

INTRANETS: PASADO, PRESENTE Y FUTURO

RESUMEN

Se analiza el origen, uso, desuso y futuro de las intranets. Desde una perspectiva histórica vemos su pasado: la peculiaridad del origen del término y qué fueron, y siguen siendo, las intranets. Desde una perspectiva práctica vemos su presente: qué uso tienen actualmente las intranets para distintas organizaciones, y discutimos la ambigüedad que hay al usar el término en muchos casos, provocado en gran parte por el desarrollo de la tecnología usada hoy día en Internet y en la Web. Desde una perspectiva tecnológica vemos su futuro: por qué se ha llegado al uso actual de las intranets y hacia dónde se dirige su desarrollo y uso de cara al futuro próximo.

PALABRAS CLAVE

Intranet; Internet; comunicación; historia; Web.

INTRANETS: PAST, PRESENT AND FUTURE

ABSTRACT

We analyze the origin, use, disuse and future of intranets. From a historic standpoint we see their past: the peculiarity of the origin of the term and what the intranets were and still are. From a pragmatic standpoint we see their present: what use intranets have nowadays for different organizations, and we discuss the ambiguity that arises many times when using the term, caused largely by the development of the technology used today in the Internet and the Web. From a technologic standpoint we see their future: why we have come to the current use of intranets and where their development is headed to for the near future.

KEYWORDS

Intranet; Internet; communication; history; Web.

INTRODUCCIÓN: HISTORIA DE LAS REDES DE COMPUTADORES

Como tantos otros grandes avances tecnológicos, el origen de las redes de computadores tiene tintes militares y se remonta a los años de la Guerra Fría (Segaller, 1998). El lanzamiento en 1957 del primer satélite artificial de la historia, el Sputnik, por parte de la URSS, no solo dio pie a la carrera espacial. En 1958 el Departamento de Defensa de EEUU creó la Agencia de Investigación de Proyectos Avanzados (ARPA, o DARPA como pasó a llamarse después) para el desarrollo de nuevas tecnologías de aplicación militar. Uno de los objetivos de ARPA era el desarrollo de sistemas de comunicación fiables que aseguraran la conexión de los radares en tiempos de guerra, así como la conexión de computadores en el Pentágono y otros centros militares. En 1965 Lawrence Roberts empezó a trabajar en ARPA para solucionar este problema, y le fue encargado el desarrollo de una red de comunicación entre computadores. Basándose en el trabajo de Paul Baran y Leonard Kleinrock a principios de los años 60, Roberts escribió un trabajo que dio pie a ARPANET (Roberts; Merrill, 1966), considerada la red precursora del Internet de hoy día.

EEUU obtuvo su mayor logro de la carrera espacial cuando Neil Armstrong puso sus pies en la Luna en Julio de 1969, y ARPA obtuvo uno de sus mayores logros pocos meses después, cuando en Octubre se realizó la primera conexión de datos entre los dos primeros nodos de ARPANET. A principios de los años 70 surgieron muchas otras redes inspiradas en ARPANET: en 1971 las universidades de las islas Hawai fueron interconectadas con la red de radio ALOHAnet; en 1974 Telenet apareció para dar acceso de forma comercial en siete grandes ciudades de EEUU; en 1976 la red

CYCLADES apareció en Francia y además unía centros en Londres y Roma. Todas estas redes solían tener un propósito específico, como por ejemplo el envío de mensajes.

Poco después, en 1973, los conceptos de ALOHAnet fueron ampliados en la tesis doctoral de Robert Metcalfe, que daría pie a las redes Ethernet (Metcalfe, 1976). Estas redes permitieron el acceso de múltiples computadores a una red usando el mismo medio físico de forma automática, es decir, el mismo cable de comunicación para todos. Esto supuso una verdadera explosión de redes de computadores a pequeña escala en universidades, empresas y todo tipo de organizaciones que empezaron a interconectar y compartir los sistemas que, normalmente, estaban en el mismo edificio. A día de hoy, este tipo de redes siguen siendo las más habituales para conectar ordenadores, impresoras, y otros equipos cercanos entre sí (Tanenbaum, 2003). Además de la posibilidad de acceso compartido a la red, Ethernet ofrecía otra ventaja sobre el resto de redes: velocidad. Lo habitual en la época era usar módems conectados a la red telefónica, lo cual ofrecía velocidades de tan sólo 56Kb/s. Gracias entre otras cosas a la proximidad entre los nodos que conectaba, inicialmente Ethernet permitía una velocidad de 10Mb/s.

Una vez que se establecieron las primeras redes de computadores, en ARPA se empezó a trabajar en la interconexión de las mismas. Por aquél entonces, las redes tenían mayor o menor tamaño, mayor o menor velocidad, pero no permitían la comunicación desde una a otra. Si, por ejemplo, un usuario quería enviar un correo electrónico a otro usuario, los dos debían estar conectados a la misma red. En 1974 la primera especificación de los protocolos TCP/IP vería la luz de la mano de Vinton Cerf y Robert Kahn (Cerf; Kahn, 1974). En esta especificación se hacía uso, por primera vez, del término internet, y es que de hecho estos protocolos son los que más tarde darían lugar al Internet de hoy día. Estos protocolos se diseñaron para permitir la comunicación directa desde dos computadores cualesquiera conectados a dos redes cualesquiera, y durante los nueve años siguieron evolucionando a la par que la tecnología usada en las redes de comunicación y su popularidad (Kurose; Rose, 2004). Ya en 1983 ARPANET contaba con más de 200 nodos y empezó a adoptar TCP/IP, a la vez que otras redes fueron apareciendo: Tymnet conectaba miles de empresas, universidades y agencias gubernamentales; Usenet apareció como primer foro de discusión; BITNET comunicaba varias universidades en EEUU; CompuServe se convirtió en el principal servicio de comunicaciones; JANET conectaba varios centros educativos en el Reino Unido; Minitel ofrecía en Francia servicios de compra online, reserva de trenes y correo electrónico; MCI Mail se convirtió en el primer proveedor de correo electrónico comercial en EEUU.

En 1985 la Fundación Nacional de Ciencia de EEUU (NSF), comenzó el desarrollo de su propia red: NSFNET. Ya en 1985 aparecen los primeros intentos por interconectar todas estas redes para alcanzar una red global, y NSFNET adopta TCP/IP para unirse a ARPANET. En 1988 otras redes comerciales como MCI Mail, OnTyme, CompuServe y Telemail se unen a NSFNET y, por tanto, a ARPANET. El resto de redes no tardaron en unirse también, y aparecieron los primeros Proveedores de Servicio de Internet (ISP), que ofrecían acceso comercial a esta nueva red que, usando protocolos estándar, interconectaba el resto de redes: el Internet. En 1990 ARPANET dejó de usarse, en 1991 se permitía ya el uso comercial de NSFNET, y en 1995 dejó de funcionar. La interconexión pasó a ser asumida por una nueva infraestructura desplegada por numerosos ISP comerciales que empezaban a formar el Internet que hoy conocemos. Para entonces, prácticamente todas las pequeñas redes a las que Ethernet dio paso podían interconectarse y formar la gran red de redes.

El principio de la década de los 90 fue testigo de otro de los grandes avances en Internet: la World Wide Web (WWW). En 1991 Tim Berners-Lee se basó en trabajos de varias décadas atrás para desarrollar versiones iniciales de HTML, HTTP y servidores y navegadores web (Berners-Lee, 1989). Sólo un año después ya había más de 200 servidores web en Internet, y lo que vino después ya lo conocemos. Fue tal el éxito de la Web, que muchas veces se habla de Internet como

su sinónimo. En la última década se desarrollaron diversas tecnologías, protocolos y aplicaciones que permitieron un mejor y mayor acceso a Internet y sus servicios.

PASADO: QUÉ FUERON LAS INTRANETS

Cuando en 1974 se empezó a hablar de internet, a la par se dio origen al término intranet. La idea original de TCP/IP era interconectar varias redes ya existentes, a cada una de las cuales llamaron intranets. Internet sería pues la interconexión de todas esas intranets. La propia ARPANET, NSFNET, Telemail, Minitel, Usenet y tantas otras, eran consideradas intranets en el sentido de que un usuario sólo se podía comunicar con otro si ambos formaban parte de la misma red. En particular, las redes Ethernet que proliferaron tanto en las décadas de los 70 y los 80 son un ejemplo perfecto de intranet porque sólo los computadores conectados a esa red podían tener acceso unos con otros, y toda comunicación permanecía en esa Ethernet: no había comunicaciones ni hacia ni desde fuera. Con la llegada de TCP/IP todas estas redes empezaron a usar los mismos protocolos, por lo que la comunicación entre nodos de dos redes distintas al fin se hacía posible.

Sin embargo, a pesar del desmesurado crecimiento de Internet, algunas intranets siguieron sin ser interconectadas, manteniendo su carácter privado y desconectado. Varias razones podían llevar a una organización a este extremo, pero principalmente eran dos: la seguridad y la velocidad de las redes.

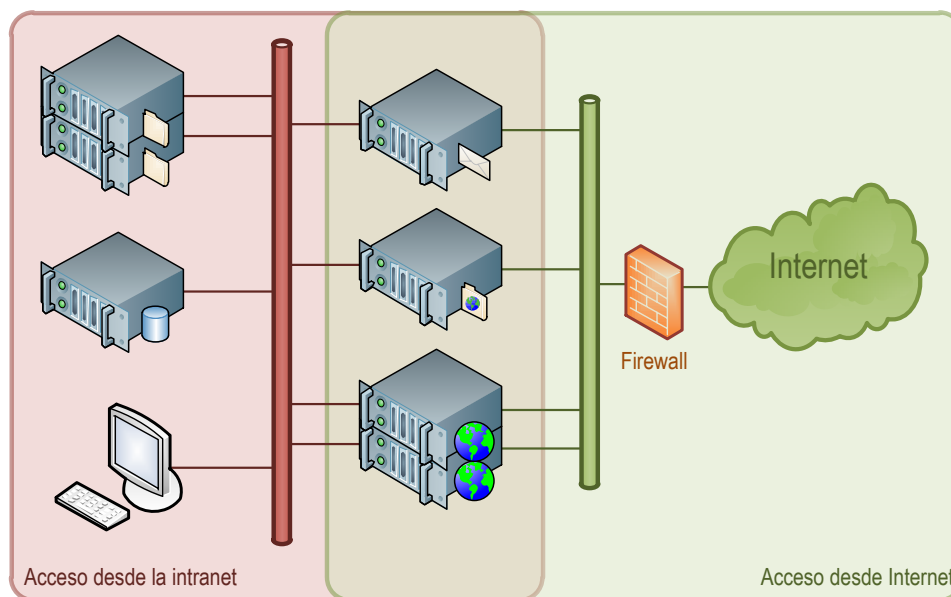


Figura. Un ejemplo de intranet parcialmente accesible desde Internet. En la parte izquierda de la intranet (en rojo) un ordenador personal y seis servidores están conectados, y todos pueden acceder a Internet. En la parte de Internet (en verde), un firewall corta los intentos de acceso a la intranet, permitiendo sólo accesos a los servidores que se han hecho públicos (los de la zona intermedia) y no a los de la derecha (privados de la intranet).

Hasta que las redes se abrieron, la seguridad no se consideraba un problema grave. Después de todo, sólo gente autorizada a usar un terminal de la red podía acceder a la información. Sin embargo, con la aparición de Internet se hizo patente la necesidad de establecer protocolos criptográficos para asegurar ciertos servicios de seguridad como la autenticación y el cifrado de datos. A principios de los años 80 ya se contaba con algoritmos criptográficos ampliamente aceptados como DES, y a principios de los 90 aparecieron los primeros firewalls para controlar el tráfico, así como otros algoritmos orientados a la firma digital como MD5 y SHA-1 (Stallings, 2003). Sin embargo, estos algoritmos no fueron utilizados por protocolos de Internet hasta 1995, cuando empiezan a aparecer IPSec, TLS, HTTPS, PPP y otros. Su implantación se retrasaría más aun, y no eran muy comunes hasta finales de siglo. Dado que las redes de computadores

eran mayoritariamente usadas por agencias gubernamentales y empresas, la información que por ellas viajaba era lo suficientemente sensible como para necesitar servicios de seguridad. Como la tecnología de la época no ofrecía suficientes garantías, no había mejor seguridad que mantener las redes cerradas y permitir el acceso a sus terminales solo al personal autorizado. Es decir, mantener una intranet fuera de Internet.

La velocidad de las redes disponibles también suponía un problema. Si los usuarios de una organización tenían que acceder a grandes volúmenes de datos (relativos a la época, claro), el uso de comunicaciones sobre la infraestructura de la red telefónica podía suponer grandes tiempos de espera. Sin embargo, con las redes Ethernet se podían alcanzar velocidades de varios Megabits por segundo, y hacia la mitad de los años 90 ya se disponía de las redes a 100Mb/s que aun en nuestros días siguen siendo tan populares. Así pues, en organizaciones que trabajaban con grandes volúmenes de datos, como agencias militares y administrativas o bancos, era normal mantener intranets conectando sus trabajadores y servidores. Con el uso de firewalls apropiados, estos usuarios podían estar conectados a Internet, pero se podía denegar el acceso no permitido desde el exterior.

PRESENTE: QUÉ SON LAS INTRANETS

En pleno siglo XXI, donde Internet llega a un cuarto de la población mundial, las intranets siguen teniendo mucha importancia para distintas organizaciones. Gracias a tecnología como las Redes Privadas Virtuales (VPN), impulsadas en parte por la aparición de protocolos de seguridad, se permite a empleados conectarse a las intranets de su empresa para trabajar desde otros sitios (Tanenbaum, 2003). Es importante recalcar que la intranet sigue sin poder ser accedida directamente desde el exterior, sino que se usan protocolos que permiten a usuarios remotos aparecer en la red como si estuvieran físicamente dentro de la misma. Por otro lado, el volumen y complejidad de la información digital con que se trabaja en nuestros días no para de crecer, y el uso de información multimedia hace que los archivos de empresas y otras organizaciones cada vez sea mayor (Gantz; Reinsel, 2010). Aunque puedan haber impedimentos tecnológicos y de formación para trabajar con grandes cantidades de información (Barreau, 2009), la velocidad de las conexiones a Internet desde zonas residenciales es hoy día suficientemente alta como para permitir trabajar de forma interactiva desde casa y desde otros lugares geográficamente muy apartados. Esta capacidad de las redes, unida a la tecnología VPN, hace que cada día sea más fácil acceder a las intranets de forma suficientemente segura y controlada, aunque sigan sin ser parte directa de Internet al estar su acceso restringido al público general.

Además, si a la mejora en estandarización, seguridad y velocidad unimos el amplio despliegue y éxito de la Web, nos encontramos con una plataforma y una tecnología idóneas para abrir las intranets al exterior, o al menos parte de ellas (Eíto, 2002). Ejemplos claros de los beneficios de esta unión son los servicios de comercio electrónico seguro como Amazon (<http://www.amazon.com>) y los servicios de streaming de video como Youtube (<http://www.youtube.com>). Con el nuevo siglo aparecieron multitud de plataformas y gestores de contenido que permiten a una organización gestionar y controlar el acceso a sus recursos de una forma sencilla (Goodwin, 2011). Por ejemplo, varias organizaciones usan el mismo software que Wikipedia (<http://www.wikimedia.org>) para gestionar su cuerpo de conocimiento y mantenerlo accesible a sus empleados; otros servicios permiten el acceso a archivos y bases de datos específicos; hay software que ofrece servicios de correo electrónico, agenda y mensajería instantánea para empleados de una organización. En el peor de los casos, todas estas plataformas suelen ser suficientemente fáciles de extender y configurar para necesidades propias de cada organismo, y en el mejor de los casos son además gratuitas y ofrecen multitud de añadidos listos para ser usados.

Así pues, en multitud de casos hoy día varios de estos servicios que antes eran privados y permanecían dentro de las intranets, son ahora llevados al exterior y alojados en la Web, donde

pueden ser accedidos desde cualquier sitio. Ahora bien, gracias a los protocolos de seguridad y a la implementación de ciertos mecanismos en estas plataformas, sólo las personas autorizadas tienen acceso a los diferentes recursos que la organización lleve al exterior (Urbano, 2002). En la mayoría de casos los empleados acceden a estos recursos desde una página particular en la web corporativa, en la cual deben autenticarse con un nombre de usuario y una contraseña. Tanto a esta página, como a la zona privada del site a la que da acceso, se las suele denominar intranet, aunque de forma incorrecta. De hecho, en muchos casos la intranet ha desaparecido completamente, pues no hay una red privada de la organización a la que no se tiene acceso desde el exterior. Es más, no se accede a ninguna otra red al autenticarse en estos sitios: durante todo el proceso trabajamos únicamente con Internet. Estas partes de sites corporativos son también conocidas como portales privados, y suelen llevar a confusión con el término intranet, que en su origen se refería a la infraestructura física de una red y no a los servicios que proporcionaba.

Cuántos casos hay de este uso del término intranet es prácticamente imposible de saber, pero una búsqueda en Google nos puede dar una idea. Si buscamos la frase “acceso intranet” obtenemos cerca de 900.000 resultados de páginas de universidades, centros de investigación y distintas empresas. Una revisión rápida de los primeros 30 resultados nos indica que 26 de esas 30 páginas sirven para que los empleados se autenticuen y tengan acceso a ciertos recursos privados, haciendo uso de otro significado del término intranet. Por ejemplo, el site del Departamento de Informática en la Universidad Carlos III de Madrid (<https://www.inf.uc3m.es/es/acceso>), o el Centro Superior de Investigaciones Científicas (<https://intranet.csic.es>), siguen esta convención al referirse a partes privadas del portal y no a la red en sí, que sigue siendo Internet.

Esto tampoco significa que una organización con este tipo de plataformas disponibles online no disponga de intranets. Por ejemplo, los bancos tienen una web corporativa públicamente accesible desde Internet, desde la cual los clientes y trabajadores pueden acceder a zonas privadas para, por ejemplo, gestionar sus cuentas y realizar transferencias. Sin embargo, cada sucursal suele tener una intranet que conecta las estaciones de trabajo de los empleados y una serie de servidores, normalmente usando tecnología Ethernet. Aunque los empleados pueden acceder a Internet, un firewall impide el acceso a los recursos de la intranet desde el exterior. A su vez, estas sucursales están conectadas con las oficinas centrales del banco, en donde probablemente hay intranets que conectan los servidores centrales para realizar todos los procesos de tratamiento de datos.



Así pues, las intranets siguen jugando un papel muy importante en las comunicaciones actuales, aunque cada vez son más particulares de escenarios selectos como banca, administraciones, agencias gubernamentales, centros militares y diplomáticos, etc. Un ejemplo muy claro apareció recientemente con el caso de la fuga de comunicaciones secretas entre embajadas estadounidenses, filtrado por la asociación WikiLeaks a finales de 2010 (Assange, 2011). SIPRNet y NIPRNet son dos de las redes de comunicación usadas por el Departamento de Defensa y el Departamento de Estado de EEUU, y que a principios de los años 90 sustituyeron a la red MILNET, que a su vez formaba parte de ARPANET. Estas redes pueden ser consideradas intranets porque no son accesibles desde Internet, y sólo permiten el acceso desde ciertos terminales dispuestos, entre otros sitios, en embajadas y bases militares. Bradley Manning, un soldado de la Armada de EEUU, accedió a mediados de 2010 a SIPRNet desde un terminal en su base militar en Irak y descargó a su ordenador personal cerca de 250.000 documentos secretos que están siendo publicados poco a poco por parte de WikiLeaks y varios medios de prensa de todo el mundo (El País, 2010).

Una situación similar se dio en el Ejército de España el pasado 2009 (El Confidencial Digital, 2011). Varios archivos de inteligencia, con información sobre militares y agentes del Centro de Seguridad del

Ejército de Tierra fueron compartidos en redes P2P. Estos archivos contenían información de alto secreto que se usaban en la red del centro, y fueron compartidos por negligencia de un empleado que usaba el programa de intercambio de archivos eMule, debido a una mala configuración de su sistema. A la vez, estos son ejemplos de qué es realmente una intranet y de que, por supuesto, no son infalibles, pues muchas veces el factor de riesgo es el humano y no el tecnológico.

FUTURO: QUÉ SERÁN LAS INTRANETS

En los últimos años Internet y las redes de computadores se han ido desarrollando en la dirección de la movilidad y la ubicuidad. Cada día son más los dispositivos que, como los teléfonos móviles, permiten conexión a Internet desde prácticamente cualquier sitio. En general, la globalización obliga a usar estas conexiones móviles y remotas, y acentúa mucho la necesidad de tecnología de banda ancha, protocolos de seguridad y acceso a redes virtuales y tecnología Web. Poco a poco toda la información relevante de una empresa podrá estar en Internet de forma segura, lo que de por sí permitirá reducir costes de mantenimiento, y podrá ser accedida de forma eficiente por sus empleados. En esta línea son de suma importancia los avances en algoritmos y protocolos de seguridad, de los que a su vez dependen las plataformas de comercio electrónico; el progresivo aumento de la velocidad y ancho de banda de las conexiones a Internet; y los avances en compresión de datos que permitan reducir los tiempos de

transferencia, con especial énfasis en grandes bases de datos y grandes archivos multimedia. A su vez, la proliferación de redes P2P, Web 2.0, Web semántica y redes sociales hacen que cada vez se estudien más los aspectos colaborativos de Internet y de la Web, lo que presenta ventajas para los usuarios que poco a poco han de usar estas tecnologías no sólo por ocio, lo que reduce la necesidad de formación ante estas nuevas tecnologías que usamos de forma cotidiana.

Poco a poco toda esta información que antes permanecía cerrada en intranets se abrirá a Internet por medio de plataformas web que, seguramente, seguirán llamándose intranets, y el uso de VPN y accesos remotos estará al orden del día para acceder a recursos que, por unos motivos o por otros, no pueden ser sacados al exterior de forma directa. En cualquier caso, el uso de intranets seguirá produciéndose en entornos selectos de características militares, políticas y financieras donde los requisitos de seguridad y velocidad aun no pueden ser satisfechos o deben ser máximos.

CONCLUSIONES

Las redes de computadores son uno de los principales valores para cualquier organización. El nacimiento de Internet abrió puertas antes inimaginables al interconectar varias redes de propósito específico ya existentes. En el momento en que Internet estaba siendo creado, cada una de esas redes específicas fue llamada intranet, y su hasta entonces característico uso privado y restringido ha seguido con nosotros hasta las intranets de hoy día, basadas por lo general en tecnología Ethernet. Innumerables organizaciones han usado, y siguen usando, redes de computadores para conectar a sus empleados y compartir sus recursos de forma eficiente. Si estas redes no pueden ser accedidas directamente desde Internet, son llamadas intranets en correspondencia con las intranets originales que dieron lugar a Internet.

Sin embargo, el desarrollo de nuevos protocolos para Internet, especialmente en cuanto a seguridad y acceso virtual, así como el aumento en la velocidad de las redes, ha provocado un progresivo acercamiento de las intranets hacia Internet. Además, la inmediata expansión y mejora de la tecnología Web ha hecho que muchos de los recursos que las organizaciones mantenían en sus intranets vayan poco a poco siendo llevadas a Internet en forma de portales web de acceso restringido. Es aquí cuando el término intranet resulta ambiguo al confundirse la infraestructura de red de acceso restringido con la plataforma web corporativa de acceso restringido que permite publicar recursos online más fácilmente.

La tecnología asociada a Internet y a la Web sigue creciendo y madurando a pasos agigantados, con un enfoque muy claro en las redes móviles y la computación ubicua, así como en las redes sociales y la Web 2.0. Todos estos desarrollos hacen que los recursos que antes estaban cerrados en intranets aparezcan poco a poco en la gran red acompañando al resto de servicios que hemos venido a usar todos los días, pero con los mecanismos adecuados para seguir restringiendo el acceso. En cualquier caso, muchas de las intranets seguirán siendo totalmente cerradas, especialmente en entornos militares y financieros, debido a la sensibilidad de la información que por ellas circula.

REFERENCIAS

- J. Assange, "WikiLeaks", <http://www.wikileaks.ch>, accedido Enero 2011.
- D. Barreau, "Gestión de información personal, no sólo recuperación de información personal", *El profesional de la información*, vol. 18, n. 4, pp. 361-364, 2009.

- T. Berners-Lee, "Information management: a proposal", CERN, 1989.
<http://www.w3.org/History/1989/proposal.html>, accedido Enero 2011.
- V. Cerf y R. Kahn, "A protocol for packet network intercommunication", IEEE Transactions on Communications Technology, vol. 22, no. 5, pp. 627-641, 1974.
- El Confidencial Digital, "Wikileaks en el Ministerio de Defensa español. Detectadas fugas de información: incluyen lista, dirección y coches de los 'espías militares'. La filtración se produjo por eMule", 14 de Febrero de 2011,
<http://www.elconfidencialdigital.com/Articulo.aspx?IdObjeto=27766>, accedido Marzo 2011.
- R. Eíto Brun, "¿La colaboración será libre?", El profesional de la información, vol. 11, no. 1, pp. 34-46, 2002.
- J. Gantz y D. Reinsel, "The Digital Universe Decade, Are You Ready?", IDC iView, 2010.
- S. Goodwin, "Open Source CMS Demos & Information", <http://www.opensourcecms.com>, accedido Enero 2011.
- J. Kurose y K. Ross, "Redes de computadores: un enfoque descendente basado en Internet", Addison Wesley, 2ª edición, 2004.
- R. M. Metcalfe y D. R. Boggs, "Ethernet: distributed packet switching for local computer networks", Communications of the ACM, vol. 19, no. 7, pp. 295-404, 1976.
- El País, "Preguntas y respuestas sobre los papeles del Departamento de Estado", 28 de Noviembre de 2010,
http://www.elpais.com/articulo/internacional/Preguntas/respuestas/papeles/Departamento/Estado/elpepuint/20101128elpepuint_11/Tes, accedido Enero 2011.
- L. Roberts y T. Merril, "Toward a cooperative network of time-shared computers", AFIPS Fall Conference, 1966.
- S. Segaller, "Nerds 2.0.1, A brief history of the Internet", TV Books, 1998.
- W. Stallings, "Fundamentos de seguridad en redes", Prentice Hall, 2003.
- A. S. Tanenbaum, "Redes de Computadoras", Prentice Hall, 4ª edición, 2003.
- J. A. Urbano Pérez, "El portal intranet, una plataforma abierta para la información", El profesional de la información, vol. 11, no. 1, pp. 9-13, 2002.