última consulta en Julio de 2015.

140. E-Gov STC IEEE [Disponible en https://sites.google.com/a/ieee.net/stc-egov/] última consulta en Julio de 2015.

141. La evolución de la seguridad cibernética: 1968-2012, Rev. NoticIEEEro-IEEE Latinoamérica, V.24, N.3 (83), pp. 31-33, 2013. ISBN: 2157-8354.

142. IEEE Spectrum, The cyber security workforce, pp 67, Nov 2011.

143. Jim Clinch, ITIL V3 and Information Security, OGC, 2007.

144. ITU-T X.1205, Series X: Data Networks, Open System Communications and Security, Telecommunication, Security - Overview of Cyber security [Disponible en http://www.itu.int/rec/T-REC-X.1205-200804-I], última consulta en Julio de 2014.

145. ISO/IEC 27032 [Disponible en http://www.iso.org/iso/iso_technical_committee.html?commid=45306], última consulta en Julio de 2015.

146. Why Cyber Security [Disponible en http://www.mod.uk/DefenceInternet/AboutDefence/], última consulta en Julio de 2015.

147. ENISA-European Network and Information Security Agency , The threat from Flame, EU, 2012 [Disponible en http://www.enisa.europa.eu/media/news-items/The-threat-from-Flamer.pdf], última consulta en julio de 2015.

148. Ben Frankel, Editor of Homeland Security Newswire, *Cyber attacks on critical infrastructure reach U.S.*, 21 November, 2012, Washington, USA.

149. Roman Rodrigo et al, *Securing the internet things*, IEEE Computer, September 2011, pp 51-58

150. Deutsche Telekom, Monitor de ataques cibernéticos [Disponible en http://sicherheitstacho.eu/], última consulta en julio de 2015.

151. Google & Arbor Networks, Digital Attack Map for DDoS, [Disponible en http://www.digitalattackmap.com], última consulta en julio de 2015.

152. Hendleer J., Lassila O, Berners-Lee T., *The semantic web*, Scientific American, pp 28-37, 2001.

153. Sanchez Carballido Juan Ramón, *Perspectivas de la información en internet: ciber democracia, redes sociales y web semántica*, Zer, pp 61-81, Vol. 13, No. 25, 2008.

Capítulo VI

154. IMF Data Maper 2016, Disponible en: http://www.imf.org/external/datamapper/index.php

155. Datos de banco Mundial, 2016 http://databank.bancomundial.org/data/views/reports/chart.aspx#

156. A National Innovation Agenda, Center for American progress, 2007, http://cdn.americanprogress.org/wp-content/uploads/issues/2007/11/pdf/innovation_chapter.pdf.

157. Smith Hedrick, Who stole the american dream?, USA, 2012

COLOFÓN

Esta obra está dirigida a quienes desean introducirse en los principios de las comunicaciones de datos que dan forma a las redes de computadoras. El valor de las referencias de corte académico es indudable, pero el corte de la experiencia agrega otro valor al texto, por ello, para que el lector tenga una idea mucho más amplia respecto de nuestra realidad en tecnología incluyo secciones que hacen referencia al estado que cada tecnología guardaba o guarda en México y, en algunos casos, en países de Latinoamérica. Adicionalmente la experiencia en la academia, industria y gobierno, así como en comités técnicos de organizaciones de estandarización, sin fines de lucro, como IEEE e ISO permite al autor abordar el texto con un enfoque amplio que combina teoría y práctica. También se abordan en lo general las 6 iniciativas IEEE: "Cloud computing", "Cyber security", "Smart cities", "IoT," "Big data" y "Smart grids", en un contexto que está gestando lo que se llamará la cuarta revolución industrial.

EL AUTOR

José Ignacio Castillo Velázquez Cuenta con 20 años de experiencia en TICs, tanto en empresas (Datacenter Dynamics, RedUno-Telmex, CEDAT-IFE y DICINET), como en universidades públicas y privadas (UACM, BUAP, UPAEP, UTM). Ha participado en más de 40 proyectos nacionales e internacionales como líder o miembro en las áreas técnicas y de gestión.

Como académico ha impartido más de 100 cursos de licenciatura y posgrado. Es árbitro en revistas (IEEE LA Transactions y Springer-Health and Technology) y congresos nacionales e internacionales (IEEE II&TT, LASCCDCN, ICEDEG, COLCOM & ROPEC). Cuenta con más de 20 publicaciones en revistas y congresos; 2 reportes técnicos y un libro. Ha impartido más de 60 conferencias magistrales en congresos nacionales e internacionales. Desde 2008 es profesor de ingeniería en electrónica y telecomunicaciones en la Universidad Autónoma de la Ciudad de México. En 2015 fue profesor visitante en la Universidad de la Defensa y Fuerza Aérea de México (UDEFA).

Como profesional y consultor ha escrito 12 reportes técnicos en telecomunicaciones y colabora como consultor para Datacenter Dynamics. Es miembro de International Computer Room Experts Association (ICREA).

En IEEE es *Senior Member* y conferencista distinguido del programa "Distinguished Visitor Program" de IEEE Computer Society (2015-2017). También es miembro de los comités técnicos de redes IEEE LAN/MAN y *cloud computing*. Fue miembro del consejo de administración de IEEE *Computer Society de 2011-2014,* donde presidió del comité de auditoría; Recibió el reconocimiento *IEEE Computer Society Golden Core Member en 2011.* En IEEE Latinoamérica ocupó los cargos de Secretario Regional 2012-2013, Editor en Jefe de NoticIEEEro 2008-2011, Presidente del comité de comunidades virtuales 2007-2010 y miembro del comité de planeación estratégica 2009-2013.

J. I. Castillo obtuvo los grados de Licenciado en Ciencias de la Electrónica con mención honorífica por la Facultad de Ciencias de la Electrónica, y la Maestría en Ciencias en Dispositivos Electrónicos en el Centro de Investigación en Dispositivos Semiconductores, ambos por la Benemérita Universidad Autónoma de Puebla, México.

ISBN 978-970-94-2968-8

9 789709 429688 >