novática
Revista
de la Asociación
de Técnicos
de Informática
SEPTIEMBRE - OCTUBRE 1998
135

/DOCS/Rentabilidad de las inversiones en TI y complejidad

7882334

Comercio Electrónico

novática
Revista de la Asociación de Técnicos de Informática

SEPTIEMBRE - OCTUBRE 1998

135

SUMARIO

Novática, revista fundada en 1975, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática)

ATI es miembro de CEPIS y tiene un acuerdo de colaboración con ACM. Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AII y ASTIC

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3°, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 / *novatica@ati.es*
Composición, Edición y Redacción ATI Valencia
Palomino 14, 2°, 46003 Valencia
Tlf./fax 963918531 / *secreval@ati.es*
Administración y Redacción ATI Cataluña
Via Laietana 41, 1°, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 / *secregen@ati.es*
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 / *secreand@ati.es*
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 / *secreara@ati.es*
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 / *gpgal@ati.es*

Publicidad: Padilla 66, 3°, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 / *novatica.publicidad@ati.es*

Imprenta: Gráficas Sierra S.L., Atenas, 3, int. bajo, 08006 Barcelona.
Depósito Legal: B 15.154-1975
ISBN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix

Presentación

Comercio Electrónico

José A. Mañas
Consultor independiente, E.T.S.I. de Telecomunicación, Universidad Politécnica de Madrid

jmanas@selva.dit.upm.es

¿Qué es comercio electrónico? Una pregunta inocente pero que no tiene una contestación fácil o, para ser más preciso, no tiene una contestación única. Si comerciar es intercambiar bienes, materiales e inmateriales, comercio es el conjunto de actividades que soportan dicho intercambio y lo llevan a buen fin, y comercio electrónico es lo mismo pero soportado con tecnologías de la información y comunicaciones. O sea que cada vez que ponemos un poco de informática o de telecomunicaciones al servicio de un proceso de negocio estamos haciendo comercio electrónico.

Alguno dirá que esto no es ninguna novedad y en efecto, la evolución desde los fenicios y los trueques de mercancías hasta la fecha no ha sido sino un continuo evolucionar pasando por el dinero como valor de intercambio, el papel como soporte y la utilización de las nuevas tecnologías según han ido apareciendo y, sobre todo, convirtiéndose en soporte ubicuo (lo que los ingleses llaman *commodities*). Porque es difícil negarle al teléfono, al télex o al fax el calificativo de medios electrónicos de soporte al proceso comercial. Por no hablar del uso de las tarjetas de plástico o los intercambios EDI.

¿Qué hay ahora de nuevo? Pues nada en concreto, pero sí una conjunción de nuevos medios y una penetración espectacular. Se llama digitalización (o soporte multimedia), se llama comunicaciones (o líneas de teléfono y módems por doquier) y se llama protocolos aceptados universalmente. Abusando un poco del término, se llama Internet. En conjunto tenemos medios muy potentes de intercambio de información, ampliamente accesibles a una parte sustancial de potenciales compradores y vendedores. Disponemos de un medio tecnológico compartido para compartir información, para pasar de unos a otros sistemas, de unos a otros datos sin solución de continuidad, evitando la tediosa reintroducción manual de datos (que, además es fuente notoria de errores y ruido en el sistema), y garantizando la supervivencia de datos correctos a lo largo de toda la cadena de valor.

Esta percepción de que se pueden hacer maravillas con la tecnología disponible y el alcance global levanta cantidades ingentes de dinero que busca rentabilidad rápida y elevada, capital-riesgo que apoya el nacimiento de nuevas empresas que con extrema agresividad quieren hacerse un sitio entre las grandes. Entre la fortuna del nombre y la actividad de marketing de estas empresas tenemos un fenómeno que, amplificado por los medios de comunicación, da lugar a la moda actual.

Personalmente pienso que esta es una moda que va a quedarse con nosotros. La novedad se irá convirtiendo en hábito cotidiano y nos iremos acostumbrando a nuevas formas de comprar y de vender. Nuevas formas que revuelven muchas cosas que creemos establecidas y asentadas pero que en definitiva son consecuencia de los medios disponibles.

Empezamos por la intermediación, que se ve fuertemente afectada por la globalización y por la posibilidad de acceso directo entre compradores y vendedores. No creo que vayan a desaparecer los intermediarios pero sí estoy seguro de que no los va a reconocer ni su madre dentro de unos años: adaptarse o adaptarse, no hay más opción. Y van a cambiar los bienes comercializables, donde van tomando cada vez más auge los bienes inmateriales o intangibles (información y servicios, primordialmente) que son idóneos para una entrega sobre soporte electrónico. Y va a cambiar la capacidad de elegir cuando vamos a de compra, pues la conectividad mundial nos acerca a cualquier rincón del globo con bastante facilidad, si bien hay un límite: la logística de distribución y entrega al cliente final. Y va a cambiar el análisis de mercados, la estimación del público objetivo al que un comercio puede dirigir su fuerza de ventas.

Parece pues que va a cambiar todo, o más bien ya está cambiando todo, y poco a poco nos vamos acostumbrando a vivir en este nuevo modelo de comercialización. Un nuevo escenario que tiene que reproducir uno de los componentes más delicados de los intervinientes: la confianza mutua, entre las partes y en el medio. No hay comercio si no nos fiamos y las nuevas tecnologías son un mar profundo y agitado en el que a veces no sabes si haces pie o si navegas sobre una charca llena de tiburones. Esta confianza se está buscando a marchas forzadas, explotando la criptografía como jamás se había hecho (ni en las más sofisticadas guerras), desarrollando protocolos de utilización que garanticen el resultado final incluso cuando fallan las partes involucradas y buscando mecanismos de identificación fehaciente de las partes que permitan intercambiar bienes y dineros con confianza.

Dentro del mar de cosas que es la actividad comercial, una singular es el pago. Siempre hay que pagar. Y pagar es un tema que se lleva muchos siglos cuidando con precaución y mimando en extremo, pues la relación entre las personas, entre las empresas y entre las naciones se basa en que nos podamos fiar de esa cosa llamada dinero que representa un valor por el que alguien debe responder. Es un tema muy delicado al que se ha ido dotando de solidez a través de la economía mundial y del sistema financiero. No podemos tirar por la borda todo lo logrado y sustituirlo sin más por nuevas cositas electrónicas. Primero porque la confianza no se crea de la noche a la mañana, segundo porque la experiencia requiere años de utilización, y tercero porque el comercio tradicional no va a desaparecer y hay que hacerles convivir: lo clásico y lo nuevo, sin solución de continuidad.

En este escenario, innovador pero realista, hemos intentado llenar esta monografía de Novática, seleccionando aquellas contribuciones que ayudan a entender los aspectos operativos y de integración de la nueva faz electrónica del comercio. Con un toque nacional, si se me permite decirlo. Porque una cosa son los Estados Unidos donde la venta por catálogo parecen llevarla en la sangre e Internet no es sino un nuevo canal para seguir haciendo lo mismo. Otra cosa es España, donde la cultura de las tarjetas de plástico ha crecido espectacularmente y se usa con absoluta normalidad. Otra es Europa, donde la diversidad es monetaria, de idioma y de culturas y costumbres.

No creo que debamos pensar que lo que ocurre en EE.UU va a ocurrir en España sin más misterio que esperar un plazo prudencial para que penetre. Toda adopción tecnológica supone una adopción y una integración, y la integración del comercio electrónico en la cultura comercial española la estamos viendo ya y la veremos asentarse en los próximos años, años por otra parte muy complejos pues coinciden con la integración económica europea, creando una situación única, complicada pero con muchísimas oportunidades para ir muy muy lejos.

Volviendo a nuestro monográfico, tenemos una visión magistral de la situación en nuestro país de la mano de Rodolfo Carpintier, Presidente de CommerceNet en España. A continuación la visión más académica de Manel Medina, de la Politécnica de Catalunya, que nos acerca la problemática del proceso de pago. El punto de vista legal nos lo aporta Xavier Ribas, abogado, comentando la situación actual de la legislación sobre firma digital de la Comunidad Europea. Francisco Ruiz, de Telefónica I+D, nos centra en la problemática y las soluciones disponibles para el comercio entre empresas. Seguiremos con la descripción de Cybermercado, una interesante experiencia en desarrollo en Asturias. Y terminaremos con un análisis de los protocolos de micropago, la que parece ser la solución para pagar electrónicamente cuando los costes de las tarjetas de plástico empiezan a ser desproporcionados.

Y más pusiéramos si tiempo y espacio hubiera, que aunque son todos los que están, mucho nos queda en el tintero para desarrollar, pues tan complejo es el mundo comercial que imposible resulta contemplarlo en su totalidad en media docena de artículos. Espero que la selección haya sido afortunada y que los lectores de Novática tengan al cabo de la lectura de este número una visión amplia y abierta de lo que el comercio puede ser cuando los medios sean electrónicos.

Comercio Electrónico

¿Comercio Electrónico en Internet?... ¿En España?

Rodolfo Carpintier
Presidente Commerce Net Español

rcarpintier@smmkt.es

Mientras las grandes consultoras mundiales anuncian el despegue definitivo del **Comercio Electrónico** mundial. ***Forrester Research*** (*http://www.forrester.com*) habla de 207 mil millones de dólares en el año 2000. Europa en general, con unos 67 mil millones de dólares según la misma fuente y España en particular, esta vez en mi propia estimación, apenas facturará 28 mil millones de...pts. No se lo traduzco a dólares para que no les de pena la cifra.

En este año el Comercio Electrónico en España dará un pequeño salto. Se habla de cifras entre los 1.500 millones de pts. y los 3.000 millones. Subir esta cifra, en tan solo dos años, a los 28 mil que espero se facturen en los albores del cambio de siglo es un buen salto. Sin embargo, no es suficiente si no queremos vernos en la situación de ser (o cuanto menos parecer) unos subdesarrollados virtuales y todos debemos contribuir a que esta nueva forma de hacer negocios se implante en España.

En realidad, soy optimista, creo que, como pasó con el acceso a Internet, en España habrá un salto hacia el Comercio Electrónico que hará mejorar nuestro posicionamiento global rápidamente. El país líder, EE.UU., comprará una media de 2.000 dólares por usuario de Internet en el año 2000 (Forrester *dixit*) mientras que los 28.000 millones de pts. que yo menciono representan, según el desarrollo del número de usuarios de Internet que se estime, entre unos 75 y unos 150 dólares de compra electrónica en España. La UE, con excepción de los Países Escandinavos, que estarán casi a la altura de los americanos, estará de media entre los 300 y los 600 dólares. Es decir, entre un 25 y un 30 % de la cifra de EE.UU.

Para los americanos Internet se ha convertido en un nuevo 'maná' caído del cielo. Su influencia ha convertido al inglés en el lenguaje franco de la red y todos los cibernautas pueden, cuanto menos, manejarse en ese idioma. Esto ha traído como consecuencia el que las empresas americanas en La Red contemplen el mundo como el patio de su casa y sean capaces de crear PYMES multinacionales a un ritmo feroz que hace peligrar la competitividad futura de las nuestras.

Desde la Asociación que presido, **Commerce Net Español** (*http://www.commercenet.org*) estamos intentando promover un consenso entre nuestros asociados y la Administración para implementar un Plan de Choque que contribuya al lanzamiento del Comercio Electrónico en España. Como recientemente mencionaba mi buen amigo Luis Carrera en su editorial en *Gran Cuenta*, los países nórdicos lo han hecho con gran éxito y han conseguido reconvertir a buena parte de la población parada e integrarla de nuevo en los procesos productivos de su país.

El caso de EE.UU. es una demostración de que, bien promocionadas, las nuevas tecnologías crean puestos de trabajo aunque, de momento, produzcan paro en las capas menos preparadas de la sociedad. Existe además un riesgo adicional inminente: en el mercado global que se ha conformado alrededor de Internet, si Europa no reacciona, nuestra juventud, ayudados por la apertura de sus Leyes de Inmigración para profesionales de la Tecnologías de la Información, emigrarán a EE.UU. que, de nuevo, un siglo más tarde, vuelve a ser El Dorado. Si no reaccionamos, se aproxima un nuevo *brain drain* (fuga de cerebros) europeo hacia America que, además, en muchos casos y gracias al teletrabajo, servirá para crear verdaderas colonias de europeos trabajando para empresas americanas desde el Viejo Continente.

La anterior característica del idioma inglés -convertido en un nuevo Esperanto en la Red- hace que muchas PYMES americanas de alta tecnología sean capaces de estar en docenas de países a los pocos días de haber construido su oferta sobre una Web en Internet. Esto crea una nueva demanda sobre los recursos informáticos necesarios para poder atender y prestar un buen servicio a miles de clientes en pocas horas y obliga a un nuevo planteamiento de lo que es una PYME y a lo que son sus necesidades de financiación.

También aquí los americanos lo tienen más fácil. Los inversores de Capital Riesgo y las Grandes Empresas americanas están mucho más inclinados a apoyar un nuevo proyecto en base a un Plan de Negocio bien formulado y suficiente credibilidad profesional del equipo directivo. Algo que, en Europa y, sobre todo, en España es mucho más dificil.

El resultado es que la empresa española que se plantea comerciar en Internet, lo hace sin visión global y como prueba. El resultado es siempre descorazonador. Mientras tanto, Amazon ha pasado a ser una de las librerías de más venta en España y multitud de pequeñas empresas americanas de software, de tamaño ínfimo y perfectamente comparables a otras existentes en España, tienen ya venta electrónica de sus productos en toda Europa. En España, no conozco muchas empresas de 10/15 personas que hayan concebido un producto de software con atractivo global ni que se lo hayan planteado desde un primer momento como tal. A la PYME europea -sobre todo a la española- le falta garra y ambición para dominar un mercado emergente... aunque lo hayan inventado, que existen ya casos. Una de las multinacionales del software antivirus tiene origen español aunque, para lograrlo, tuviera que fijar su sede en EE.UU.

Meta4 (*http://www.meta4.es/*) es probablemente otro caso a emular. La compra de una participación en la empresa por la multinacional **BAAN** (*http://www.baan.com/*) sólo confirma el proyección multinacional de la compañía, líder tecnológico en el desarrollo de software de gestión de RR.HH.

Ya he explicado en algún otro de mis artículos que España, con la proliferación de Proveedores de Internet, ha formado un equipo técnico de calidad en todas las tecnologías de la Red y tiene por ello el recurso más importante para la creación de empresas de nuevo cuño, el conocimiento... Sepamos canalizarlo.

¿Cómo conseguir que Europa tenga un buen posicionamiento en el Comercio Electrónico del futuro? Desde luego no es falta de tecnología, ni es falta de seguridad en la Red. Es,

sobre todo, una falta de cultura sobre la llamada **Economía Digital** (Negroponte). En ella, por definición, cualquier nueva empresa debe aspirar a ser global. Para ello la concepción empresarial, la preparación de sus gente y los planteamientos transaccionales previstos deben ir unidos a una visión de globalidad que no es frecuente en Europa.

Las PYMES europeas creen que, por ser pequeñas, no pueden aspirar más que a un mercado muy local, cuanto mucho nacional. Su ambición termina ahí. Esa es la gran diferencia con el mercado americano...

En EE.UU. se ha asumido el que una buena idea con atractivo global hay que venderla, casi desde el principio, a nivel mundial, si no, se llega demasiado tarde. Por ello, tras una fase muy breve de lanzamiento a nivel USA, empiezan una expansión furiosa luchando por copar el mayor número posible de mercados. Eso requiere infraestructura, conocimiento de los mayores mercados, contactos rápidos y contratos muy pensados para cualquier eventualidad.

Esto no se consigue sin inversiones importantes, en general fuera del alcance de una PYME, ahí es donde los americanos tienen una ventaja de salida importante ya que sus accesos a Capital Riesgo y *Development Funds* (inversores para desarrollo) es mucho más fácil que el viejo continente.

Desde Asociaciones como **Commerce Net Español**,debemos fomentar tanto el cambio de cultura inicial como la facilidad para conseguir fondos cuando una empresa dispone de un producto o servicio de atractivo global. Nuestra misión debe ser el convencer a la Administración, central y regional, que sus intereses son los mismos que los de sus empresas pioneras y que tendrán más éxito cuando más capaces sean de descubrir, arropar y motivar al despeque a este tipo de empresas de nuevo cuño. Algunas regiones (la Comunidad Valenciana, por ejemplo) están queriendo crear infraestructuras de soporte y mejorar la accesibilidad de sus empresas a nuevas formas de financiación pero, en Europa, con la CE cada día más burocratizada, es difícil conseguir algo comparable a los mercados financieros que se han creado alrededor de Silicon Valley. Sólo la región de Munich, en Alemania, poco a poco, parece ser un entorno comparable.

Unas recientes declaraciones del *President* Jordi Pujol en Cataluña ponen cierta esperanza para España, aunque de momento se centre en su área de influencia. Bien es verdad que Cataluña, según las últimas estadísticas del **EGM**, ha duplicado su número de internautas en tan solo medio año dejando atrás a las demás regiones y tiene una Institución de carácter y objetivo global, **LA CAIXA** (*http://www.lacaixa.es*) que está entre los líderes dentro del sector de Grandes Empresas, en la aplicación de nuevos conceptos de comercio electrónico y soporte a sus PYMES para que entren en él. Creo que la banca tiene un papel importante que jugar y que este tipo de iniciativas son básicas para un despegue en Europa y, sobre todo, en España.

La Banca Española es líder mundial en la aplicación de tecnologías de la información a la gestión bancaria. No debemos dejar que ello se convierta en un impedimento para el desarrollo de un mercado abierto como el de Internet. Francia, que, debido al éxito del **MINITEL**, ha sido algo tardía en su aplicación de soluciones de comercio electrónico a este nuevo medio, ahora está acelerando sus inversiones, tanto en infraestructura como en soporte de la Administración y se espera que, a finales del 2001 esté ya en segunda o tercera posición en Europa, detrás sólo de Alemania y/o Inglaterra.
Iniciativas como la llevadas a cabo por **OPENBANK** (*http://www.openbank.es*), **BANESTO** (*http://www.banesto.es*), **Banco Santander** (*http://www.bsantander.com*), **BANKINTER** (*http://www.bankinter.es*), **BANC SABADELL** (*http://www.BancSabadell.es*) o **Argentaria** (*http://www.argentaria.es*) no deben ser enjuiciadas a corto plazo por su Dirección. Estos esfuerzos iniciales son costosos y solamente probarán su valía con el tiempo.

Sin embargo, en la banca española se está extendiendo una peligrosa impresión de que "esto de Internet es carísimo y no aporta nada a la cuenta de resultados" cuando, en realidad, el problema es que, incluso estas iniciativas, se quedan cortas en lo que deberían hacer como soporte a sus empresas, existentes y futuras, y que quizás el resultado es precisamente debido a la falta de convicción real necesaria a nivel de los Consejos de Administración, que siguen viendo sus iniciativas como "una aventura de ....(en cada banco existe una persona, verdadero motor de esta iniciativa)", quien, aparte de su carrera, ha puesto un esfuerzo personal importante en su concepción del comercio electrónico y el posicionamiento que en él debe jugar su banco. Que no termine la historia con la muerte (virtual con el exilio) del mensajero.

España, que tiene ya poca industria local que defender, podría y debería ser mucho más agresiva en perseguir el lanzamiento de nuevas empresas de la **Economía Digital** que fueran capaces de llevar sus ventas a EL DORADO que representa los EE.UU. Existe una revista americana muy activa en el seguimiento de los nuevos conceptos empresariales, ***Fast Company*** (*http://www.fastcompany.com*) , que en un reciente número nos habla de lo mal preparado que está el mundo actual para enjuiciar las presentaciones reales de la nueva economía. En concreto cita el ejemplo de una persona, propietaria de su propia consultora de marketing - después de una carrera de éxito en *Procter & Gamble*- y con trabajo hasta el año 2000 que ve con incredulidad que su banco le deniega un préstamo porqué no tiene nómina, ni ingresos regulares que avalen su capacidad para devolverlo.

Sin embargo, el mismo banco le concede a su marido, sin pensarlo dos veces, un préstamos por una cifra superior, a pesar de que su empleo, de alto ejecutivo en una acería de la ciudad, está en juego ya que han anunciado una reducción de plantilla de un 30 %.

Estamos entrando en la era del conocimiento pero la mayoría de las Instituciones, tanto públicas como privadas, no tienen sistemas de gestión orientados a enjuiciarla. Los sistemas de gestión de créditos, basados en estadísticas de la era industrial, no tienen por que ser los mismo en la era del conocimiento. De hecho, muchos de los nuevos productos en el área de los servicios financieros y de seguros no son otra cosa que el reconocimiento de que las cosas están cambiando y que si anticipamos nuestra oferta a la demanda, somos capaces de posicionarnos en un mercado que, no por no existir en la actualidad, deja de tener mejor cariz para el futuro.

Dejemos de ver el pendiente en la oreja de nuestro Director Técnico y analicemos sus verdaderos conocimientos y su capacidad de transportarnos al futuro. Que la Santa Nómina no sea el único medio de conseguir financiación y que las Grandes Empresas e Instituciones Financieras apuesten algo por el futuro. Es descorazonador ver las cantidades que se invierten en industrias sin salida y, en proporción, lo poco que invertimos en el futuro de nuestros hijos.

Comercio electrónico

Arquitectura para el Comercio Electrónico

Manuel Medina*, Francisco Jordán**, Jordi Buch***

Director de cANet y esCERT-UPC, Profesor UPC**, Director Técnico de esCERT****

medina@ac.upc.es
jordan@ac.upc.es
escert@escert.upc.es

Resumen: *Se pretende dar una visión general de las estrategias que el Comercio Electrónico (CE) ofrece a las empresas, para mejorar sus oportunidades de negocio y el rendimiento de los servicios administrativos, de promoción y ventas. Sin entrar en detalles de cómo el comercio electrónico debe implantarse en la empresa, se relacionan los aspectos que se deben tener en cuenta a la hora de planificar su implantación en la empresa. Se analizan el entorno de aplicación SET y los riesgos que se deben evitar en su integración con los servicios informáticos de la empresa.*

1. Introducción

La diferencia fundamental entre un sistema de información y un servicio de Comercio Electrónico radica en la palabra "valor", es decir que la información transmitida por las redes de ordenadores debe tener un "valor" determinado, que se compensará de alguna forma por mecanismos paralelos (transferencia de fondos, cupones electrónicos, cargos en cuentas de crédito/débito, etc.).

Distinguimos dos tipos de relaciones de comercio electrónico:
· Intercambio electrónico de datos (**EDI**) entre ordenadores, o mejor dicho, entre aplicaciones informáticas.
· Acceso remoto de individuos a las aplicaciones de gestión de ventas/facturación/post-venta de empresas comerciales o de la administración.

En ambos casos la codificación de la información es importante, pero especialmente en el primero, pues de ella depende la simplicidad de las aplicaciones que deben interpretar los datos transmitidos en los mensajes EDI. En el caso de individuos accediendo a aplicaciones remotas de CE, en cambio, el aspecto más importante es el interfaz de usuario y su carácter amigable. En este sentido **JAVA** constituye una herramienta muy esperanzadora.

2. Modelos de Comercio Electrónico

2.1. Modelo Arquitectónico

En la **figura 1** se distinguen los tres casos que hemos denominado como el "núcleo del Comercio Electrónico". Cada uno de ellos puede establecer distintos entornos de trabajo, según el tipo de producto "negociado" y según las fases del ciclo de negocio a las que se aplique el CE.

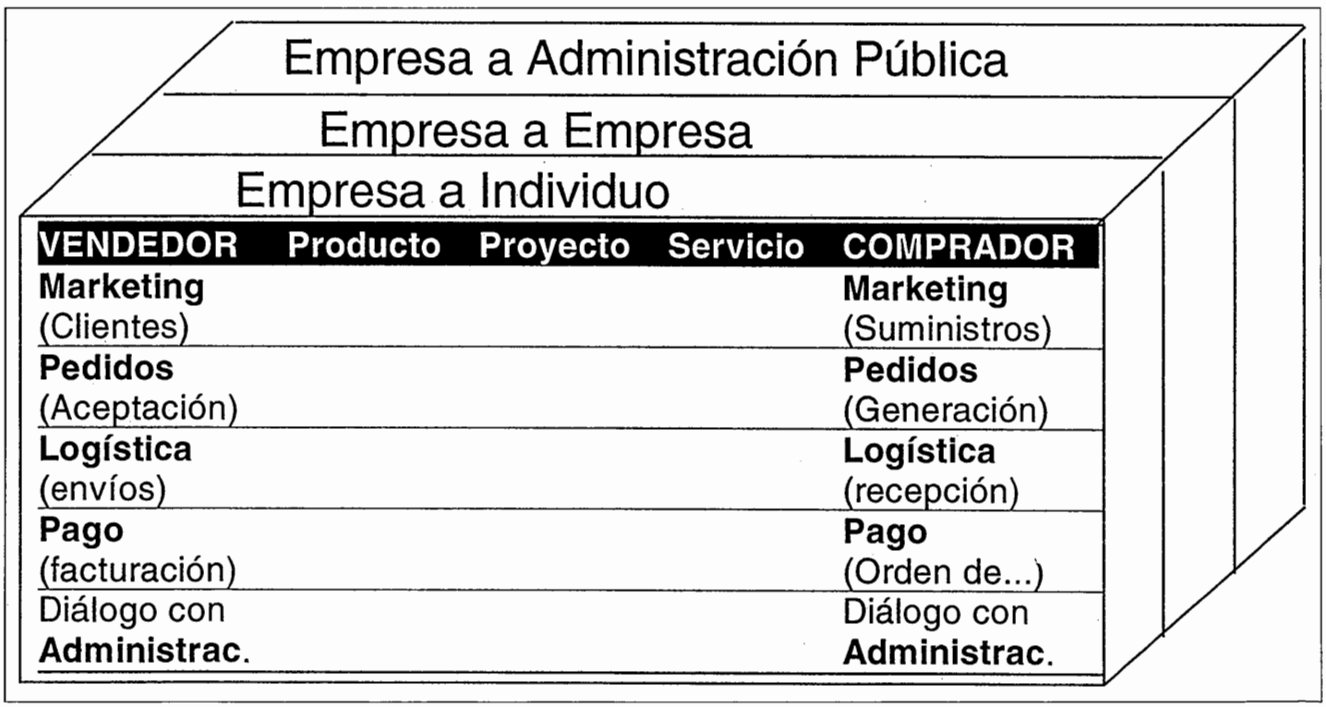


Figura 1: Matriz del negocio

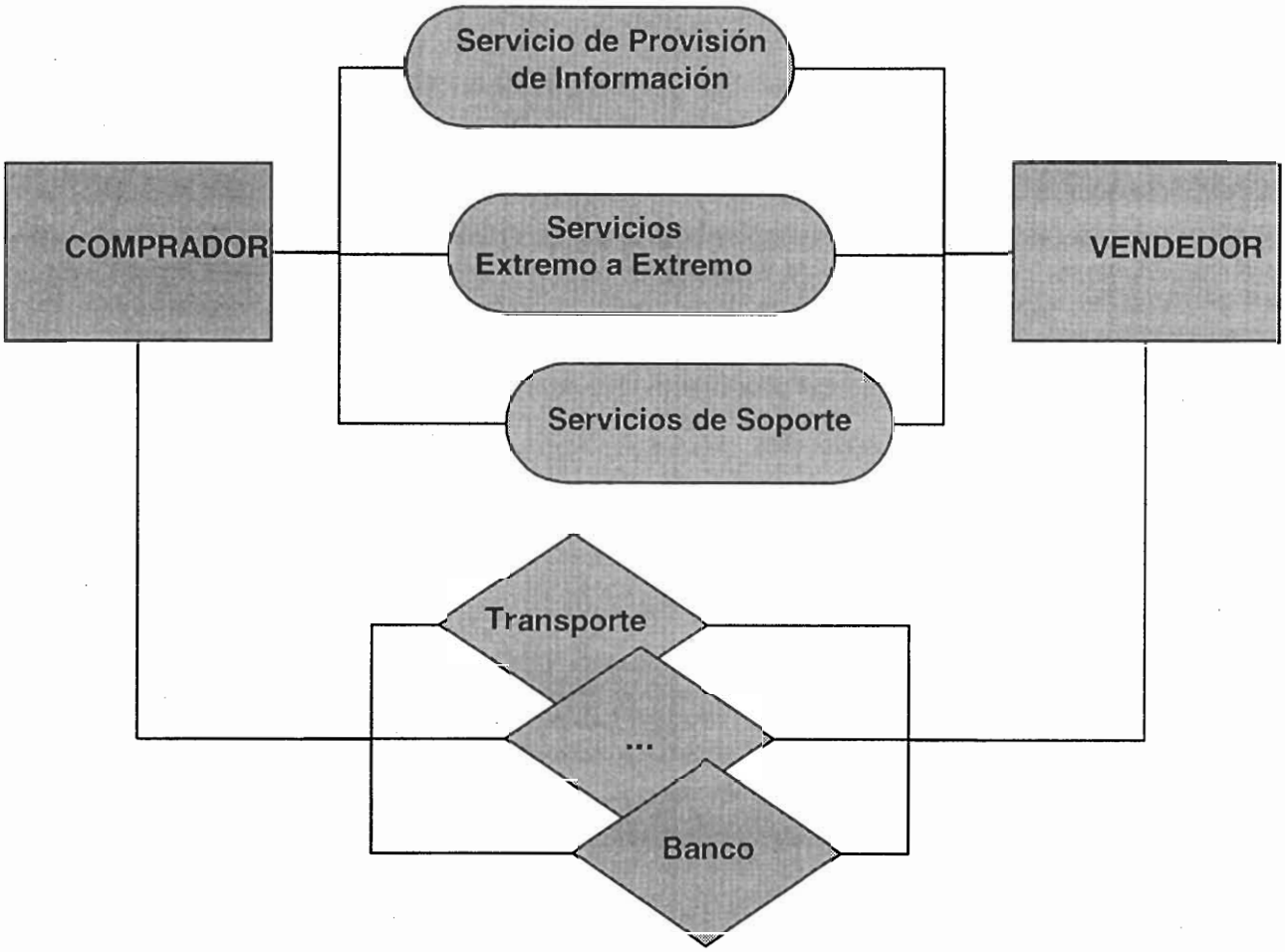


Figura 2: Modelo general de negocio

Un aspecto del ciclo de negocio no mencionado es el servicio post-venta. La razón es que no deja de ser un producto (servicio) que se debe promocionar (Marketing), contratar (Pedidos), servir (Logística), pagar, etc. como cualquier otro producto.

Cuando el comercio electrónico es algo más complicado que pedir un libro o unas imágenes por WWW, la relación entre comprador y vendedor se también complica, y en el modelo de su interrelación **(figura 2)** aparecen unos agentes intermedios, que facilitan el intercambio de información (óvalos):

· Servicios de provisión de información: Diseminación, Búsqueda, Producción, Indexación y clasificación, etc.

· Servicios de comunicación entre las partes: Gestión de transacciones EDI (centros de compensación), comunicación inter-personal (e-mail, conferencias electrónicas, trabajo en grupo), etc.

- Servicios de soporte: Directorio (X.500), gestión de claves de cifrado y certificados, servicios de seguridad, servicios de inter-operabilidad (pasarelas, traductores de sintaxis, convertidores de protocolos, etc.)

Cada tipo de intermediario tiene unas responsabilidades (roles, papeles) en el modelo de comercio electrónico, y en consecuencia estará preparado para procesar unos tipos de mensajes concretos.

2.2. Modelos de escenario de comercio electrónico

En la **figura 3** se muestran algunos ejemplos de mensajes que se pueden intercambiar comprador y vendedor a través de los intermediarios correspondientes:

· Anuncios e información de promoción a través de servidores de alquiler de páginas de información o *brokers*.

· Catálogos, listas de precios y descripciones de productos a través de servicios de distribución electrónica de catálogos.

· Pedidos y facturas a través de servicios de comunicación inter-personal o de trabajo en grupo, incluyendo o no

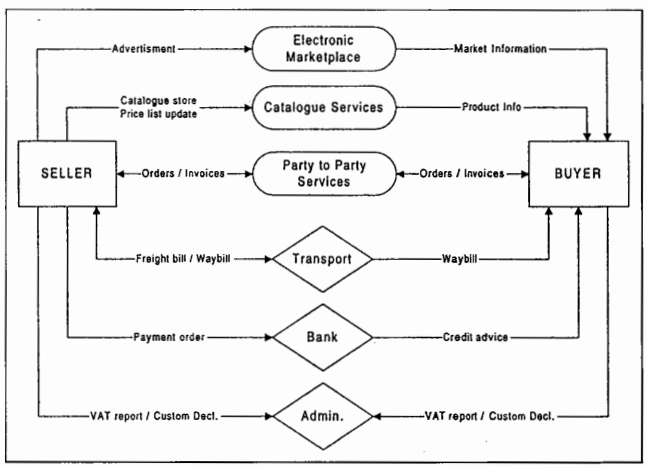


Figura 3: Relaciones entre intermediarios

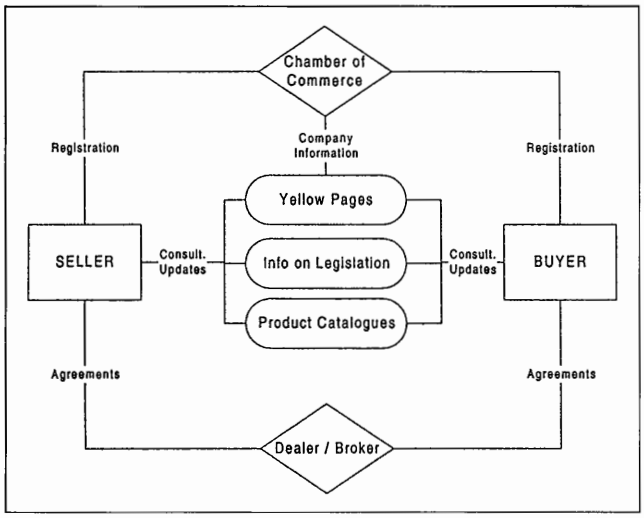


Figura 4: Modelo de marketing

servicios de transacciones seguras, dependiendo del valor de la transacción y de los mecanismos paralelos (no estrictamente electrónicos, como fax o teléfono) empleados para confirmar la transacción.

· Albaranes para los transportistas.

· Ordenes de pago y notificaciones de abonos para/de los bancos.

· Liquidaciones de IVA o declaraciones de Aduanas para la Administración.

En la **figura 4** podemos ver un escenario en el que se ilustra un modelo de Marketing a través de Comercio Electrónico puede implicar a agentes tradicionales, como las Cámaras de Comercio[1], encargadas de registrar a las empresas "reconocidas legalmente" en el sector correspondiente, lo cual permite a comprador y vendedor reconocerse mútuamente capacidad legal para negociar.

Pero también intervienen agentes nuevos, como las páginas amarillas o servicios de distribución de documentación comercial o legal, que en el fondo significan una traducción al mundo electrónico de servicios ya conocidos en el comercio tradicional.

Otros agentes, como el distribuidor o el *broker*, adquieren una perspectiva completamente distinta, pues, aunque realizan funciones similares a sus homónimos del comercio convencional, su forma puede ser completamente distinta. Pensemos por ejemplo la diferencia entre un banco o agente de seguros tradicional, con agencias o delegaciones distribuidos por su "territorio" y otros que sólo actúen telefónicamente (o electrónicamente a través de redes de datos).

En este último caso la ubicación física de la empresa no tiene ninguna importancia y por supuesto tampoco la decoración de la oficina, mostradores, vitrinas, etc., que ni siquiera existirán. Pero la diferencia puede ir más allá incluso, pues pueden no tener ni siquiera almacenes de productos, y "distribuir" directamente desde el fabricante al cliente, con lo que la reducción de costes de infraestructura e inmovilizado se reducen drásticamente.

3. Seguridad en el Comercio Electrónico

La toma de consciencia de las ventajas del comercio electrónico seguro está consiguiendo la proliferación de elementos de seguridad para las aplicaciones de Comercio Electrónico:

· Las **Autoridades de Registro (RA) y Acreditación (CA)**: permiten reconocer de forma unívoca y segura a nuestros interlocutores, empleándolas como terceras partes fiables en caso de litigio, pues podrían certificar la autenticidad de una firma electrónica sobre un mensaje o documento de comercio electrónico. La CA también mantiene las listas de revocación de certificados para resolver los casos de robo, pérdida o suspensión de identificadores digitales. La seguridad de la CA es crítica; un problema de seguridad que afecte a la CA puede afectar a toda la infraestructura existente.

· **Directorio.** El directorio es la base de datos donde se publican los certificados. De esta forma, los certificados están disponibles para todo el mundo. En el directorio, además se guardan otros datos como la dirección de correo electrónico, empresa del usuario, etc. La última generación de navegadores ya incorporan mecanismos automatizados de búsqueda en el directorio.

· **El servidor alquilado:** ofrece la oportunidad de distribuir información sobre una empresa, sin necesidad de dotar a ésta de medios de comunicación avanzados, para hacerla accesible a través de las redes de datos. Pero sobre todo la ventaja es que no expone los ordenadores de la empresa a ataques informáticos desde el exterior de la empresa, que, aunque constituyen un porcentaje relativamente bajo de los ataques sufridos por empresas en sus instalaciones informáticas (20%), no se debe despreciar. Evidentemente, hay que considerar también la seguridad del servidor alquilado, pues al estar fuera de nuestro control directo, también nos costaría más detectar un ataque a nuestra información en él almacenada.

· **La acreditación de servidores y usuarios:** permite evitar problemas de intrusismo al acceder a información mínimamente sensible, mediante el uso de sistemas de cifrado de clave pública, acreditados por alguna CA. La acreditación del servidor permite al usuario tener la certeza de que sus credenciales y peticiones van realmente al servidor que él espera. La acreditación del usuario permite proteger la información confidencial almacenada en el servidor, y mantener un registro de los accesos realizados, pero sobre todo simplifica enormemente la gestión del control de acceso de usuarios (passwords, contraseñas desechables, gestión de privilegios de acceso, etc.).

· **Las terceras partes fiables (TTP)** y los centros de compensación: ofrecen mecanismos de trazado de los intercambios, para demostrar su realización en caso de litigio.

4. Acuerdo de Intercambio

La transferencia de información entre comprador y vendedor requiere una compatibilidad, no sólo de intereses económicos, sino también de los protocolos de comunicación empleados para transferir la información, desde distintos puntos de vista. Actualmente *http* y S/MIME se están consolidando como las normas *de facto*, pero no debemos olvidar las alternativas:

1. Sintaxis de la transferencia de mensajes

· UN/EDIFACT: ISO (Organización Internacional de Normalización), auspiciada por las Naciones Unidas, ha desarrollado una norma para el intercambio de mensajes correspondientes a documentos comerciales tradicionales (ISO-9735).
· ANSI (Instituto de normalización Nacional Estadounidense) por su parte ha definido otra norma, que se emplea sobre todo en USA y sud-este asiático.

2. Protocolo de transferencia de intercambios

· X.400 es el mecanismo de transferencia de mensajes recomendado por la Administración, aunque la reciente admisión de normas disponibles públicamente hace pensar que el correo electrónico de Internet desbancará también en este sector a X.400.

· Transferencia de ficheros. Hay dos protocolos normalizados para realizar la transferencia electrónicamente: FTAM de ISO y FTP de Internet.
· S/MIME Correo electrónico con énfasis en la seguridad o PGP, que enfatiza la "privacidad". Ambos permiten transmitir documentos con seguridad. Se supone que S/MIME desplazará a todos los otros.
· http y https, utilizados por las aplicaciones WWW. Se está trabajando para que admitan el intercambio y la codificación de mensajes comerciales normalizados.

5. Arquitectura SET

Con la ayuda de los grandes fabricantes de la industria de ordenadores y programas, Visa y MasterCard han desarrollado el que se está erigiendo en el protocolo de pago por excelencia para la práctica del Comercio Electrónico minorista (es decir, venta entre comerciante y usuario final). **SET** (*Secure Electronic Transaction*) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito[2].

Como método de pago basado en tarjeta, la solución SET (**figura 5**) conlleva la presencia de 3 nuevas entidades aparte de los sistemas tradicionales ya utilizados en la actualidad. Los nuevos componentes son:

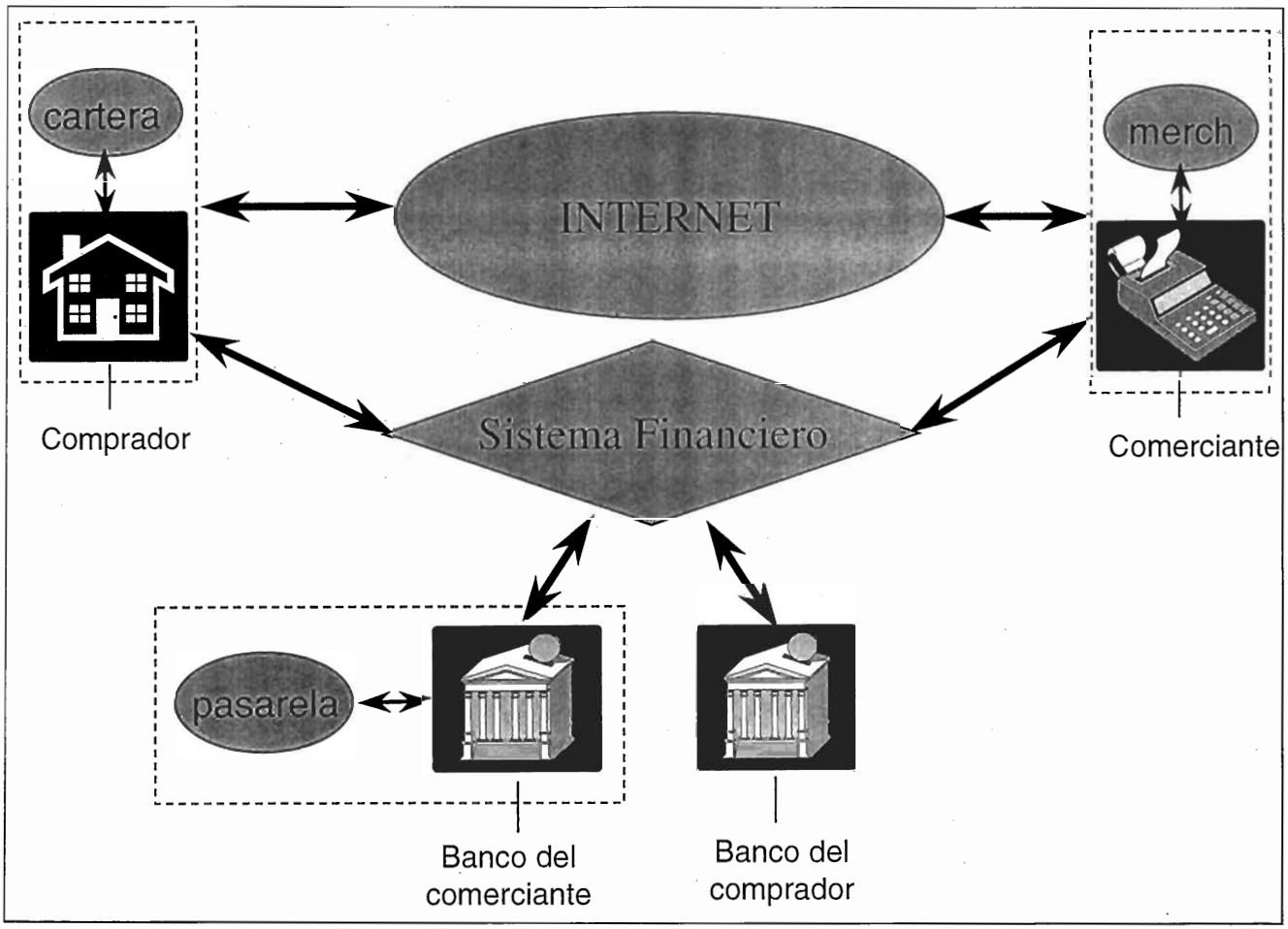


Figura 5: Solución SET

- **Cliente.** El cliente es quien inicia la transacción. Éste se identifica al comerciante y entidad financiera mediante la firma digital, y se verifica la identidad de éste mediante el correspondiente certificado emitido por una CA reconocida. Estas funciones se realizan mediante la entidad *Cardholder* **SET** o Titular SET la cual se encarga de actuar en nombre del titular de la tarjeta virtual, para realizar el pago. Habitualmente a esta entidad se le conoce como *Wallet* o **Cartera**, ya que su funcionalidad es muy similar a una cartera en la cual se almacenan las tarjetas.

- **Comerciante.** Se identifica ante el cliente y el banco o entidad financiera. Verifica la autenticidad del cliente para asociarle datos económicos. En el protocolo SET, el comerciante no tiene acceso al número de tarjeta de crédito del cliente. La entidad *Merchant* **SET** o Comerciante SET es la encargada de gestionar el pago del bien o servicio adquirido por un comprador. El pago siempre lleva asociado una transacción con un aceptador (*acquirer*) para la autorización del importe a pagar por el comprador. Habitualmente a esta entidad se le denomina **POS** (*Point Of Sale*) o **TPV** (Terminal Punto de Venta) virtual ya que su comportamiento, entre otras funciones, simula el de los sistemas tradicionales.

- **Administrador del comercio.** Mantiene los catálogos del comercio y realiza las actividades de gestión propias del comercio como recibir pedidos, datos de *stock*, etc. El mantenimiento puede realizarse de forma local o remota.

- **Banco o entidad financiera.** Recibe las autorizaciones de pago del cliente a través del comerciante. El banco consulta al emisor de tarjetas (aceptador) para obtener la autorización firmada de la transacción. La entidad *Gateway* **SET** o Pasarela SET es la encargada de hacer esta función de puente entre el sistema aceptador SET y el sistema financiero propietario ya existente. Esta entidad es muy importante en cuanto supone la conexión de los sistemas y redes de autorización privados existentes con el mundo de Internet. En el sistema SET la seguridad en las transacciones se ha cuidado hasta el último detalle. El sistema utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet.

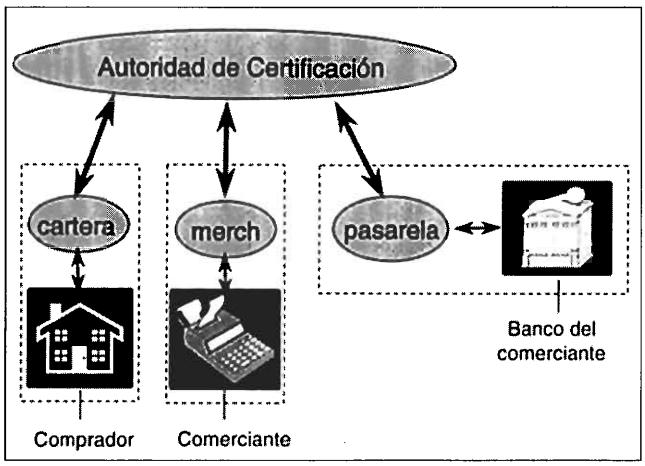


Figura 6: Autoridad de certificación SET

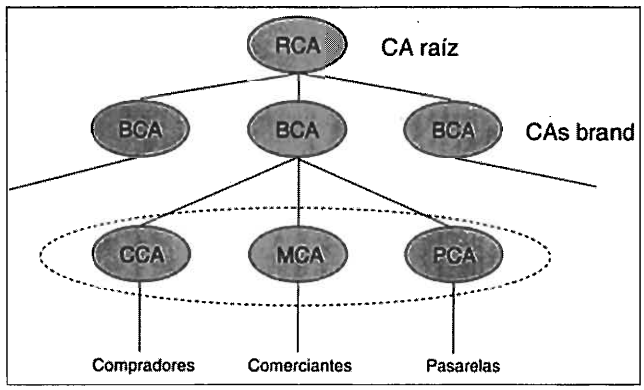


Figura 7: Jerarquía de certificación SET

Todas las entidades implicadas en el SET deben estar en posesión de un certificado válido para poder intervenir en una transacción de pago. Esto quiere decir que tanto titulares, comerciantes y pasarelas SET deben de ser identificadas previamente y proveerles de un certificado para que puedan funcionar dentro del sistema. Actualmente, los navegadores más populares ya permiten el uso de esta tecnología. Este hecho supone una importante disminución de la barrera de entrada tradicionalmente presente en el comercio electrónico. Sin embargo, el marco no se completará hasta que los lectores de tarjetas inteligentes se popularicen y se integren plenamente en los productos existentes.

Las entidades que generan los certificados para las entidades SET participantes se denominan **CA SET** o Autoridades de Certificación SET y generalmente son operadas por instituciones financieras capaces de emitir tarjetas (emisores) o instituciones asociadas, como bancos, que solicitan la emisión de tarjetas.

Las **Autoridades de Certificación** siempre están asociadas a una Marca de tarjeta particular. Esto quiere decir que los certificados de todas las entidades sólo son válidos para una Marca determinada siendo imposible utilizarlo en otro ámbito (al igual que en los sistemas tradicionales, es imposible utilizar una tarjeta Visa como si fuera una MasterCard). De lo que se desprende que una entidad deberá estar en posesión de tantos certificados como Marcas diferentes utilice (de ahí la acepción cartera para referirse a la entidad SET de titulares). Esto por otra parte hace muy flexible el sistema, lo que, como se verá a continuación, nos permitirá utilizarlo dentro del ámbito de Marcas privadas.

Por último mencionar que existen varios tipos de Autoridades de Certificación SET dependiendo de su función y a quien certifiquen.

Las **Autoridades de Certificación** SET están organizadas jerárquicamente existiendo una única raíz operada por una compañía denominada **CertCo** localizada en Estados Unidos. La raíz a su vez certifica las **Autoridades de Marca**[3] **(BCA)** como Visa o MasterCard que a su vez certifican las Autoridades usuarios compradores, comerciantes y pasarelas de pago.

6. Conclusiones

La existencia de problemas de seguridad en Internet es un hecho, sin embargo no es prudente descartar dicha red por esta simple razón. Internet es más segura que otros medios y las dudas y temores que aparecen no son sino producto de la resistencia al cambio.

¿Acaso el remitente que aparece en el correo postal es inmanipulable? ¿Acaso un delincuente no puede comprar con una tarjeta de crédito robada? ¿No es relativamente fácil la falsificación de firmas?

Con la firma digital, y el uso de tarjetas inteligentes, estos problemas quedan más que resueltos, el resto queda en manos de los responsables de seguridad para que nos garanticen la disponibilidad de acceso en los sistemas y que nos encontremos allí lo que esperamos encontrar.

Es simplemente cuestión de tiempo. Si bien la tecnología disponible ya permite el establecimiento del comercio electrónico con los requerimientos de seguridad mínimos, cabrá esperar a corto plazo una considerable mejora de la disponibilidad de ésta para todas las partes -las tecnologías de seguridad exigen a los clientes la disponibililidad de unos recursos considerables como actualización de soft, soporte de hard adecuado, etc.

El problema de la disponibilidad de los lectores de tarjetas inteligentes que permitan el uso seguro de la información económica asociada al cliente desde cualquier localización física es urgente.

7. Documentación

7.1. Comercio Electrónico

Más de 20.000 compradores en un día visitaron la *companion World Cup boutique* del reciente Mundial de Francia (*http://store.france98.com*), donde se ofrecieron más de 400 productos. Se aceptaron pagos en una docena de monedas y se distribuyeron productos a más de 54 países. Los 30 millones de *hits* registrados se tradujeron en cerca de 1 millón de compradores.

European Initiative of Electronic Commerce **COM** (97)157), *http://www.ispo.cec.be/Ecommerce*

Bonn Conference on Electronic Commerce, *http://www.echo.lu/bonn/conference.html*

EPHOS Electronic Commerce

EWOS ETG066 - ***Technical Guide on Electronic Commerce Law model for Electronic Commerce,*** *http://www.un.or.at/uncitral/index.html*

DEDICA, *http://www.ac.upc.es/ DEDICA/*

Good Practice Guidelines on Open Access to Electronic Commerce for European SMEs, *http://www.ispo.cec.be/Ecommerce/MoU/glines3.htm*

Comercio Electrónico Global, *http://www.geocities.com/CapeCanaveral/Lab/9964/*

G8: Global Markeplace for SMEs: International Testbeds for Electronic Commerce, *http://www.ispo.cec.be/Ecommerce/g7init.htm*; *http://nii.nist.gov/g7/10_global _mp/testbeds/registered.html*

7.2. Seguridad

Importantes fuentes de información sobre **SSL, SET** y **S/MIME** están disponibles en los servidores de información de **Netscape** (*http://www.netscape.com*), **RSA** (*http://www.rsa.com*), **VISA** (*http://www. visa.com*).

Se puede consultar información sobre autoridades de certificación en **Verisign** (*http://www.verisign.com*), es**CERT-CC** (*http://ca.upc.es/demo*) o en el servidor de **ICE-TEL** (*http://www.darmstadt.gmd.de/ice-tel*).

Autoridad de Certificación IPS, *http://www.ips.es*

Autoridad de Certificación UPC, *http://ca.upc.es*

Servicios de seguridad esCERT, *http://escert.upc.es*

IFIP TC11, *http://ifip.or.at/ - http://www.cs.purdue.edu/homes/spaf/ifip11.4*

7.3. Infraestructuras públicas de Autoridad de Certificación en Europa

EDIFACT: DEDICA, *http://www.ac.upc.es/ DEDICA/*

e-mail: **BelSign,** *http://www.belsign.be*

Web-sites: EuroTrust, *http://www.baltimore.ie/eurotrust/pi_contents.html*

7.4. Firma Digital

Summary of legislation: **USA & others,** *http://www.mbc.com/ds_sum.html*

EU Comission: Digital Signature, (COM(97)503 final 1997/10/08), *http://www.mbc.com*

International Hearing (Copenhagen 1998-04-23), *http://www.fsk.dk/fsk/div/hearing/*

ITU-T: X.509 v3: ***The Directory,*** *ftp://ftp.bull.com/pub/OSIdirectory/ITU*

8. Notas

[1] *EuroChambers* está poniendo en marcha un piloto para su constitución como entidad "aval" de la calidad de los certificados emitidos por sus socios participantes (ej. Consejo Superior de Cámaras de Comercio Españolas).

[2] Inicialmente sólo se pensó en tarjetas de crédito dada la naturaleza de sus patrocinadores, sin embargo posteriormente también se ha introducido el uso de tarjeta de débito.

[3] En España existe una raíz para las marcas privadas de tarjetas SET, avalada por **FESTE** (Fundación para el Estudio de la Seguridad en las Telecomunicaciones), patrocinada por **SET-*Projects*** y operada por **esCERT-UPC**.

Criptología

Xavier Ribas
Ribas & Rodríguez

Esquema de la propuesta de Directiva sobre firmas electrónicas

Preceptos más significativos

Texto de la propuesta de Directiva

Efectos legales de las firmas electrónicas

Artículo 3.- Efectos legales

1. Los Estados Miembros deberán asegurar que, con respecto a los datos autentificados por medio de una firma electrónica suministrada por un proveedor de servicios de certificación, que cumple los requisitos establecidos en esta Directiva, existe la presunción legal de que:

(a) los datos no han sido alterados desde el momento en que la firma electrónica fue añadida a ellos;
(b) la firma electrónica pertenece efectivamente a la persona que realizó la firma digital; y
(c) la firma electrónica fue añadida por dicha persona con la intención de firmar los datos

Esquema y Comentarios

1. Presunciones legales

En este precepto se recogen los principios establecidos tradicionalmente por la doctrina respecto a los fundamentos jurídicos que deben regir una transacción de comercio electrónico.

La necesidad de establecer presunciones legales respecto a la integridad y autenticidad de una operación electrónica en la que se funden las voluntades contractuales de ambas partes resulta fundamental para otorgar seguridad jurídica al negocio realizado y al tráfico mercantil o de consumo que tenga lugar en el nuevo entorno generado por las redes telemáticas.

El principio de INTEGRIDAD queda recogido en la presunción de que los datos no han sido alterados desde el momento en que la firma electrónica fue añadida a ellos. Ello garantiza que los elementos básicos del negocio, como el precio, la cantidad y las característica de lo contratado, entre otros, se considerarán válidos salvo que la parte en desacuerdo demuestre que efectivamente han sido alterados o se han incumplido las normas de seguridad establecidas para garantizar la integridad de la información.

El principio de AUTENTICIDAD se integra en la presunción de que la firma electrónica pertenece efectivamente a la persona que realizó la firma digital. Esta garantía es necesaria para dar a cada parte la certeza de que la otra es realmente quien dice ser. La base técnica de esta presunción se encuentra en el desarrollo de protocolos de seguridad como la especificación SET que permitan la generación y el tratamiento de firmas digitales. Esta garantía está asociada a las normas de custodia de las claves y certificados de cada parte, penalizando un uso o tenencia negligente de los elementos de seguridad que participan en la autentificación de los intervinientes. La carga de la prueba corresponderá a la parte que niegue su intervención en el negocio.

El principio de NO REPUDIO se encuentra recogido en la presunción de que la firma electrónica fue añadida por dicha persona con la intención de firmar los datos y que, por lo tanto, dió su pleno consentimiento al contenido de la transacción. Ello significa que las partes intervinientes no podrán rechazar las obligaciones contractuales derivadas del negocio llevado a cabo, salvo en el caso de que demuestren que concurre algún vicio del consentimiento previsto en la legislación nacional, o cualquier otra prueba que desvirtúe la presunción. En las transacciones de consumo siempre quedará a salvo el derecho al desistimiento en el plazo de siete días, o «repudio jurídico», previsto en la Directiva de Venta a Distancia y en la correspondientes legislaciones nacionales.

2. Los Estados Miembros deberán asegurar que los datos a los que una firma electrónica es añadida, y que está basada en un certificado calificado válido suministrado por un proveedor de servicios de certificación, de acuerdo con los requisitos establecidos en esta Directiva, cumple con los requisitos de forma legal de la misma manera que si los datos hubiesen existido en un documento firmado manualmente.

2. Asimilación de la firma electrónica a la convencional

La actual doctrina del Tribunal Supremo español sostiene que la firma autógrafa no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que asimismo conceden autoría y obligan. Así, las claves, los códigos, los signos y, en casos, los sellos con firmas en el sentido indicado. Y, por otra parte, la firma es un elemento muy importante del documento, pero, a veces, no esencial, en cuanto existen documentos sin firma que tienen valor probatorio (como son los asientos, registros, papeles domésticos y libros de los comerciantes). En consecuencia, aunque, al igual que en el caso de los documentos comunes, puede haber documentos electrónicos sin firma, el documento electrónico (y, en especial, el documento electrónico con función de giro mercantil) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido. Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de los ordenadores o procesadores y se garantiza, con las pruebas periciales en su caso necesarias, la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil en soporte informático, con función de giro, debe gozar de plena virtualidad jurídica operativa.En este sentido, es importante conseguir que la asimilación de la firma electrónica a la firma convencional, existente ya en la jurisprudencia española, adquiera rango de ley en el momento de la trasposición de la Directiva propuesta en este texto de la Comisión Europea.

3. Los Estados Miembros deberán asegurar que los datos a los que una firma electrónica es añadida, y que está basada en un certificado calificado válido suministrado por un proveedor de servicios de certificación, que cumple los requisitos establecidos en esta Directiva, puede ser utilizada como prueba en un juicio

3. Valor probatorio

La legislación española ha previsto, en distintas normas, la validez del documento electrónico y de las comunicaciones telemáticas como prueba documental. (Véase una selección de dichas normas en *http://www.onnet.es/08020001.htm*). Asimismo, la jurisprudencia ha reconocido que, a efectos probatorios, ha de entenderse por documento el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un diskette, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como "cualquier cosa que sirve para ilustrar o comprobar algo" (se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el aplicador del derecho tener en cuenta la evolución social), siempre que el llamado 'documento' tenga un soporte material, que es lo que sin duda exige la norma penal. En la actualidad dicha fórmula jurisprudencial tiene adecuada correspondencia en la norma contenida en el artículo 26 del nuevo Código Penal, según el cual "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

Sin embargo, es importante que la ley establezca directamente la fuerza probatoria en juicio de un documento firmado electrónicamente y, en este sentido, debe reconocerse la importacia de este apartado en la propuesta de Directiva sobre firmas electrónicas.

4. Los Estados Miembros deberán asegurar que, sin perjuicio de la legislación nacional relativa a los documentos firmados bajo coacción, mala fe, fuerza o engaño, las presunciones del párrafo 1 pueden ser rebatidas mediante prueba que indique que el procedimiento de seguridad, incluyendo los productos, utilizado para verificar la firma electrónica, no puede ser reconocido técnicamente como seguro.

4. Prueba en contrario

Es lógico que, en aras a la seguridad del tráfico mercantil, se introduzcan presunciones legales a favor de la integridad, autenticidad y validez de las transacciones electrónicas, pero también es lógico que dichas presunciones sean *iuris tantum*, es decir, admitan una prueba en contrario, puesto que el consentimiento puede estar viciado y los datos pueden haber sido objeto de una manipulación no autorizada. El principio de integridad asigna la carga de la prueba a la parte que mantenga que los datos han sido alterados, demostrando la insuficiencia del procedimiento de seguridad empleado.

5. Los Estados Miembros pueden someter los efectos legales, la validez o la fuerza ejecutiva de las firmas electrónicas en los casos regulados por el derecho público, a requisitos adicionales.

5. Relaciones con las Administraciones Públicas

Una vez creado un entorno seguro en el que las autoridades de certificación, los protocolos de seguridad empleados y las presunciones legales establecidas garanticen los principios de integridad, autenticidad, confidencialidad, no repudio y fuerza probatoria de los datos firmados electrónicamente, no deberían existir diferencias entre los requisitos de seguridad establecidos para una transacción electrónica sometida al derecho privado y una transacción electrónica sometida al derecho público. Si las autoridades de certificación cumplen los requisitos establecidos en la Directiva propuesta, los efectos legales, la validez o la fuerza ejecutiva de las firmas electrónicas y de los datos asociados a las mismas no deberían estar sometidos a requisitos adicionales que entorpeciesen las relaciones de los ciudadanos con las administraciones públicas.

6. Los Estados Miembros no limitarán la libertad contractual de las partes para acordar entre ellas los términos y condiciones bajo los que aceptarán datos firmados electrónicamente.

6. Autonomía de la voluntad en los contratos

El principio de libertad contractual y de autonomía de la voluntad de las partes que intervienen en un negocio debe quedar siempre garantizada, sin que pueda ser limitada por normas que impidan concretar las condiciones bajo las que aceptarán datos firmados electrónicamente. En entornos de banca telefónica y banca electrónica, por ejemplo, es habitual establecer cláusulas específicas respecto a la validez de los asientos generados por el usuario o la entidad financiera utilizando medios y soportes diferentes al papel ya la firma autógrafa. Aunque dichos pactos no deberían ser necesarios una vez hayan entrado en vigor las leyes de trasposición de la Directiva propuesta, es importante que se mantenga la libertad contractual de las partes.

Finalmente, se tendrán en cuenta las normas derivadas de la Directiva de Cláusulas Abusivas en las operaciones de consumo.

7. Confidencialidad de la información

Se echa en falta, en el texto propuesto, una mención al principio de CONFIDENCIALIDAD que debe regir en cualquier transacción electrónica y ampliamente discutido a raíz del desarrollo y la implementación de la especificación SET. De acuerdo con este principio, debería existir un apartado con el siguiente texto: "Los Estados Miembros deberán asegurar que los sistemas y procedimientos de seguridad y cifrado utilizados garantizarán la confidencialidad de los datos a los que una firma electrónica es añadida".

3. Los Estados Miembros deberán asegurar que, no obstante el párrafo 1, un proveedor de servicios de certificación no es responsable si puede demostrar que ha adoptado todas las medidas razonablemente aplicables para evitar errores en un certificado cualificado.

4. Los Estados Miembros deberán asegurar que, no obstante el párrafo 1, un proveedor de servicios de certificación puede, en el certificado cualificado, limitar el uso del certificado. El proveedor de servicios de certificación no será considerado responsable de los daños ocasionados por un uso contrario del certificado.

5. Los Estados Miembros deberán asegurar que , no obstante al párrafo 1, un proveedor de servicios de certificación puede, en el certificado cualificado, limitar el valor de las trasacciones para las que el certificado es válido. El proveedor de servicios de certificación no será considerado responsable de los daños que exceden dicha limitación del valor.

6. Los Estados Miembros deberán asegurar que, no obstante el párrafo 1, un proveedor de servicios de certificación puede, en el certificado cualificado, limitar su responsabilidad a una cantidad específica por certificado.

Aspectos internacionales

Artículo 7.- Aspectos internacionales

1. Los Estados Miembros deberán asegurar que los certificados emitidos por un proveedor de servicios de certificación de un tercer país son reconocidos como legalmente equivalentes a los certificados emitidos por proveedores de servicios de certificación que operan bajo esta Directiva:
(a) si el proveedor de servicios de certificación tiene una autorización de un Estado Miembro de la Unión Europea; o
(b) si el certificado es reconocido por un proveedor de servicios de certificación que opera bajo esta Directiva, y que el proveedor de servicios de certificación garantiza el certificado, con el mismo alcance que sus propios certificados;
(c) si el certificado es reconocido bajo el régimen de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

2. La Comisión tomará todas las medidas necesarias para facilitar los servicios de certificación transfronterizos con terceros países. Con este propósito, la Comisión hará propuestas para llevar a cabo todas las acciones necesarias para conseguir la efectiva implementación de acuerdos internacionales aplicables a los servicios de certificación, y en particular, cuando sea necesario, remitirá propuestas al Consejo para la negociación de acuerdos bilaterales y multilaterales, incluyendo los derechos de organizaciones de la Comunidad, con terceros países y organizaciones internacionales. El Consejo decidirá por mayoría cualificada.

3. Supuesto de exoneración

Adopción de las medidas razonablemente aplicables

4. Limitación de uso

Exoneración de responsabilidad en casos de uso contrario a lo establecido

5. Limitación de la cuantía de las transacciones

Exoneración de responsabilidad en el caso de exceso

6. Limitación cuantitativa de responsabilidad

Posibilidad de fijación de una cantidad máxima

1. Equivalencia de certificados de terceros países

a. Autorización
b. Reconocimiento por CSP comunitario
c. Reconcimiento por tratado

2. Servicios de certificación transfronterizos

Medidas y propuestas para facilitarlos

Protección de datos

Artículo 8.- Protección de datos

1. Los Estados Miembros deberán asegurar que los proveedores de servicios de certificación y los cuerpos nacionales de acreditación cumplan con los requisitos establecidos en las normas nacionales que implementan las Directivas 95/46/CE y 97/66/CE.

2. Los Estados Miembros debrán asegurar que un proveedor de servicios de certificación sólo pueda recoger datos personales directamente del afectado y sólo hasta donde sea necesario para la finalidad de emitir un certificado. Los datos no pueden ser procesados con otros propósitos

3. Los Estados Miembros deberán asegurar que, a solicitud del firmante, el proveedor de servicios de certificación indique un seudónimo en vez del nombre del firmante en el certificado.

4. Los Estados Miembros deberán asegurar que en el caso de personas que utilicen seudónimos, el proveedor de servicios de información transmitirá los datos relativos a la identidad de dichas personas a las autoridades públicas que lo requieran con el consentimiento del afectado. Cuando el consentimiento no pueda ser obtenido porque la transferencia de los datos que revelan la identidad del afectado sea necesaria para la investigación de delitos criminales graves, la transferencia se conservará y el afectado será informado de la transferencia de los sus datos tan pronto como sea posible después de que la investigación haya sido completada.

Nota

El texto de la propuesta de Directiva ha sido traducido y comentado por Xavier Ribas a partir de su original en inglés. No se trata por lo tanto de un texto oficial.

1. Cumplimiento de los requisitos establecidos en las normas de protección de datos
2. Recogida de los datos directamente del afectado
3. Utilización de seudónimos
4. Comunicación de la identidad del usuario de un seudónimo exclusivamente:

- Con consentimiento del afectado
- En el contexto de un procedimiento judicial por delito grave

Comercio electrónico

El comercio electrónico entre empresas

Francisco J. Ruiz

Telefónica I+D

1. Introducción

Durante los últimos tiempos el comercio electrónico se ve como una nueva revolución, revolución que lleva gestándose desde hace largo tiempo. El comercio electrónico se debe entender como traslación de las operaciones del mundo económico al mundo electrónico, basándose en la universalización y abaratamiento de las telecomunicaciones y las tecnologías de la información. Así, la **OCDE** define el comercio electrónico de la siguiente manera: "El comercio electrónico generalmente referencia todas las formas de transacciones relativas a actividades comerciales, incluyendo tanto organizaciones como individuos, que están basadas en el procesamiento y transmisión de datos digitalizados, incluyendo texto, sonido e imágenes visuales".

El comercio entre empresas sobrepasa con diferencia el comercio entre empresas y consumidores, por tanto este mercado el que tiene principal potencial de crecimiento trasladado al comercio electrónico. Forrester estima que el comercio electrónico entre em-presas alcanzará 327 mil millones de dólares para el 2002. Todavía un volumen pequeño comparado con el total de la economía, pero con un factor de crecimiento muy elevado.

2. Características del comercio entre empresas

El comercio electrónico entre empresas consiste en la evolución de las empresas hacia una gestión electrónica de sus actividades con proveedores y con otras empresas consumidoras. En este caso la empresa forma parte de una cadena de suministradores de bienes y servicios, donde cada empresa eslabón de la cadena añade valor al producto del que forma parte el/los productos de las empresas inferiores de la cadena. La forma en que las empresas operarían, es decir las actividades que realizarían de una forma electrónica serían de forma muy esquemática, y no siendo exacto en ciertos casos, las que se muestran en la **figura 1**.

Las empresas clientes pueden 'consultar' catálogos de los productos deseados, catálogos 'publicados' por las empresas proveedoras. Una vez la empresa cliente se interesa por uno determinado, podrían 'negociar' los términos de la operación: precio, forma de pago, aplicación de descuentos, derechos de uso, distribución, etc. A menudo, los términos de la operación habrán sido prenegociados y formarán parte de los términos contractuales de todas la operaciones futuras. Tras el acuerdo, se pasaría al 'pedido' para realizar la operación de obtención del producto.

En casos de cadenas de comercio entre empresas ya establecidas y operaciones rutinarias, no se darían las actividades de publicidad-busqueda y negociación de términos, siendo el pedido la primera operación. Cuando la empresa proveedora proporciona el producto (bien o servicio) se realiza la 'facturación' al comprador, incluyendo o no referencia al pago. El 'pago' se puede realizar por adelantado o ante recepción del producto, en función de los términos de la operación, haciéndose uso de algún tipo de medio de pago, y normalmente involucrando una notificación al proveedor. La 'entrega' del producto se producirá antes, durante o después del pago, proporcionando la empresa comprador 'acuse de recibo' del mismo.

La operación realizada se traduciría en uno o más apuntes de la 'contabilidad' de las empresas participantes, así como en el 'inventario', etc. La empresa por otra parte ofrece a los clientes servicios de 'soporte' sobre uso del producto, problemas con el producto, actualizaciones, etc., e información del progreso de las operaciones que están realizando. Una actividad final de cada una de las empresas participantes en la cadena es la 'recolección', 'gestión', 'análisis' e 'interpretación de los datos' relativos a las transacciones realizadas con el objetivo de establecer la estrategia de la empresa.

3. La tecnología de comercio electrónico entre empresas

3.1. Los comienzos

Las actividades indicadas anteriormente son total o parcialmente realizables mediante medios electrónicos. A medida que los ordenadores y las comunicaciones se han extendido y abaratado, muchas de ellas se han automatizado. Así, hace mucho tiempo que las empresas disponen de sistemas informáticos para procesamiento y contabilidad de operaciones, inventario, etc., así como medios más o menos elaborados de tratamiento de los datos acumulados de dichas operaciones. Sin embargo estos sistemas estaban aislados entre sí, surgiendo la necesidad de unirlos a través de redes de comunicaciones. Surgieron numeras iniciativas de intercambio electrónico de documentos, en sectores muy concretos como **ERMA** en el sector bancario, **DISH** y **SHIPNET**. Posteriormente, durante los años 80 surgieron lo que se denominaron **VAN** (*Value Added Network*) proporcionando canales de comunicación seguros para intercomunicación diversos sectores empresariales. Estas redes se diversificaron y se crearon estándares de mensajes para **EDI** (*Electronic Data Interchange*).

3.2. EDI y Redes de Valor Añadido

EDI se puede definir de forma sencilla como intercambio de datos estructurados entre ordenadores. La realización de

e-business

Las soluciones de software para Comercio Electrónico de IBM le ayudarán a aprovechar Internet al máximo. Podrá incrementar sus ventas y mejorar su servicio al cliente. Es lo que ha hecho, por ejemplo, el Club de Fútbol Chelsea.

¿Cuántas empresas que vendan a través de Internet ve usted en esta foto?

Es muy posible que se haya quedado corto porque tanto si organiza acontecimientos deportivos, como si fabrica artículos para el deporte, podemos ayudarle a abrir su negocio en Internet de una forma fácil y a crecer con rapidez, al ritmo que usted imponga. Con las Soluciones de Comercio Electrónico de IBM, abrirá nuevos mercados y servirá a sus clientes las 24 horas del día, facilitándoles una vía para realizar transacciones seguras a través de Internet. Además, podrá integrar su sistema de gestión y optimizar sus recursos. IBM junto con su red de Business Partners le ayudarán desde el principio, hasta el final.

Si desea saber más al respecto, visítenos en www.software.ibm.com/ec/spainfo

IBM

Soluciones para nuestro pequeño mundo

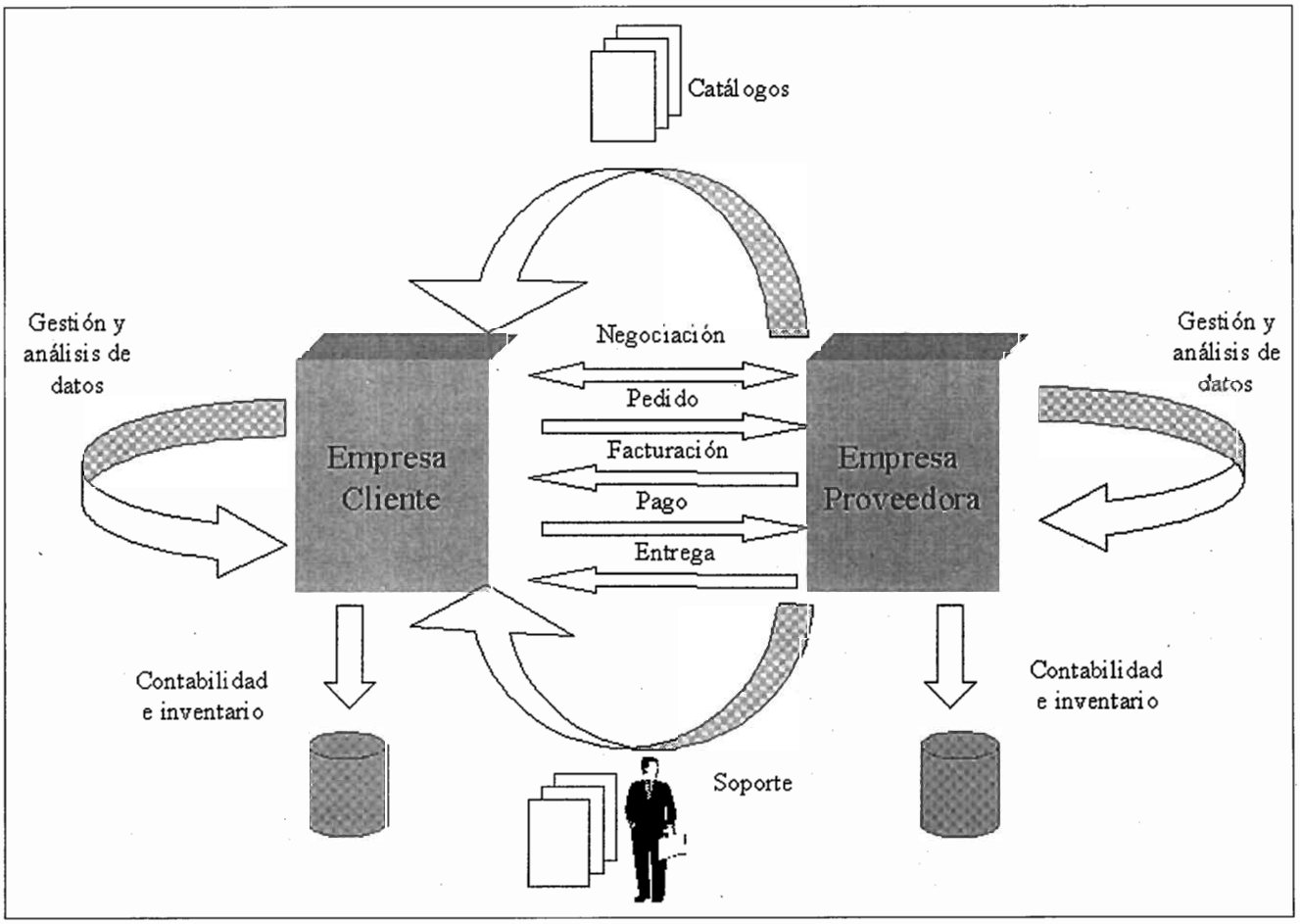


Figura 1

comercio electrónico entre mediante *Email* no es EDI, ya que se trata de datos no estructurados. La ventaja de intercambiar datos estructurados es que su procesamiento se puede realizar con el mínimo de intervención humana. Así, de forma muy esquemática, tal como muestra la **figura 2**, los datos de un sistema corporativo, dentro de su lógica de negocio, se codifican en un mensaje de formato estándar EDI, se envían por la red de comunicaciones al ordenador destinatario, donde se decodifica y procesa por la aplicación corporativa destino siguiendo su propia lógica de negocio.

La impresión de los mensajes hace perder el sentido de EDI, ya que su gran ventaja de y razón de implantación es el tratamiento automatizado de los mensajes. Sin embargo, en una cadena sectorial, pueden existir socios que no implanten un sistema automatizado, necesitándose lo que se denomina EDI híbrido. En el EDI híbrido todas las transacciones se tratan como si fuesen para socios que aceptan EDI, pero que en la etapa final se convierten en fax, *email* o papel. Las VAN son el medio de comunicación más utilizado para realización de EDI. Estas redes están gestionadas por terceros, proporcionando un servicio de "almacenamiento y recuperación", donde cada usuario tiene un buzón para la recepción de mensajes. Las aplicaciones corporativas pueden procesar los mensajes allí almacenados y conectarse para mandar y recibir mensajes de sus socios comerciales, siguiendo los flujos de información de la empresa. Estas redes proporcionan un entorno seguro (autentificado) y fiable (sin perdida de mensajes) para la realización de transacciones, teniendo una amplia cobertura geográfica y con conexión desde diversas redes de acceso como X.25, X.400, ISDN, etc.

Entre las funcionalidades de valor añadido pueden encontrarse: posibilidad de *backups* de la información que pasa por los buzones del usuario, garantía de la integridad de los datos mandados/recibidos, facilidad de envío automático de documentos mediante llamada al receptor del mensaje, estadísticas (auditorías) sobre los documentos intercam-

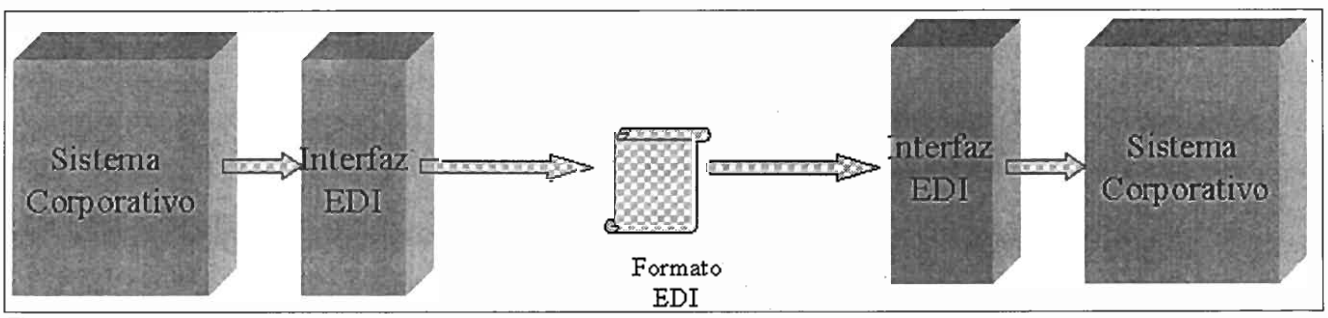


Figura 2

biados, aceptación y validación sintáctica de diversos estándares de formatos de documentos, funciones de "notaría" electrónica, conversión de documentos a fax u otro medio (EDI híbrido), etc. El objetivo de estas diversas funcionalidades es garantizar y ayudar a las empresa a llevar su relación comercial con sus socios comerciales de forma electrónica sin problemas.

Uno de los problemas más importantes de EDI es el establecimiento de estándares unificados de documentos, adecuados a las necesidades de las distintas empresas y tipos de operaciones a realizar entre ellas. Existen multitud de estándares por sectores y países, así por ejemplo en Japón llegaron a convivir 26 conjuntos de estándares. En EE.UU. el estándar más extendido es **ANSI X12**.En la actualidad los estándares se están moviendo hacia **EDIFACT** (***EDI for Administration, Commerce and Transport***), en un intento de unificar las necesidades de los diversos sectores. Una derivación interesante de **EDIFACT** es **OO-EDIFACT** (***Object Oriented EDIFACT***), una versión formalizada en objetos, todavía por desarrollar, y que no sería compatible con la sintaxis actual. Open-EDI es una interesante propuesta que permite dialogar a las diversas partes sin necesidad de acuerdos previos, gracias a su modelización de la información de negocio. Esta propuesta incluye interfaces a aspectos de negocio, aspectos legales, seguridad, comunicaciones, etc, de forma que no sea necesario en principio utilizar ninguna tecnología propietaria. A finales de esta década había grandes expectativas de éxito, que sin embargo no se cumplieron, existiendo un lento crecimiento de EDI. Las causas principales, como luego se analiza posteriormente, fueron la dificultad de integrarse con un sistema de EDI, los costes de integración con el sistema informático corporativo y la falta de beneficios claros obtenidos del nuevo sistema, sobre todo para las pequeñas y medianas empresas. Estas empresas utilizaban teléfono y fax para comunicarse entre sí, por lo que además las grandes empresas tampoco podían sacar todo el partido posible a su sistema EDI debido a que la mayor parte de las empresas con que trataban no lo utilizaban.

3.3. Internet como medio de comunicación universal entre empresas

Al desarrollarse Internet surge un entorno abierto y variado para la transmisión de mensajes entre empresas, siendo no sólo EDI por Internet, sino también *email*, fax, mensaje de voz, etc., así como el Web para las actividades de publicidad y búsqueda de productos en catálogos electrónicos, soporte al cliente, etc. En este entorno se buscan medios que garanticen la seguridad de las comunicaciones de las redes de comercio electrónico, a semejanza de las VAN, pero sobre Internet.

Las aplicaciones de tipo **WebEDI** (*Web Electronic Document Interchange*) permiten mandar/recibir mensajes EDI de forma segura por Internet, autentificados por firma electrónica y protegidos mediante encriptación. El movimiento del mensaje se controla y rastrea todo el tiempo, a semejanza de la funcionalidad de las VAN tradicionales. Este sistema permite, simplemente con un *browser*, acceder a un Web seguro desde donde podrán mandar y recibir mensajes EDI, rellenando formularios de documentos EDI estándar. Así, las principales operadoras de VAN ofrecen pasarelas desde Internet a sus redes tradicionales, de forma que ahora las pequeñas y medianas empresas pueden acceder de forma

barata a la cadena EDI establecida por las grandes empresas de su sector, para complementar su oferta de comercio electrónico. Es de suponer que a medio y largo plazo las VAN establecidas se migren completamente a Internet.

Para la transmisión de datos EDI en el *email* se creó una extensión de tipo **MIME** (rfc-1767) preparado para tal efecto. A continuación las especificaciones de **EDIINT** (*Electronic Data Interchange- Internet Integration*) que se están desarrollando intentan ofrecer además cuestiones como la integridad de las transacciones, privacidad y no-rechazo en diversas formas, de forma que se asegure la interoperabilidad de las diversas soluciones EDI sobre Internet. Además, a parte de las transmisión de EDI sobre *email*, se ha generado una especificación para HTTP. Los estándares se generan, pero sin embargo no se utilizan salvo por unos pocos, creándose en su lugar estándares *de facto*.

Desde hace relativamente poco tiempo, los catálogos se han convertido en una forma fundamental de realizar el comercio electrónico entre empresas. Basado en los formatos de X12 de documentos EDI aplicables, surge **OBI** (*Open Buying in the Internet*), que pretende unificar, sin depender de ninguna tecnología propietaria, las comunicaciones de comercio electrónico entre empresas a través de Internet, siguiendo el siguiente modelo basado en catálogos: a través de una acción realizada por el peticionario a través de browser al catálogo de la empresa vendedora, que genera un objeto OBI por HTTP hacia la empresa compradora, que lo convierte en una orden OBI que se autorizará en la empresa vendedora mediante algún medio de pago. En el futuro planean ampliar los formatos sobre EDIFACT y XML.

XML es una tendencia actual de realización de operaciones EDI y de otro tipo, gracias a que a diferencia de intercambiar simplemente datos, permite intercambiar datos de sincronización entre sistemas, es decir plantillas de control. Gracias a este sistema de plantillas de control es posible utilizar reglas de negocio más flexibles y adaptativos. Las plantillas de control o de proceso permiten establecer información sobre la tarea a realizar con la información EDI y están codificados en lo que se denomina **DTD** (*Document Type Definition*). Los agentes software de los sistemas EDI son capaces de interpretar estos DTD y los datos, a partir de unos repositorios (diccionarios) de entidades globales. De esta forma surgen nuevos estándares para el nuevo entorno; así, derivación de este estándar es el **OBI** (*Open Buying in the Internet*) y EDIINT.

3.4. El cambio de la forma de trabajar de las empresas

Pero lo más importante para el éxito del comercio electrónico no es la tecnología de comunicaciones utilizada, sino el cambio en la forma de operar de las empresas, de forma que saquen partido del sistema. En primer lugar eliminando las operaciones manuales y realizadas sobre papel por sistemas electrónicos. A continuación rediseñando los flujos de trabajo, simplificándolos y creando formas nuevas que exploren las posibilidades del comercio electrónico: es lo que se denomina **BPR** (*Business Process Redesign*). Sólo de esta forma las empresas obtendrán un beneficio superior al coste de introducir el nuevo sistema. Esta transformación está muy unida a utilizar sistemas de ***Workflow*** u **ERP** (*Electronic Resource Planning*) de forma que se racionalicen los flujos de trabajo internos de la empresa.

Las operadoras de las VAN, así como consultoras especializadas facilitan la implantación del EDI, cubriendo diversos aspectos de su desarrollo: estudio de los beneficios de introducir EDI en la empresa, análisis de los flujos de información, análisis de los cambios organizativos necesarios para aprovechamiento de EDI, elaboración de un plan de implantación, incorporación de documentos al sistema EDI siguiendo los estándares y preparación de las herramientas de cliente a utilizar.

Con respecto al comercio electrónico, los sistemas de ***Workflow*** (**ERP**) están evolucionando para interactuar entre sí, bien mediante EDI, bien mediante tecnologías propietarias, aunque se tiende a la estandarización. Así, los productos comerciales (SAP, Baan, etc) normalmente ofrecen un conjunto de soluciones (componentes) de comercio electrónico entre empresas que integra la cadena de *workflow* de suministradores, fabricantes, distribuidores, etc, con los sistema de planificación avanzada corporativos y los sistemas de *data warehouse* para análisis de la información corporativa. Una tendencia en estos sistemas es a utilizar cada vez más tecnologías de procesamiento basados en agentes.

No existe en la actualidad ningún estándar aceptado de *workflow*, aunque existen iniciativas. La **WfMC** (*Workflow Management Coalition*) es una asociación internacional, sin animo de lucro, de vendedores de productos de *workflow*, clientes y consultores, cuya misión es promover el uso del *workflow* mediante el establecimiento de estándares sobre terminología, interoperabilidad y conectividad. El modelo conceptual que proponen tiene un núcleo (*engine*) con 5 Interfaces: herramientas de definición de procesos, aplicaciones clientes, invocación de aplicaciones terceras, interoperabilidad con otros sistemas de *workflow* y herramientas de control/monitorización. Hace poco han remitido **SWAP** (*Simple Workflow Access Protocol*), un estándar propuesto para que los productos de *workflow* pueden interrelacionarse a través de Internet, y sustituye la definición de Interface 4 de interoperabilidad, basada en tipos **MIME** de *email*. El estándar se basa en HTTP 1.1 y no sólo permitiría a los sistemas de *workflow* interactuar entre sí, sino también con otro tipo de servicios basados en Web, basándose en **XML**. Otro estándar importante es **DMA** (*Document Management Alliance*), que pretende que la gestión de documentos de los diferentes sistemas puedan interoperar.

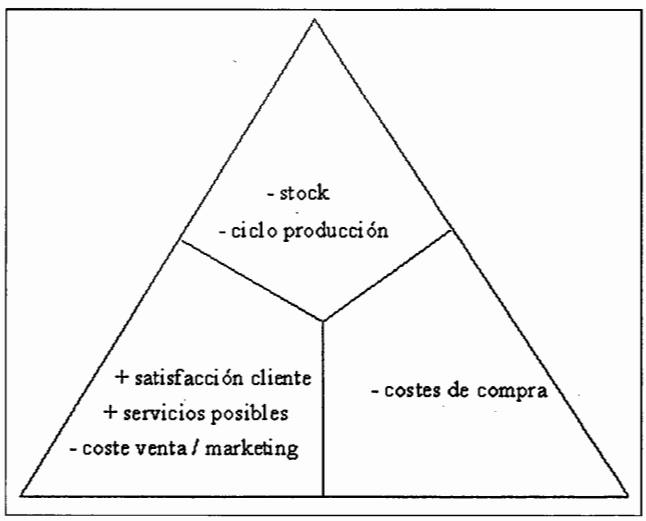


Figura 3

Dada la proximidad de los sistemas de *workflow* al mundo de las empresas, surge como posibilidad que los sistemas de comercio electrónico futuros se deriven de los **ERP**, a base de componentes especializados (p.e los de SAP y el interfaz BAPI), que a la larga se conviertan en un estándar de facto.

4. Beneficios para las empresas

4.1 Ventajas potenciales

Gracias a este entorno, muchas empresas se están moviendo hacia Internet, creando allí sus intranets, extranets con sus socios comerciales y redes de valor añadido privadas. Las empresas ven la oportunidad de obtener beneficios en diversos aspectos: menores costes de compra, ajuste de los productos en *stock*, ciclos de desarrollo menores, un mejor servicio al cliente, menores costes de venta y *marketing*, y nuevas oportunidades de venta. Estas ventajas, que se estudian a continuación, se representan de forma esquemática en la **figura 3**.

El proceso de compra de productos puede ser complejo. Como se indicó de forma simplificada, las empresas compradoras deben buscar los proveedores de aquel producto que satisface los requisitos de características, precio, entrega, etc. Una vez elegido el proveedor, se le indican las características del producto. Si se aprueba la muestra del producto, se le proporciona un pedido por una cierta cantidad, que es respondido con una notificación de que el pedido fue recibido y se puede satisfacer. Una vez el comprador recibe el pedido, recibe una notificación con la factura asociada, que se verifica contra el pedido y sus características. Al automatizarse el proceso de realización de la operación mediante EDI, se reducen los costes administrativos de compra, que la empresa puede dedicar a negociar mejores precios y a construir relaciones con proveedores.

Por otra parte, dentro del ciclo de producción en una empresa, cuanto mas tarda la planificación de producción en alcanzar la demanda, mayor inventario en *stock* debe tener la empresa para manejar retrasos y errores, al tiempo que se reduce la capacidad de reacción frente a cambios en la demanda. Cuando los diversos departamentos y secciones de una compañía se comunican por EDI de forma electrónica, dentro de un sistema de planificación avanzado, el ajuste de la planificación de producción a la demanda es mayor, reduciendo la necesidad de producto en stock y sus costes asociados.

El tiempo de diseño de un producto puede ser reducido mediante soporte electrónico, al compartirse entre empresas las especificaciones del producto a entregar, así como entre los diversos departamentos de la empresa, formándose equipos virtuales de trabajo. Así diseñadores, ingenieros, proveedores, etc. pueden trabajar como un único equipo virtual sobre el producto, en vez de seguirse un proceso secuencial de desarrollo. También se puede reducir el tiempo de producción, al comunicar los pedidos a los proveedores vía EDI, comunicación que sigue a la planificación de producción, que así puede adaptarse rápidamente a los cambios de demanda de clientes y producción de los proveedores.

Pero no sólo se puede optimizar la compra y producción: se pueden optimizar también los servicios de soporte a los clientes. Mediante el Web de la compañía se puede ofrecer soporte al cliente, proporcionando información técnica como manuales, información de resolución de problemas del producto y seguimiento *online* de las operaciones solicitadas (estados de los pedidos, facturas, etc.). Al tiempo que se obtiene una mayor satisfacción del cliente, se produce un ahorro considerable en costes de soporte.

El mismo Web de la compañía permite incrementar fácilmente el número de clientes con poco coste, a diferencia del sistema tradicional de equipo de vendedores, ya que se pueden trasmitir pedidos *on-line*. Al mismo tiempo, ofrecer en el Web catálogos electrónicos permite a los cliente potenciales ofrecer más información y más actualizada sobre los productos de la empresa.

Dada la naturaleza de acceso universal de Internet, gracias a buscadores e índices, mediante su Web las empresas pueden alcanzar una audiencia nacional y/o internacional que sería muy costosa de conseguir por otros medios tradicionales (publicidad, equipo de comerciales, etc.).

4.2. Casos de éxito

En la actualidad son dos sectores los que principalmente comercian empresa contra empresa a través de Internet, el sector de las tecnologías de la información (software, ordenadores, infraestructura de red, etc.) y el sector de las agencias de viaje. Sin embargo, son de especial atención unas cuantas empresas que son claro ejemplo de éxito en su aprovechamiento de los beneficios potenciales del comercio entre empresas en Internet

General Electric, no perteneciente a los sectores indicados anterior, fue una de las primeras empresas en establecer un sistema interno de obtención de productos *on-line*, **TPN Post**. El departamento de abastecimiento recibe las solicitudes de sus consumidores internos y las encamina a los proveedores con la información de los formularios asociada, vía EDI, fax o *email*. El resultado fue que los costes para esta labor se redujeron en un 30 %.

El sector de la automoción en EE.UU. es uno de los sectores que se ha beneficiado de la reducción de los tiempos de desarrollo gracias a compartir información de diseño realizada con herramientas **CAD**, formando equipos virtuales de desarrollo. Igualmente, los fabricantes de vehículos y sus mayores proveedores se comunican ahora con EDI, en vez de utilizar el correo, teléfono o fax, reduciéndose y racionalizando el tiempo de producción, al adaptarse a un plan de producción actualizado casi en tiempo real. De esta forma las fábricas planifican sus líneas de montaje con la llegada de los camiones con componentes.

Cisco es quizá el más claro ejemplo de éxito en el comercio electrónico entre empresas, habiendo facturado más de 1000 millones de dólares por Internet. Esta empresa se dedica a la venta de elementos de infraestructura de red (*routers*, *switches*, etc.), generalmente con la configuración solicitada por el cliente, y mantiene un Web donde permite realizar pedidos *on-line*, así como ofrece soporte al cliente. El cliente a través del Web, puede realizar consultar el catálogo de productos, realizar la configuración *on-line* deseada, comprobar si existen errores y mandar el pedido. El cliente puede posteriormente de forma *on-line* comprobar el estado de progresión de sus pedidos y facturas. Gracias a este

sistema, aparte de la satisfacción del cliente, el coste de venta, sometido antes a errores en la especificación de configuración del pedido, se ha mejorado en un 20 %. Por otra parte al proporcionar a los clientes soporte en información técnica de los productos, información de errores reportados, y descargas de software, ha conseguido un ahorro de 125 millones de dólares en costes de soporte a cliente.

Industry.net es un ejemplo de las posibilidades de intercomunicación entre fabricantes y proveedores que ofrece Internet. Tiene como misión permitir el marketing directo de productos y servicios en el sector industrial, y constituye una comunidad virtual de productores y compradores de productos industriales, con cerca de 500.000 miembros.

5. Barreras al triunfo del comercio electrónico entre empresas

Sin embargo, a pesar de todas las ventajas potenciales y los casos con éxito reconocido, ¿por que no acaba de triunfar de manera masiva el comercio electrónico entre empresas? Según diversos estudios, la primera razón es la falta de modelos de negocio adecuados para sacar beneficios del comercio electrónico, lo que es especialmente cierto para las pequeñas y medianas empresas, que, unido a su general desconocimiento del tema, no pueden permitirse gastos que no lleven asociado beneficios claros de reducción de costes. Este primer problema puede ser parcialmente resuelto por la evolución actual. Gracias a la introducción de EDI en Internet y/o sus variantes (pequeñas y medianas empresas) pueden acceder más fácilmente a las cadenas sectoriales de comercio electrónico. Con el avance de las asociaciones para promoción y conocimiento del comercio electrónico, así como de consultoras especializadas, es de esperar que se produzcan avances en la adaptación de la forma de trabajar de las empresas con el fin de que sean capaces de obtener los beneficios potenciales del comercio electrónico. A continuación de las razones anteriores se situarían la falta de un entorno legal claro al respecto y, de forma muy relacionada con la anterior, la falta de una infraestructura pública preparada para el comercio electrónico, con los estándares, la seguridad, fiabilidad y responsabilidades bien establecidas. Para afrontar estos problemas es fundamental que las Administraciones Públicas promuevan espacios de diálogo para la iniciativa privada con el fin de establecimiento de estándares, marcos legales, etc., de forma que se solucionen las incertidumbres que impiden que las empresas tomen la decisión de entrar en una forma de trabajar que aún consideran arriesgada.

6. El futuro

Muchos expertos del sector pronostican un crecimiento espectacular; otros se muestran más reservados dada la persistencia de muchas de las barreras que impiden el despegue del comercio electrónico. Lo más probable es que el comercio electrónico entre empresas siga creciendo, en especial en EE.UU., sobre todo en grandes empresas y sectores especialmente preparados para el cambio, hasta que se llegue a un umbral en el que quizá se produzca un efecto avalancha. Las pequeñas y medianas empresas irán adoptándolo por mimetismo dentro su propio sector y por imposición de las grandes. En paralelo, las Administraciones, junto con las asociaciones de la empresa privada, irán estableciendo marcos de regulación a medida que lo exija la sociedad. A medida que un número creciente de empresas tomen ventaja competitiva en los diferentes sectores gracias al comercio electrónico, las empresas reticentes tendrán que subirse al tren de esta nueva forma de comerciar y, sobre todo, de trabajar. Porque el comercio electrónico representa un cambio fundamental en la forma en que las empresas trabajan, si es que desean pasar el umbral del nuevo milenio.

7. Referencias

General

The Emerging Digital Economy, U.S. Department of Commerce. Mayo 1998, *http://www.ecommerce.gov*

A European Initiative in Electronic Commerce, E.C. *Information Society Proyect Office*. Abril 1997, *http://www.ispo.cec.be/ecommerce*

Measuring Electronic Commerce, *Commitee for Information, Computer and Communications Policy*. OCDE. 1997, *http://www.oecd.org*

Dismantling the Barriers to Global Electronic Commerce, *Ministerial Conference on Global Information Networks*. OCDE. Diciembre 1997, *http://www.oecd.org*

Barriers and Inhibitors to the Widespread Adoption of Internet Commerce, Research Report. *Commerce Net*. Abril. 1997, *http://www.commerce.net*

VAN

Harbinger Network, Harbinger, *http://www.harbinger.com/products/comm/network/*

EDI*Net, MCI VAN, *http://firstunion.com/business/cashman/edi/mciedi1.html*

Servicios EDI de TSAI

TSAI (Telefónica Servicios Avanzados de Información), *http://www.tsai.es/TSAI/servicios_arb_edi.htm*

EDI

Estándar X12, EC Resource. Harbinger. *http://www.harbinger.com/resource/X12/*

Estándar EDIFACT, EC Resource. Harbinger, *http://www.harbinger.com/resource/edifact/*

OBI standard 1.1 y 1.0, The OBI Consortium, *http://www.openbuy.org/obi/library.html*

EDIINT: EDI over the Internet, IETF Electronic Data Interchange-Internet Integration (ediint) ***Working Group***. Internet Mail Consortium, *http://www.imc.org/ietf-ediint*

Guidelines for using XML for Electronic Data Interchange, XML/EDI Group, *http://www.xmledi.net*

ERP

SAP Solutions, SAP, *http://www.sap.com/*

Baan Business Systems, Baan, *http://www.baanbbs.com/*

Workflow Management Coalition, Association for the Information Management Community, *http://www.aiim.org/wfmc/*

Comercio electrónico

Cybermercado: marco tecnológico de un servicio de venta en Internet dirigido a PYMES

José García, Angel Goitia, José Antonio Corrales, Javier Tuya

Departamento de Informática, Universidad de Oviedo

fanjul@lsi.uniovi.es
goitia@lsi.uniovi.es
ja@lsi.uniovi.es
tuya@lsi.uniovi.es

Resumen: *El proyecto Cybermercado tiene como objetivo principal el desarrollo de una metodología y el software correspondiente que faciliten la creación y puesta en marcha de un servicio de venta en Internet. Se enfoca no a grandes empresas multinacionales, sino a negocios minoristas, para proporcionarles de una forma sencilla y económica una presencia en Internet a través de la cual realizar transacciones comerciales. Se describe en el artículo la etapa de identificación de requisitos y marco tecnológico del proyecto Cybermercado, y se muestra su aplicación en el desarrollo de una tienda real.*

Palabras Clave: *Comercio electrónico, Internet, Web, Bases de datos en la Web, Tiendas en la Web, Seguridad en la Web*

1. Introducción

El tremendo crecimiento de Internet [7], y particularmente de la World Wide Web, ha despertado un gran interés a nivel internacional. Las empresas, conscientes de ello, se preguntan por las posibilidades de este nuevo medio de comunicación desde el punto de vista comercial y de esta inquietud han surgido multitud de técnicas en el campo del comercio electrónico: acceso a bases de datos de productos a través de Web, plantillas para ayudar en la realización de tiendas e innovadores métodos de pago.

Comercio electrónico

El uso de Internet, y más concretamente la Web, lleva el comercio electrónico a su máxima expresión, permitiendo desde una simple venta hasta la creación de un servicio técnico en línea, y todo ello con un rendimiento mucho mayor, tanto desde el punto de vista del comprador como del vendedor.

Concretamente, para los proveedores, Web ofrece, entre otras ventajas:

- Reducción de costes en general. En concreto los costes tecnológicos están experimentando un contínuo descenso y es de esperar que la liberalización del sector de telecomunicaciones a nivel europeo, tenga una repercusión a la baja en estos costes.
- Más posibilidades para la comunicación de información sobre sus productos: El carácter interactivo de la Web permite estrechar el canal de comunicación de marketing, haciéndolo casi personalizado. Además el mercado potencial es el mundo entero, sin necesidad de una mayor inversión.
- Obtención rápida y fiable de datos de mercado. Los límites a este beneficio están regulados en España mediante la LORTAD [5].

Pero no todo son ventajas, existen factores que aún dificultan la adopción del comercio electrónico por parte de las empresas:

- Falta de información acerca de las posibilidades y costes reales del comercio electrónico a través de Web; e infraestructura inadecuada a nivel europeo para el aprovechamiento máximo de la tecnología [4].
- Sólo el 11,1% de los usuarios de Internet la utilizan para realizar compras, el 60% alegan preocupación por la seguridad de sus datos para no utilizar servicios de venta basados en la red [3].
- En el caso español, donde la mayor parte del tejido empresarial es de tamaño pequeño y mediano (PYMES), el alto coste de las soluciones de comercio electrónico existentes es un factor importante. Esto conlleva la agrupación de varias empresas en centros comerciales e invita a la realización de herramientas y metodologías que permitan abaratar estos costes.

2. Proyecto Cybermercado

Cybermercado es un proyecto fruto de la colaboración entre la Universidad de Oviedo y la empresa SATEC S.A., con financiación del Principado de Asturias a través de la Fundación para el Fomento en Asturias de la Investigación Científica Aplicada y la Tecnología (F.I.C.Y.T.). El objetivo del proyecto es el desarrollo de una **metodología** y el **software** correspondiente que faciliten la creación y puesta en marcha de un servicio de venta en Internet.

No obstante, se ha partido de una premisa básica: el producto desarrollado debería estar enfocado sobre todo a PYMES, y por tanto se imponen serias limitaciones económicas.

2.1. Plan del proyecto

Debido a los continuos avances en la materia se previó que los requisitos serían constantemente actualizados, por tanto el proyecto Cybermercado debía tener un ciclo de desarrollo incremental [8], con la implementación de prototipos que sucesivamente se acerquen al producto final.

Antes de comenzar a diseñar el primer prototipo se realizó un estudio sobre qué características serían deseables y el método de implementación. Con estos datos se ha elaborado un análisis cuidadoso de los servicios de este tipo ya existen-

tes en Internet y de las herramientas que ofrecen características de interés para la implementación: servidores Web, sistemas de gestión de bases de datos, motores de búsqueda, software para el acceso a bases de datos desde Internet y paquetes específicos para la creación de tiendas. Como resultado de este estudio previo se obtuvo una lista de objetivos o requisitos y un marco tecnológico para el desarrollo del sistema.

2.2. Objetivos

Las características que debería presentar un sistema de este tipo, y que constituyen por tanto el objetivo del proyecto, son las siguientes:

- Poder **crear desde cero** y mantener un servicio de venta, tanto a nivel de una tienda como a nivel de un **centro comercial**. Para ello son necesarias herramientas que guíen dichos procesos.
- **Identificación de los clientes** y almacenamiento temporal de sus pedidos, de forma persistente entre visitas.
- **Navegación sencilla y práctica**: Es fundamental tener en cuenta los estándares [9] seguidos por la gran mayoría de los servicios de este tipo en lo relativo a la organización de los contenidos de la tienda, de esa forma el usuario se encuentra con un entorno conocido donde le resulta más sencillo realizar compras (véase la **figura 1**).
- **Ofertas, promociones, novedades y ventas cruzadas**: mecanismos de recomendación de productos y publicidad. El aprovechamiento de los datos de mercado disponibles es vital para elevar su efectividad.
- **Búsquedas**: se deben proporcionar búsquedas completas sobre los productos, con la posibilidad de hacerlas complejas mediante operadores lógicos y de buscar palabras clave en el texto de la descripción u otros.
- **Personalización del producto:** la personalización se refleja en detalles como la frase que el comprador desea que sea grabada en un pulsera, por ejemplo, o el dibujo de una camiseta.
- **Personalización del servicio**: consiste en aprovechar los datos de que se dispone sobre el cliente para variar los datos que se ofrecen e incluso la forma en que se ofrecen.
- **Contenido multiligüe:** La oferta de información en varios idiomas diferentes, a elección del usuario, permite la superación de las fronteras nacionales a las empresas. ([1] para más información).
- **Gestión de posventa:** el cliente debe ser capaz de realizar un seguimiento del estado de sus pedidos pendientes. Tras la adquisición de productos, puede recibir información a través de correo electrónico sobre productos nuevos de su interés y sería interesante el establecimiento de libros de sugerencias automáticos.
- **Administración y mantenimiento** sencillos: una de las características que dan un mayor valor añadido al comercio en Internet es el bajo coste de administración y mantenimiento. Para ello se utilizan páginas Web para la gestión de todos los elementos de la tienda, entre ellos los productos, ofertas, pedidos y clientes.
- **Auditoría:** la obtención de datos sobre los eventos de venta permite, por una parte, la elaboración de estadísticas, por otra, la personalización y mejora del servicio.
- **Seguridad:** se debe cuidar la confidencialidad de los datos, en especial de aquellas partes de la tienda relativas a los

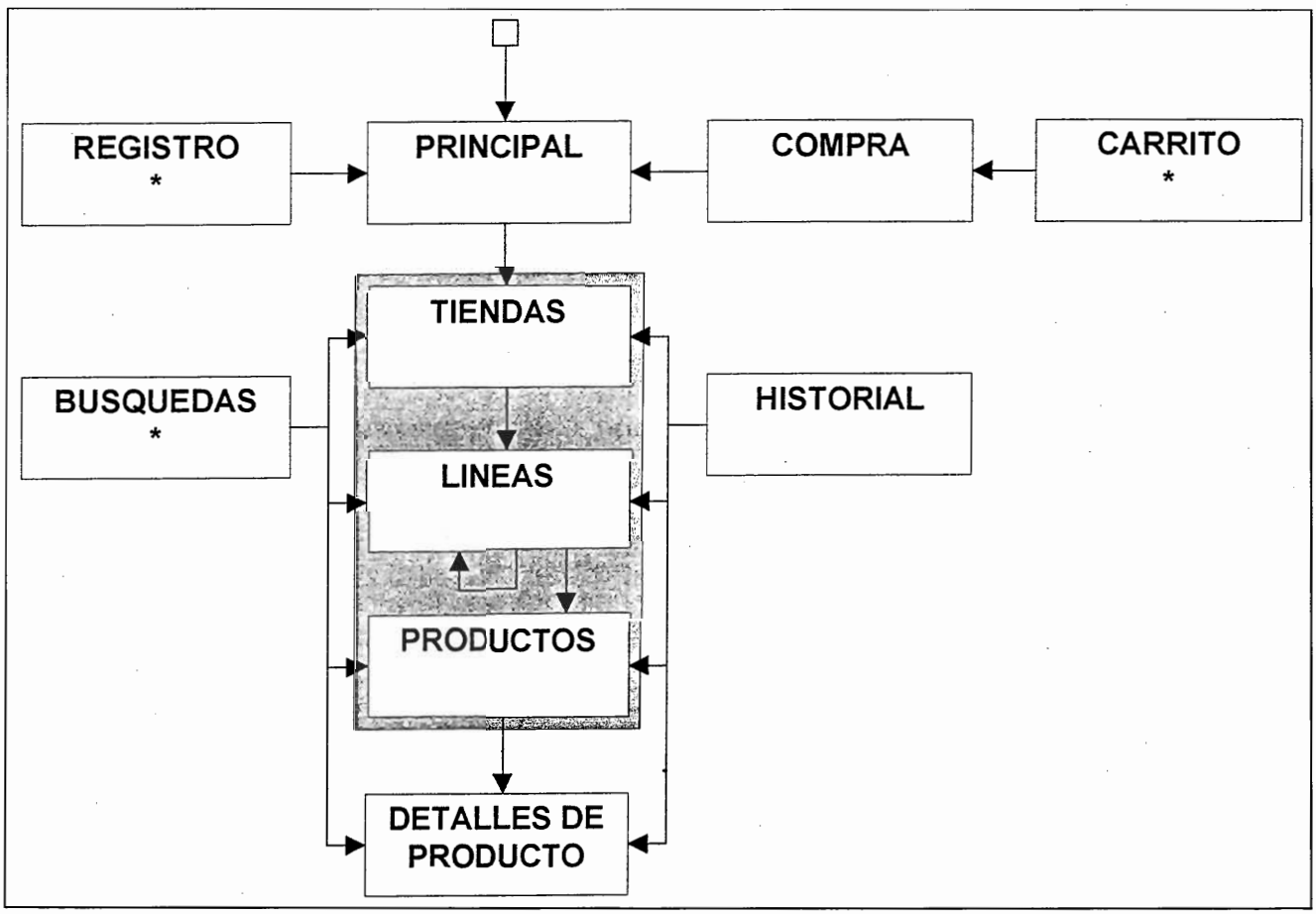
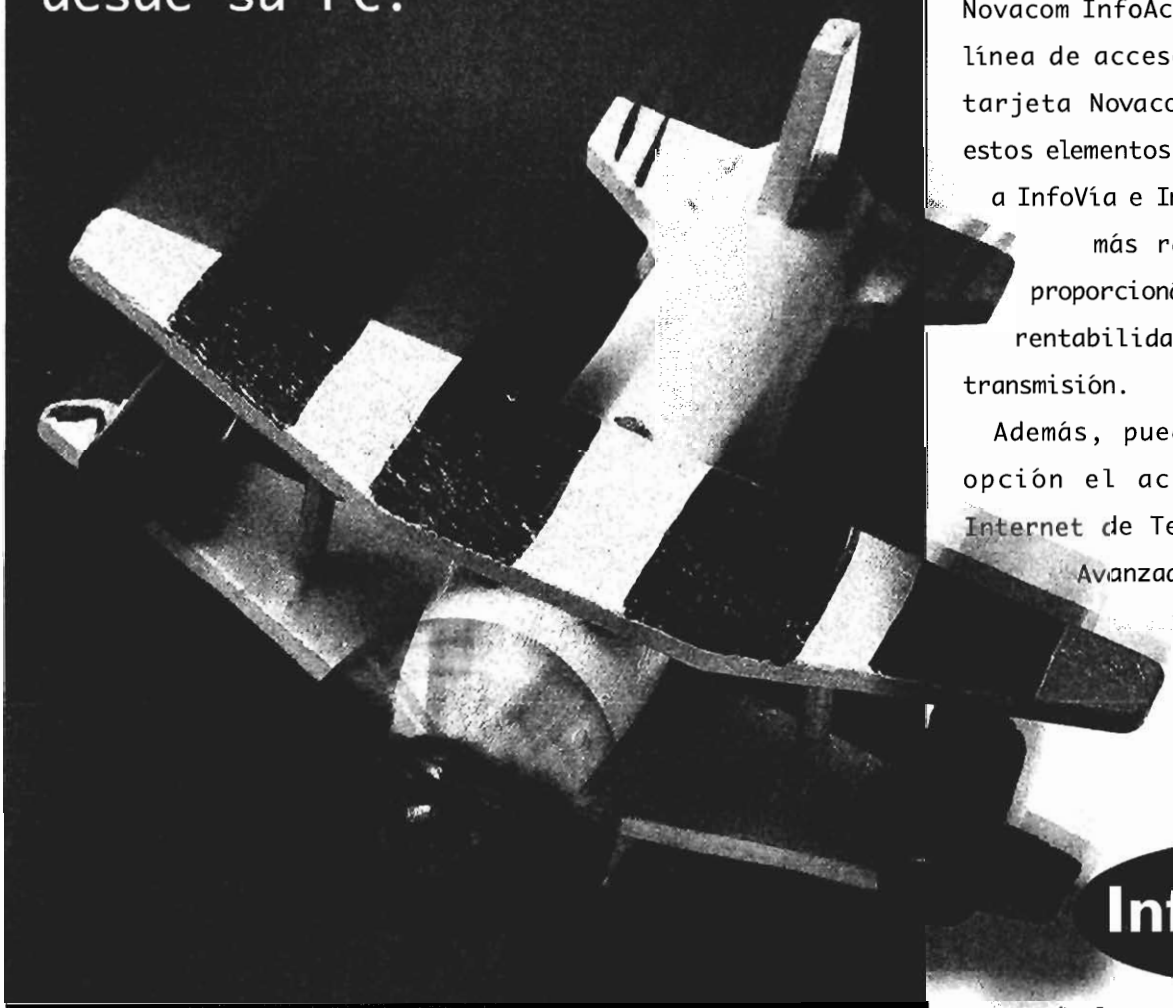


Figura 1: Esquema de navegación simple en un servicio de venta

Novacom InfoAcceso de Telefónica.

La respuesta más rápida y económica para acceder a InfoVía e Internet desde su PC.



Novacom
SOLUCIONES RDSI

Si usted accede habitualmente a InfoVía e Internet desde su PC, Novacom InfoAcceso es lo que necesita.

Novacom InfoAcceso consta de una línea de acceso básico RDSI y una tarjeta Novacom Micro. Gracias a estos elementos usted puede acceder a InfoVía e Internet de la manera más rápida y económica, proporcionándole mayor calidad, rentabilidad y velocidad en la transmisión.

Además, puede contratar como opción el acceso al servicio Internet de Telefónica Servicios Avanzados de Información.

Infórmese

de la promoción de lanzamiento llamando al teléfono

900 111 022

SERVICIO PYMES DE TELEFÓNICA

AENOR ER Empresa Registrada ER-0081/1/98

EQNet

Telefónica

InfoVía http://telefonica.inf Internet http://www.telefonica.es

pedidos y al pago.
- Alto grado de **compatibilidad con los navegadores existentes**, para permitir el acceso al mayor número posible de clientes potenciales.

2.3. Marco tecnológico

En este punto se hará una breve descripción del estado del arte, para a continuación describir aquellas opciones que han sido estudiadas en más profundidad durante el trabajo desarrollado, justificar la elección de una de ellas y describir la tecnología que nos permitirá cumplir los objetivos que hemos detallado en el apartado anterior.

2.3.1. Estado del arte

Se ha observado que existe una gran cantidad de productos en el mercado que pueden facilitar la labor del desarrollo de una tienda en Internet. En el estudio realizado se han identificado dos tipos principales de productos:
- Aquellos que cubren todos o gran parte de los aspectos del funcionamiento de una tienda.
- Los que ofrecen funcionalidades generales para el desarrollo de aplicaciones Web, y que pueden facilitar ciertos aspectos de la creación de una tienda.

Este último grupo de productos no resulta útil en un entorno en el que no se puede abordar la creación y mantenimiento de un sistema de venta por la falta de recursos. Sin embargo, en las pruebas realizadas, se observó que los productos del primer tipo tampoco permitían la realización de esta tarea de una forma simple o no eran suficientemente asequibles desde el punto de vista económico. Por ello se optó por abordar el desarrollo de un producto perteneciente al primer grupo, que cubriese las carencias observadas.

2.3.2. Identificación de alternativas

El estudio realizado, junto con los recursos software y hardware disponibles indicaron como mejores alternativas para el desarrollo del producto las siguientes: (1) *Microsoft Merchant Server*, (2) *Internet Information Server* y (3) *Netscape Enterprise Server*.

En todos los casos la plataforma a utilizar es un PC compatible con sistema operativo *Microsoft Windows NT 4.0*, que se ha seleccionado por su bajo coste relativo en comparación con otras plataformas. Como servidor de bases de datos se utiliza *SQL Server 6.5*, aunque se busca la independencia entre el producto y el **SGBD**, por tanto se elige **ODBC** como método de acceso.

En la alternativa (1) se utiliza el *Internet Information Server* como servidor **HTTP**. Las principales funciones de la tienda vienen implementadas en el *Merchant Server* y se proporciona un **API** de programación que facilita la creación de algunas funciones nuevas además de una forma de **HTML** preprocesado como lenguaje de creación de servicios de venta. Como inconveniente, la creación de una tienda desde cero no viene facilitada en modo alguno por el producto.

En la alternativa (2) el *Internet Information Server* no proporciona ninguna de las funciones específicas que nos proporcionaba el *Merchant Server* (1). Lo que si se proporciona es un lenguaje de programación interpretado (**ASP** – *Active Server Pages*) que facilita la creación de cualquier aplicación WEB, incluyendo el acceso a bases de datos mediante las librerías **ADO**.

Por último, en la alternativa (3) se sigue una filosofía similar a la alternativa (2). En este caso el servidor Web utilizado es el *Netscape Enterprise Server*, el lenguaje utilizado es *JavaScript* y las librerías de acceso a bases de datos son las librerías *LiveWire*.

2.3.3. Alternativa seleccionada

Las tres posibilidades descritas han sido evaluadas y de dicha evaluación se han extraído las siguientes conclusiones:
- *Internet Information Server* es un servidor **HTTP** que se distribuye de manera conjunta con *Windows NT*. Esto conduce a que la administración, la gestión de la seguridad, etc. se hallen altamente integradas con el propio Windows, utilizando incluso las herramientas que proporciona el sistema operativo.
- En cuanto al acceso a la base de datos, el *Merchant Server* (1) implementa un juego de instrucciones limitado, como instrucciones **SELECT** extendidas a toda una tabla o bien consultas **SQL** almacenadas previamente en la base de datos. En lo que respecta a (2) y (3), son bastante similares entre sí, aunque la experiencia ha demostrado que ADO es más potente y flexible que *LiveWire*, ya que se puede realizar una mayor variedad de operaciones.
- El *Merchant Server* (1) es mucho más costoso que las otras dos opciones y, desde nuestro punto de vista, las funciones que implementa no proporcionan una ventaja notable frente a los otros dos casos, ya que pueden ser fácilmente sustituidas por unas pocas rutinas reutilizables entre tiendas.

Se ha desarrollado posteriormente un producto denominado *Microsoft Site Server Commerce Edition* que suple algunas de las deficiencias detectadas en su momento en el *Merchant Server*. No obstante, su precio sigue siendo una gran barrera para su utilización en el desarrollo de servicios de venta para el segmento de mercado al que se dirige el proyecto Cybermercado.

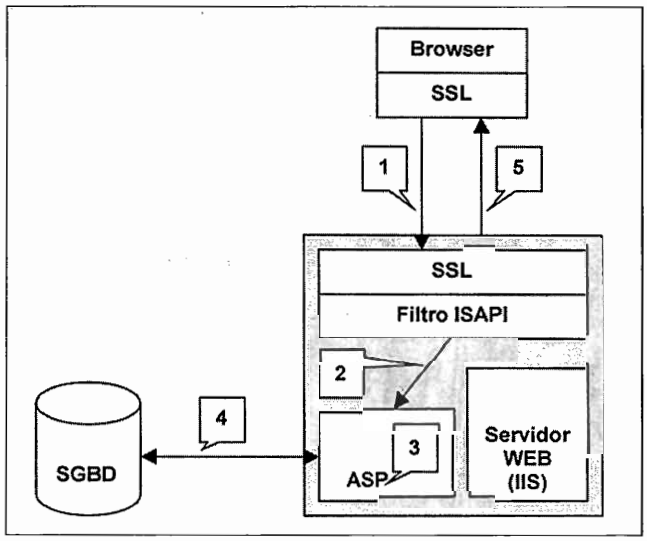


Figura 2: Esquema de integración de los componentes

Por todos estos motivos, la alternativa que finalmente se ha elegido para el desarrollo del producto es la numero (2).

2.3.4. Solución propuesta

Con la plataforma mencionada en el punto anterior se establece un marco tecnológico. En este punto se relacionarán los objetivos que previamente se habían enumerado.con las técnicas empleadas para resolverlos en dicha plataforma. Apoyándose en los recursos de desarrollo descritos en la alternativa seleccionada, en la que se dispone de un lenguaje de programación (**ASP**) utilizando código *Jscript* o *VBScript* [6] y un mecanismo de acceso a bases de datos (**ADO**), quedan por resolver dos puntos importantes:

En primer lugar, la identificación de los clientes: dada la carencia de persistencia en las conexiones HTTP se utilizan *cookies* para dotar de memoria al sistema. No obstante fue necesario diseñar un protocolo complementario que permitiese identificar no al *browser* sino al comprador.

Otra característica imprescindible es asegurar la confidencialidad de los datos de los clientes del sistema, para lo que se seleccionó el protocolo **SSL** (*Secure Sockets Layer*) [10]. De este modo, utilizando navegadores que lo soporten, se pueden realizar comunicaciones seguras utilizando mensajes cifrados.

2.3.5. Conclusiones sobre el marco tecnológico

Con la plataforma elegida se pueden solucionar todos los requisitos planteados en el apartado Objetivos. Para la tienda que será resultado de nuestro proyecto, se tiene el siguiente esquema de integración entre los distintos componentes:

1. El navegador del cliente lanza una petición **HTTP** al servidor Web de la tienda. Existe la posibilidad de usar **SSL** en los puntos de la tienda definidos por el administrador.
2. Un filtro **ISAPI** reconoce la petición como destinada al componente **ASP**.
3. El componente **ASP** procesa la petición: interpreta el código fuente incrustado en la página.
4. Si en el código **ASP** se produce alguna referencia a la base de datos, se establece la oportuna conexión **ODBC** con el **SGBD**.
5. Cuando finaliza la interpretación, el servidor Web retorna al navegador la página **HTML**.

El coste del entorno de desarrollo no es muy elevado y el esfuerzo invertido en el desarrollo del sistema influirá directamente en la usabilidad del producto. El compromiso entre la funcionalidad y la compatibilidad puede ser fácilmente equilibrado en caso de un replanteamiento de los requisitos.

3. Caso práctico: Tienda SATEC

Tras tener definido claramente el marco tecnológico en el que se va a trabajar y la integración de los componentes, se han realizado varios prototipos para el refinamiento de la funcionalidad y la definición de requisitos. En algunos casos se trataba de tiendas ficticias pero en otros se trabajó con datos reales. Uno de estos casos es la tienda SATEC, con productos de la empresa SATEC S.A.

Al entrar en SATEC el cliente ve la página principal con las principales líneas de productos presentes en la tienda. Puede seleccionar una de ellas o bien utilizar uno de los botones de la cabecera como atajo para ir a las zonas más solicitadas de la tienda: Principal, Carrito, Comprar, Buscar, Anteriores, Registro, Pedidos y Ayuda.

El funcionamiento es sencillo: al ir seleccionando los hiperenlaces que se le presentan, el usuario puede moverse entre las distintas lineas o productos que existen. En la **figura 3** se observa la descripción detallada de un producto de SATEC.

La organización de los productos en el caso de SATEC hizo generalizar la forma en que se implementan las distintas líneas. La mayor parte de las tiendas existentes están pensadas para soportar organizaciones jerárquicas, pero también es posible que un elemento rompa esa jerarquía y pertenezca a varias líneas diferentes, entonces el esquema de organización se convierte en un grafo.

Por tanto los productos de una tienda se agruparán en líneas. Las líneas están pensadas para que el administrador pueda implantar formas diferentes de ofrecer sus productos. "Metalíneas" es una forma de denominar aquellas líneas que no contienen productos directamente sino que agrupan otras líneas.

Los productos que comparten la mayor parte de sus características técnicas configuran una serie. El concepto de serie se distingue del de línea en que la pertenencia a una serie es algo intrínseco a la definición del producto. Las líneas, por el contrario, son agrupaciones más artificiales.

En la **figura 4**, el cable serie de dos metros y el de siete son en realidad el mismo producto. Todos los productos que se venden a precios diferentes dependiendo de un único atributo diferenciador, decimos que pertenecen a la misma familia. Otro ejemplo paradigmático de familia es un CD y cassette del mismo grupo y álbum; son el mismo producto en diferentes formatos, por lo que conforman una familia de productos.

Una vez localizado el producto de su interés, el cliente puede añadirlo a su pedido junto con los demás productos que haya seleccionado. En cualquier momento puede consultar o modificar el estado de su carrito y, en último lugar, puede formalizar la compra. En ese momento se le pedirá que introduzca sus datos personales entre los que están los datos necesarios para efectuar el pago. Durante la introducción de estos datos privados se utiliza **HTTP** seguro usando el protocolo **SSL**.

El cliente recibe, finalmente, un identificador de su pedido que puede utilizar para realizar un seguimiento a partir de ese momento.

4. Conclusiones y trabajo futuro

SATEC pertenece a una serie de prototipos creados en el marco de un proyecto ambicioso: **Cybermercado**. Su objetivo principal es reunir en un solo producto todos los aspectos relacionados con el desarrollo de servicios de venta en Internet para PYMES.

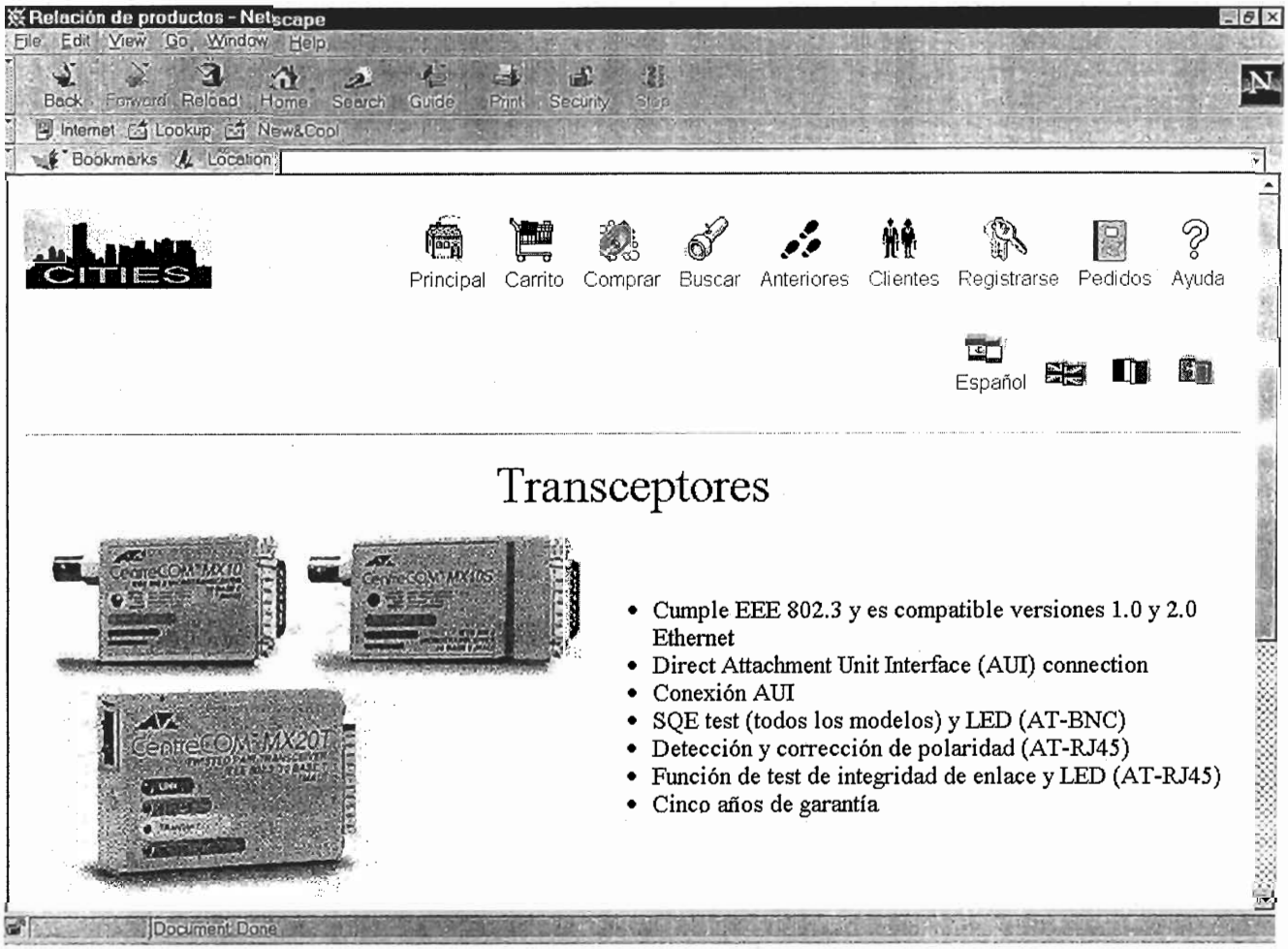


Figura 3: Página detalle de un producto en SATEC

Cybermercado pretende cubrir las carencias localizadas en los productos existentes en el mercado tanto desde el punto de vista técnico como en el económico, básico este último para el sector al que nos dirigimos. Las características identificadas durante el desarrollo de los sucesivos prototipos, que están siendo implementadas y que no se contemplan habitualmente en las herramientas existentes son:

- generación automática del código de la tienda a partir de una toma de datos previa,
- internacionalización del sistema, apariencia personalizada e individualizada para cada producto y
- para el servicio de venta, métodos de navegación alternativos, soporte multimedia y tipos de clientes [1].

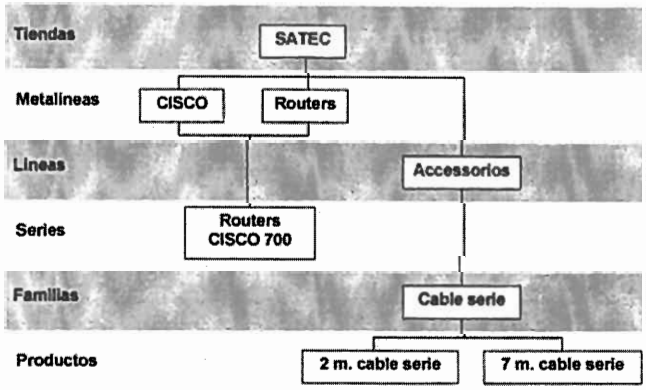


Figura 4: Esquema parcial de las líneas de productos en SATEC

5. Referencias

[1] Cano, A., Blanco, E., García-Fanjul, J., Goitia, A., Corrales, J.A. y Tuya, J.; CITIES: a model for the development of Web-based sale services. Pendiente de publicación en los *Proceedings* de SCI'98 - Orlando (Florida).

[2] Halchmi, Z. y otros; *Electronic commerce.* Abril 1996. *http://techunix.technion.ac.il/~orena/ec/index.html* (22 Sep. 1997)

[3] Pitkow, J.E. y Kehoe, C. M.; Emerging trends in the WWW user population. *Communications of the ACM*, págs. 106-108. Junio de 1996. Volumen 39, número 6.

[4] KPMG International; *e-Christmas achievements & learning.* Public report. February 1998. *http://www.kpmg.co.uk/uk/direct/industry/ice/exmas/* (20 May, 1998)

[5] Ley Orgánica 5/92 de 29 de Octubre de regulación del tratamiento automatizado de datos de carácter personal. Boletín Oficial del Estado, nº 262, del 31 de Octubre de 1992.

[6] Lomax, P.; VBScript: Active clients and servers. *World Wide Web Journal.* Spring, 1997.

[7] Gray, M.; «Internet Statistics: Web Growth, Internet Growth». 1996. http://www.mit.edu/people/mkgray/net/ (6 Oct. 1997).

[8] Ministerio de Administraciones Públicas; Plan General de Garantía de Calidad aplicable al desarrollo de equipos lógicos. Edita: Ministerio de Administraciones Públicas; Colección Informes y Documentos; Serie Administración General.

[9] Lynch, P.J. y Horton, S.; *Yale Center for Advanced Instructional Media Style Guide*, 1997. *http://info.med.yale.edu/caim/manual/contents.html* (4 Mayo, 1998).

[10] Baldwin, R.W. y Chang, C.V.; Locking the e-safe. *IEEE Spectrum, Special issue on Electronic Money.* Págs. 40-46. Febrero, 1997.

Comercio electrónico

Protocolos de Pago Comerciales para Micro-Comercio

Francisco Fernández Masaguer
Departamento de Tecnología de las Comunicaciones
ETSI. Telecomunicación Vigo, Universidad de Vigo

ffernandez@dtc.uvigo.es

Resumen: *Presentamos en este articulo el funcionamiento y propiedades de los dos protocolos de pago para micro-comercio más relevantes, Millicent y Minipay, de próxima aparición para uso comercial, realizando una evaluación de las ventajas e inconvenentes de cada uno de ellos.*

1. Introducción

Los sistemas de microcomercio son sistemas orientados a la compra de objetos de información o servicios de pequeño o muy pequeño valor. La frontera la podemos fijar alrededor de las 100 pts. que es el coste del servicio para el cual la carga mínima asociada con los demás sistemas de pago (30 pts. para el sistema de tarjeta de crédito), sería vista por el usuario como abusiva. Así, podemos considerar como sistemas de microcomercio todos aquellos que para el pago de objetos o servicios por debajo de las 100 pts. imponen unos costes por transacción no superiores al 1%.

Esta claro que estos sistemas, gracias también a la cobertura y potencia informativa de servicios como el Web, abren las puertas a la venta electrónica de una cantidad y variedad de servicios extraordinaria. Así pueden citarse por ejemplo, la venta de artículos o secciones de periódicos o revistas electrónicas, venta de juegos, música o pequeños documentales, venta de paquetes de software, applets de Java, etc. Mas aun, si el coste por transacción puede llegar a ser extraordinariamente pequeño, son imaginables aplicaciones como la medida de acceso o uso por los usuarios de recursos o servicios tales como aplicaciones, bases de datos, redes o recursos compartidos de un sistema distribuido.

2. Requerimientos de los sistemas de micro-comercio

Puesto que el objeto principal de este artículo es la evaluación de los protocolos de micropagos comerciales, creemos prudente enumerar primero algunos criterios que por otra parte nos guíen en la evaluación. Estos requerimientos, sin ánimo de ser totalmente exhaustivos, se recogen debajo. Básicamente puede decirse que estos sistemas heredan los requerimientos de los demás esquemas de pago, sólo que ahora los aspectos de coste y eficiencia adquieren una importancia casi capital, hasta el punto de que otros requerimientos, como el control absoluto de cualquier tipo de fraude, se relajen ligeramente en aras de mantener el coste al mínimo posible:

· *Autenticidad e integridad.* El protocolo debe asegurar la correcta identidad de los usuarios y la inalterabilidad de las transacciones. Idealmente la autentificación debería basarse en clave pública para evitar problemas de repudiación, siempre que ésta no degrade mucho la eficiencia. El protocolo debe por otra parte prevenir los ataques de reactuación.

· *Privacidad y Anonimidad.* La privacidad puede ser tanto o más importante en el caso del microcomercio que cuando se trata de compras mayores. El protocolo ha de garantizar que sea imposible ligar una determinada información o pago a la identidad real del comprador, independientemente de que la red de comunicación no provea de canales anónimos entre los participantes. La anonimidad del comprador ha de ser posible tanto frente a terceros (observadores) como frente a los vendedores e intermediarios financieros y/o bancos, y, en última instancia, frente a colaboraciones entre estos.

· *Control de la anonimidad.* Esta es importante como medida de prevención contra posibles abusos resultantes de una anonimidad absoluta, por requerimientos legales o gubernamentales, o por conveniencia del vendedor.

· *Divisibilidad.* El protocolo debe ser capaz de soportar el pago de cualquier cantidad inferior a la que el mprador tiene en su cartera sin necesidad de contactos adicionales con ninguna entidad.

· *Bajo nivel de fraude.* Idealmente el protocolo debería hacer imposible cualquier tipo de fraude, tanto procedente del comprador como del vendedor e intermediarios. En el caso de los micro-pagos ese objetivo puede resultar incompatible con el bajo coste y alta eficiencia imprescindibles. En todo caso el nivel de fraude debería mantenerse controlado y limitado. En el caso de los micropagos debería prestarse especial al fraude de vendedor, pues, potencialmente, cualquier usuario puede llegar a convertirse en un vendedor de información.

· *Estabilidad criptográfica.* La seguridad de los mecanismos criptograficos base del protocolo debería ser independiente del tiempo. Esta proporciona tranquilidad a los participantes, y redunda en un menor coste operativo.

· *Robustez frente a compromiso de clave secreta.* Esta característica mide lo crítico que pueda ser para cada uno de

los participantes la revelación (por descuido del usuario o rotura del criptosistema base) de una clave secreta.

· *Disponibilidad.* El protocolo debe ser poco dependiente de componentes o factores que puedan afectar la disponibilidad del servicio, tales como infraestructuras de red y autentificación.

· *Escalabilidad.* Es previsible que muchos servicios orientados al microcomercio sean utilizados por un gran numero de usuarios, por lo que la eficiencia no debe bajar notablemente con el aumento de éstos.

· *Bajo coste.* El sobrecoste asociado al sistema de pago ha de ser una fracción muy pequeña del valor del pago. Si suponemos pagos medios de 1 pts., el sobrecoste no debería ser superior a 0.01 pts..

· *Alta eficiencia.* Esta es una condición indispensable para garantizar un coste bajo y un retardo de servicio mínimo en condiciones de carga de trabajo alta.

· *Practicidad para el comprador.* El protocolo debe evitar que al comprador se le presenten con frecuencia situaciones que le lleven a costes adicionales "inesperados" o a una degradación o incomodidad en su uso. Por ejemplo, poca flexibilidad o lentitud a la hora de contactar con nuevos vendedores, perdida de valor adquisitivo como consecuencia por ejemplo de accidentes, etc.

· *Cobertura de pagos.* Idealmente y con objeto de reducir al máximo el número de protocolos distintos que el comprador precisa, los protocolos validos para micropagos deberian de valer también para pagos de mayor valor.

· *Protección contra difamación de vendedores.* El protocolo debe velar porque ningun usuario pueda difamar sin pruebas a un vendedor dada la perdida de negocio que ello podría representar para el vendedor.

Los anteriores son requerimientos orientados al protocolo de pago. Como requerimientos importantes mas orientados al "sistema" de micro-comercio y a su aplicación para pago de páginas Web, destacamos los siguientes:

· *Soporte de grupos de usuarios.* Para permitir niveles de descuento o acceso gratis a determinados mienbros o grupos o en determinados momentos.

· *Reutilización de paginas.* El vendedor debería implementar alguna politica que permitiese no pagar cada vez que se accede a la misma pagina.

· *Interfaz de usuario del comprador seguro.* Esta seguridad afecta tanto a la forma de implementar la cartera como a las páginas procedentes del vendedor. La cartera debería estar libre de código malicioso, ser infalsificable, ser configurable por el comprador en cuanto a topes de gasto por dia y por vendedor, etc. Las páginas, por ejemplo, deberían ser claras en lo que respecta a qué enlaces son de pago y cuales no.

· *Protección de derechos de autor.* La adecuada protección contra la copia y distribución y reventa ilícita de información, así como la protección de la "originalidad" de la información son aspectos que de no lograrse podrían tornar no disponibles muchos servicios en forma de microcomercio.

· *Alta Aceptabilidad.* Desde el punto de vista del comprador el sistema de microcomercio debería ser aceptado (estar implementado) por un gran numero de vendedores, lo que por otra parte puede contribuir a reducir el coste.

3. Sistemas de micropagos comerciales

Podemos contar en torno a 15 las diferentes propuestas orientadas específicamente a protocolos para micropagos. De éstas, sin embargo, prácticamente solo dos están emergiendo comercialmente, *Millicent* y *Minipay*. Agora [2], protocolo similar al *Minipay* diseñado en ATT, no ha pasado sin embargo de simple prototipo. Por otra parte, consideramos que protocolos como *E-cash* y sobre todo NetBill [1] aún cuando pueden ofrecer buen rendimiento, no cubren adecuadamente el tema de micropagos por requerir autorizaciones *on-line*. Otra de las propuestas que está cobrando cierta fuerza, es la de crear un esquema para incorporar micropagos sobre el **protocolo SET** de la que, por motivos de espacio, no presentaremos aquí los detalles "poco conocidos".

2.1. Millicent

Millicent [4] es un sistema de prepago con una filosofía de funcionamiento conceptualmente similar a la de las tarjetas telefónicas de prepago. La diferencia básica con éstas es que los *tokens* de pago no son hardware, sino cadenas digitales firmadas. Por lo demás, coinciden con aquellas en que los *tokens*, denominados *srip* (vales), son propios de cada vendedor y en que representan el saldo que a un comprador le queda disponible con un vendedor. Al igual que con las tarjetas de prepago, la seguridad del *Millicent* se basa en evitar que los *tokens* puedan ser falsificados o reutilizados varias veces, y, adicionalmente, en proteger contra su robo.

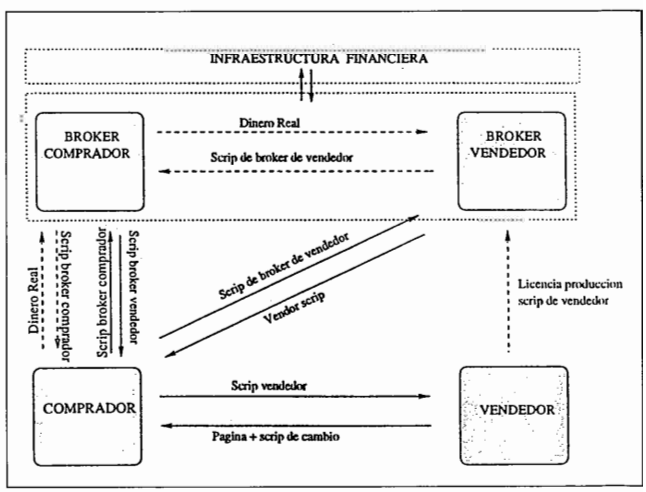


Figura 1. Sistema Millicent de DEC

El mérito fundamental del *Millicent* se basa en usar para esto solamente criptografía de clave secreta, con lo que consigue una gran eficiencia y el ideal de cero operaciones de clave pública.

Los participantes y protocolos del *Millicent* se detallan en la **figura 1**. De acuerdo con los autores la forma más normal de usar el Millicent es en una configuración con *brokers* de comprador y vendedor diferentes tal y como ilustra la **figura**, aun cuando el sistema puede funcionar de forma más sencilla con un solo *broker* común a comprador y vendedor.

Vales del Millicent. El *scrip*, vales o cupones, es el dinero del Millicent, propio o específico de cada vendedor. Cada vale actúa a modo de cuenta con saldo abierta con un vendedor y representa en cada momento el saldo que al comprador le queda disponible con un vendedor. La originalidad del Millicent reside en orientar la creación de vales de forma que la verificación de fraudes de gastos dobles, falsificación y robo sea muy rápida. Para prevenir la falsificación, los vales se acompañan de un certificado. Así, tal y como se ilustra en la *figura 2*, el *scrip* está formado por un cuerpo y un certificado sobre el cuerpo: *scrip* = *scrip_body* + *certificado_scrip*, siendo:

scrip_body = (*V_id,scrip_id, C_id,value,*exp*_time,props*)
$certificado_{scrip}$ = *hash* (*scrip_dody, Master_scrip,* sec *ret*)

siendo *V_id* el identificador del vendedor, *Value* el valor del vale, *scrip_id* el identificador del vale, *C_id* el identificador del comprador, *exp_tim* el periodo de validez del vale, y *Props* un campo opcional usado para incluir propiedades asociadas al comprador. El *certificado_scrip* es una "firma" MAC del vendedor sobre la pieza de *scrip* usando la clave maestra secreta de la serie de monedas *Master_scrip_secret_serie* (**ver figura**).

Por su parte, para prevenir el robo y posterior uso de los vales robados, los *vales* han de ser firmados por el comprador por medio de una clave secreta que el vendedor entrega al comprador (de forma *off-line*).

Producción de vales por el vendedor. Para poder vender, el vendedor contacta primero con un *broker* y negocia con él el servicio de distribución o venta de sus *vales* a sus posibles clientes. Esto puede hacerse básicamente de dos formas: o bien el *broker* compra, cuando se le agoten, *vales* al vendedor, o bien el vendedor licencia al *broker* la "capacidad" de producción de vales. Aun cuando, teóricamente, el Millicent no precisa de los *brokers*, en la practica recurre a ellos para descentralizar y descargar a los vendedores del proceso de venta de *scrip*, y como medio de centralizar para los usuarios la adquisición de *scrip* de múltiples vendedores.

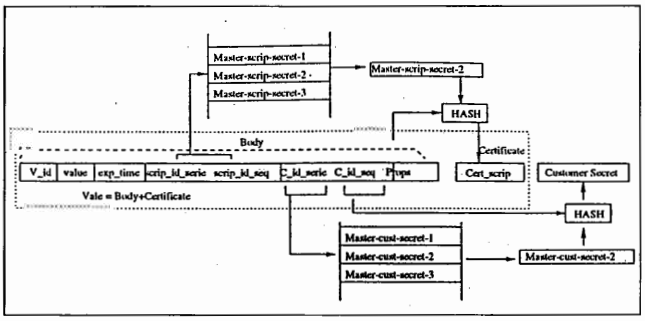


Fig ura 2. Creacion de vales, certificado y secreto de clientes en Millicent

Registro del comprador y compra de vales de *broker*. Un cliente que quiera usar el sistema debe registrarse inicialmente con un *broker* de su confianza (y al cual él sea confiable), vía el que obtener *vales* del vendedor (o vendedores) con los que quiera comerciar.

Con objeto de disminuir el número de interacciones del *broker* con el sistema de pago externo y así reducir costes, el *broker* realiza la venta de *vales* de vendedor a los compradores en dos pasos: (1) venta de *vales* de *broker* (*broker_scrip*), para lo cual el comprador ha de usar dinero "externo" al Millicent, y (2) venta de *vales* de vendedor (*scrip*), para cuya compra el comprador ha de usar *broker_scrip*. El paso (1) puede realizarse, en principio, con cualquier sistema de pago externo que el *broker* acepte, sea éste bien un medio de pago de comercio electrónico mas seguro tipo SET por ejemplo, o bien otro de comercio tradicional, por ejemplo cargo en tarjeta de crédito VISA.

Cada vez que se produce esta compra de vales de *broker*, el *broker* necesita, en principio, interactuar con el sistema externo, lo que puede ser lento y caro, con lo que interesa que el valor global de la petición de *broker_scrip* no sea pequeña. Con esto se reduce de paso el número medio de veces que el cliente necesita pedir más vales de *broker*, lo que también beneficia al cliente, aunque tenga que gastar una cantidad mayor cada vez que compra.

Compra de vales de vendedor. Esta compra se realiza cada vez que el cliente necesita vales para un vendedor particular bien porque no tiene ninguno, o bien porque el saldo de los que tiene es insuficiente para una compra(s). La información intercambiada, en el caso de un solo *broker*, es la siguiente:

C → *Broker: broker_scrip,V_id,cantidad*
C ← *Broker: scrip,broker_scrip',EKcb (costumer_secret)*

El cliente paga usando *broker_scrip*. El *broker* verifica la validez del *broker_scrip* recibido por el mismo metodo, descrito mas adelante, con el que el vendedor verifica el *scrip* recibido del cliente. Si el *broker_scrip* es válido, el *broker* deduce una pequeño porcentaje en concepto de tasas por transacción, y envia al cliente vales *scrip* del vendedor en la cantidad solicitada, y el cambio como moneda de *broker broker_scrip'* = *broker_scrip* - cantidad - tasa_trans. En este mensaje, el *broker* comunica también al cliente, si es la primera vez que se pide *scrip* del vendedor, el secreto de cliente *customer_secret* que el vendedor le tiene asignado. La encriptación *EKcb* (customer_secret) se realiza con la clave simétrica *Kcb* que el *broker* entrega al cliente cuando éste se registra.

En el caso del Millicent con dos *broker*s (**figura 1**), el funcionamiento es "parecido" al del caso con un solo *broker* salvo que el comprador obtiene *scrip* del vendedor contactando con el *broker* del vendedor previa compra a su *broker* de scrip de *broker* de vendedor.

Compra del servicio (al vendedor). El comprador adquiere el servicio del vendedor pagándole, normalmente, con un solo vale. La información que se intercambian en la compra es:

C → V: scrip,request, H (scrip, request, customer_secret)
C ← V: scrip',request, H (scrip',certificado_scrip,respuesta, customer_secret)

donde *respuesta* es la página solicitada o un error. Aquí *H(scrip, request, customer_secret)* representa la firma de gasto del *scrip*, basada en un MAC, sin la cual el pago no es aceptado. Así, los *vales* son enviados en claro, pero autentificados con una firma basada en el secreto *customer_secret* entre ese cliente y ese vendedor. Adicionalmente, el protocolo funciona como un protocolo de reto-respuesta (en donde *scrip'*, totalmente imprevisible para un oponente, funciona a modo de reto para la siguiente compra), por lo que el protocolo no es susceptible de ataques de reactuación.[1]

Sobre el *scrip* recibido, el vendedor verifica (1) que no haya expirado, (2) que no sea falsificado, (3) que no se haya usado previamente, y (4) que no sea robado, es decir, que la firma de gasto corresponda al usuario dueño de la moneda. Esto es, aunque los *vales* son transmitidos en claro, eso no significa que el ladrón pueda usarlos aunque los capture, ya que para ello ha de conocer el secreta *customer_secret*, que no es enviado en claro en los mensajes intercambiados.

Si el valor del *vale(s)* recibido(s) es superior al coste del servicio (lo que ocurrirá prácticamente siempre), el vendedor ha de devolver un *vale* de cambio por la diferencia. En el mensaje de respuesta, *certificado_scrip* es el certificado asociado a *scrip* (no al *scrip'*) y se utiliza para que el comprador puede verificar que la respuesta es la asociada a la petición (*request*). El vale de cambio *scrip'* tiene un nuevo valor (inferior) y numero de serie distinto al de *scrip*.

Autenticidad y eficiencia de los pagos. Como puede observarse, el Millicent basa la autenticidad de los pagos en un esquema de clave simétrica. El vendedor da a cada comprador una clave secreta *customer_secret* de gasto,que le permita firmar (de forma simetrica), y por tanto autentificar, cada gasto que realice. Por otra parte, y con objeto de evitar el crear una gran base de datos con las claves de todos los usuarios, la generación de cada clave *customer_secret* no se realiza de una forma aleatoria, sino mediante un *hash* del identificador único de cada cliente *C_id*, y de un secreto maestro de cliente *Master_customer_secret* (distinto al usado para firmar el *scrip*) (**figura 2**). Este esquema ofrece dos ventajas: (1) La obtención del *customer_secret* necesario para verificar cada pago se puede realizar muy rápido ya que puede obtenerse a partir del *scrip* recibido y de una pequeña tabla de secretos maestros de cliente, sin necesidad de realizar ningun (lento) acceso a una base de datos que podria alcanzar un tamaño considerable. (2) Se incrementa la eficiencia y seguridad del sistema pues no hay que almacenar y proteger una gran base de datos de secretos de cliente.

Evaluación del Millicent autentificado sin encriptación. Millicent presenta las siguientes características relevantes:

· *Anonimidad media.* Se suponen canales anonimos entre los participantes. Suponiendo que la relación entre el *C_id* y la identidad real del comprador es únicamente conocida por el *Broker* y que el *scrip* no revela ningun dato comprometedor para el comprador, el comprador es intrazable para observadores y vendedores. Claramente, sin embargo, el comprador es totalmente trazable por el *broker*. Esta desventaja es suplida por los autores via tres vías: (1) El *broker* es confiable en que respetará la anonimidad del comprador salvo requerimiento judicial. (2) Trabajando con esquemas de dos *broker*s. Bajo esta situación, el *broker* de vendedor no conoce la identidad real del comprador (el comprador solo le proporciona su identificador, pero el *broker* de vendedor como no tiene una cuenta con el comprador, no es capaz de averiguar la identidad real del comprador asociado al identificador). (3) Via la utilización de un esquema totalmente anónimo tal como el **E-cash** para la compra inicial de *scrip* de *broker*.

Otra pequeña desventaja es que los pagos entre el mismo comprador y vendedor son todos enlazables puesto que incluyen siempre los mismos identificadores de vendedor y comprador. Mas aún, los pagos con distintos vendedores son enlazables, pues el *C_id* que el *broker* pone en el *scrip* coincide entre vendedores distintos.

· *Anonimidad controlada por broker.* La desventaja anterior permite que el *broker* pueda controlar la anonimidad de sus usuarios aunque, idealmente, la anonimidad debiera controlarse por agente distinto al concesor de crédito o dinero.

· *Exportabilidad.* Millicent no usa encriptación salvo cuando el comprador compra vales de un vendedor nuevo, en cuyo caso el *broker* le pasa el *customer_secret* encriptado *EKcb(customer_secret)*. Esto podría verse como una violación de las reglas de exportación sobre encriptación, pero estas reglas permiten la encriptación de PINs, y los *customer_secret* son esencialmente PINs. De hecho, el Millicent tiene una licencia de exportación que le permite encriptar los *customer_secret* con claves Kcb de 128 bits.

· *Divisibilidad practicamente ideal.* Millicent es un esquema intrínsicamente divisible ya que el *scrip* puede ser utilizado en cualquier cantidad igual o inferior al valor que representa. Aun así, el correcto funcionamiento de la divisibilidad depende de la confianza en el vendedor asi como del buen funcionamiento de la máquina del vendedor y del canal entre comprador y vendedor. Sin embargo, puesto que con cada vendedor se tiene un *scrip* diferente, un

problema en la obtención de cambio de un vendedor no afecta a los demas vendedores.

· *Alta Estabilidad criptográfica.* La criptografía del Millicent está basada únicamente en funciones *hash* con clave. La seguridad de estas funciones se basa en la imposibilidad práctica de invertir la funcion *hash* y de computar en un tiempo razonable el espacio de claves asociado a la longitud en bits de la clave. Para valores de longitud de clave del orden de los 128 bits y funciones *hash* como MD5, como son las usadas por el Millicent, estas dos posibilidades pueden considerarse totalmente impracticables tanto actualmente como durante bastantes años. Por otra parte, cambios en la longitud de las claves no suponen pérdida de rapidez del protocolo.

· *Alto control de fraudes de comprador*

1) Imposibilidad de gastos dobles. Los gastos dobles (del mismo vale) con otro vendedor son imposibles por ser el *scrip* especifico de cada vendedor. Los gastos dobles con el mismo vendedor son controlados por éste mediante el chequeo del numero de serie y la fecha de expiración de cada vale.
2) Infalsificabilidad de vales. Criptográficamente la falsificación depende de la robustez de las funciones MAC, las cuales, como se citó antes, ofrecen seguridad máxima. Otra vía para la falsificación sería el conocimiento de uno de los secretos *Master_scrip_secret_serie*, por lo que la privacidad práctica de estas claves resulta crítica para el vendedor.
3) Protección contra robo de scrip. El robo de *scrip* se protege mediante la firma de gasto. Es decir, el ladron, para poder comprar con el *scrip* robado, necesita adicionalmente el secreto *customer_secret*.

· *Riesgo mínimo ante compromiso del customer_secret con un vendedor particular.* El compromiso de un *customer_secret* es (mínimamente) problemático si adicionalmente el ladrón es capaz de obtener *scrip* no gastado, vía, por ejemplo, la interceptación de pagos entre comprador y vendedor o la compra de *scrip* de vendedor entre comprador y *broker*. El riesgo, en este caso, es pequeño ya que el *scrip* solo le es valido al ladron para un vendedor. Suponiendo un máximo de *broker_scrip* en cartera de 7000 pts. y que por vendedor se admita un máximo de 500 pts., el riesgo máximo serían 500 pts.. Por otra parte el problema es de facil detección para el comprador.

· *Riesgo medio-bajo ante compromiso del customer_secret con el broker.* En este caso el riesgo máximo para el comprador se alcanza, cuando el ladrón es capaz de interceptar, adicionalmente, la transacción inicial de compra de vales de *broker* de comprador. Obsérvese que si inmediatamente después de esta interceptación el ladrón compra *scrip* de un vendedor cualquiera, al comprador le será imposible utilizar su *broker_scrip*, ya que el saldo que representa ha sido modificado por el *broker* como consecuencia de la compra realizada por el ladron. El riesgo en este caso sería el valor máximo que el sistema permita para la compra inicial (por lo que conviene que ésta no sea alta). El problema es de facil detección para el comprador pero de dificil solución.

· *Gran dificultad de compromiso del Master_scrip_secret de un vendedor.* Esta revelación crea problemas si el ladrón consigue hacerse también con el secreto *Master_customer_secret*, pues, de lo contrario, todas las firmas de gasto que se hagan con el *scrip* fraudulentamente generado no serían aceptadas por el vendedor. Esto supone un reto adicional al ladrón. Además, el ladron necesitaría obtener el valor en curso del siguiente numero de serie de *scrip* a usar y ser capaz de alterarlo adecuadamente en la máquina del vendedor (alterando el mapa de bits) para que la compra con *scrip* falsificado colase. Todo ello lleva a que la posibilidades de éxito para el ladrón podamos considerarlas nulas.

· *Alta Eficiencia. Millicent* alcanza una gran eficiencia tanto de almacenamiento como computacional. En cuanto almacenamiento, puesto que los *scrip_id* son asignados de forma consecutiva por el vendedor al Millicent, usando un mapa de bits, le basta con un solo bit para registrar si un determinado *scrip* ha sido o no gastado. Así, suponiendo *scrip* de duración 1 mes y una media de 3 gastos de *scrip* diarios por comprador, un sistema con 1 megabyte de memoria RAM seria capaz de soportar 100.000 compradores. El sistema puede incluso ser mas eficiente cuando se preveen transacciones repetidas del mismo comprador. En este caso el vendedor asignaría identificadores de *scrip* con m bits extra al final, con los que se podrían representar 2exp(m) transacciones.

Por otra parte, y puesto que no se necesita autorización, la verificación del pago es extraordinariamente rápida ya que únicamente requiere 4 operaciones *hash* y la verificación anterior para chequeo de scrip duplicado. Adicionalmente, la excepcional eficiencia hace que el vendedor sea difícilmente atacable por sobrecarga de mensajes.

· *Escalabilidad aceptable.* A esto contribuyen su naturaleza descentralizada en el sentido de que no necesita de una autoridad central que valide el dinero evitando de esta manera la necesidad de una gran base de datos en el *broker*. Sin embargo, la escalabilidad del esquema de claves asociado a la autentificación simétrica es asumible siempre que el número de *brokers* no crezca excesivamente (en el modelo con 2 *brokers,* el cliente necesita una clave secreta con cada *broker* de vendedor con el que contacte lo que al final redunda en cierta complejidad en cuanto a número y gestión de las claves simétricas usadas, tanto desde el punto de vista del comprador como de su *broker*). Una ventaja en este sentido es que las relaciones inter-*brokers* son escasas, por lo que el crecimiento del numero de *brokers* influye menos.

Algunos inconvenientes del Millicent son los siguientes:

· *Transacciones repudiables/irresolución de disputas.* La autenticidad de las transacciones basada en un esquema de clave simétrica provoca que el Millicent no pueda proporcionar una no-repudiación correcta. Esto lleva a que la

resolución de disputas de gasto entre el cliente y el vendedor sea teóricamente imposible. Dos situaciones irresolubles son:

a) Comprador deshonesto. Un comprador deshonesto da copias de su secreto y *scrip* a un amigo para que éste gaste. Posteriormente se queja públicamente de que su *scrip* está siendo injustamente rechazado por el vendedor, alegando que el vendedor ha revelado su secreto y *scrip* a un amigo.

b) Vendedor deshonesto. Los vendedores pueden defraudar diciendo simplemente que en *scrip* válido ya esta gastado e incluso presentar una 'prueba' falsificada (pues conocen los secretos de sus clientes). De hecho el vendedor puede generar por si solo (o pasándo el secreto a un amigo) pagos de cualquier usuario a su favor. Aunque estos pagos ya están cobrados, (el sistema es de prepago) eso le permitiría obligar a muchos clientes (eligiéndolos sin relación entre ellos) a comprar nuevo *scrip* de vendedor, con lo que podría obtener un gran beneficio en poco tiempo. Aun cuando es posible que el sistema filtre o elimine a medio o largo plazo a los vendedores que defraudan, ello no prohibe que de repente un vendedor hasta ese momento honesto cometa fraude repentino que podría llegar a ser significativo.

· *Escasa practicidad en algunas situaciones. Millicent* puede presentar problemas de practicidad debido a dos razones: (1) a la dinámica de compra sobre el Web cuando se trata de pequeñas cantidades. Esta lleva a que el numero medio esperado de vendedores que el cliente contacta (ocasionalmente o no) a corto (o medio) plazo asi como el número de vendedores nuevos, sea probablemente grande, (2) por el hecho de usar monedas especificas de vendedor, lo cual implica que el *scrip* de un vendedor no puede ser usado con otro. Esto puede traer como consecuencias:

(1) El usuario, con objeto de recuperar *scrip* no usable o de valor ínfimo, tiene que preocuparse u ocuparse cada cierto tiempo en determinar si el *scrip* que tiene de cada vendedor le sigue siendo util. Esto, aparte de restarle tiempo, en ocasiones puede no saberlo ni el mismo.
(2) Cada vez que el cliente quiere acceder a un nuevo vendedor debe contactar previamente (*on-line*) con el *broker* para obtener los *vales* adecuados. Esto limita también su aplicabilidad en entornos donde se crean con cierta frecuencia enlaces con nuevos vendedores.
(3) Incremento de coste. El numero medio de veces que el cliente necesita contactar con el *broker*, bien para conseguir nuevo *scrip* o para recuperar el valor de *scrip* no usable, puede aumentar notablemente con respecto a esquemas en los que la misma moneda es válida para todos los vendedores (asumiendo que el cliente paga al *broker* por el servicio de 'redención').

El cliente podría resolver este problema comprando *scrip* de vendedor en cantidad suficiente para un plazo largo. Sin embargo, ya que, salvo en algunos casos, el cliente desconoce *a priori* la cantidad de gasto, a corto y medio plazo, que espera realizar con cada vendedor, esto podría llevarle a tener en cartera cantidades relativamente grandes y poco usables. Esto, además, va en contradicción con el Millicent real, en el cual, por motivos de seguridad asociados a pérdida o robo de cartera, la cantidad total de *scrip* en cartera está limitada a alrededor de 7000 pts. ($50).

· *Scrip expirable.* El perido de expiración del *scrip* es estimado por los autores entre uno y dos meses. Este tiempo podria ser aceptable si no fuese por el hecho de que el *scrip* de cada vendedor es distinto. Ello lleva a que si el numero de vendedores por comprador es alto, éstos han de preocuparse diariamente por la renovación de alguno de su *scrip* y de aquí a incurrir en un gasto de comunicaciones adicional indeseado.

· *Diversidad de claves.* Puesto que el cliente usa claves secretas distintas para cada vendedor (y con cada *broker* intermediario con el que trate), a medio o largo plazo puede empezar a tener en su cartera gran numero de claves secretas. Esto no necesariamente tiene porqué representar un problema grave, pero obliga a que el programa de cliente realice una gestión (automatica) cuidadosa. Por otra parte, al ir aumentando el numero de claves, el programa de cartera podría bajar de rendimiento causando al cliente esperas indeseadas. Si la cartera se implementa de forma que las claves secretas se obtengan de una tarjeta inteligente, esto podría suponer un problema añadido y ralentizar algo el pago.

· *Robo (o copia) de cartera.* El comprador podría perder, en este caso, hasta el total de *scrip* en ese momento en cartera, (suma de *scrip* de vendedores y *brokers*).

· *Bajo Control de fraudes de vendedor.* El sistema no provee ninguna forma para prevenir fraudes de entrega de páginas vacias o incorrectas del vendedor. Además, puesto que las páginas no van firmadas (al menos en tiempo real), el vendedor siempre puede negar su envio. Por la misma razón, el comprador no puede quejarse a una tercera entidad pues podría difamar injustamente al vendedor. El único recurso del comprador es cancelar su relación con el vendedor (el vendedor, sin embargo, gracias a la rapidez de las funciones *hash,* podría recurrir al uso de firmas MAC con el *customer_secret,* para proporcionar un mínimo de autentificación para las páginas).

· *Incompatibilidad con otros esquemas.* Millicent es un sistema que difiere totalmente de cualquier otro esquema de pago conocido y por tanto difícilmente compatible con esquemas de pago para cantidades mayores que logren aceptación. Asimismo, dada su aproximación basada en clave simétrica, difícilmente puede extenderse para su uso en pagos mayores (compárese por ejemplo con la versatilidad que ofrecería un esquema de micropagos basado en SET).

Estado de implementación. Millicent está actualmente en fase experimental proporcionando una cartera, un *broker* y un vendedor de ejemplo para todo aquel interesado (no está todavia disponible comercialmente). Para más Información acerca de como cargar la cartera y experimentar con Millicent ver *http://www.millicent.digital.com/*

3.2 Minipay (*IBM Micropayments*)

El sistema *Minipay* [3] es un sistema de crédito tradicional que trabaja contra una infraestructura de *broker*s y/o bancos. Su aproximación a los micropagos, para conseguir eficiencia y seguridad, consiste en tratar de eliminar, en la medida de lo posible, la autorización *on-line* del pago típica de los sistemas de crédito. Para ello el *Minipay* propone:

1) Control de la autorización de compra de cada usuario, vía concesión de certificados diarios.
2) Limitación de la cantidad diaria que el usuario puede gastar con cada vendedor.
3) Autorizaciones *off-line*, salvo cuando el usuario sobrepasa el límite anterior, en cuyo caso el vendedor contacta con el concesor de crédito para determinar si debe o no dar el pago por bueno.

Criptográficamente, el *Minipay* usa firmas digitales, asumiendo que, con la tecnología actual de procesadores, la carga que supone la validación de las firmas digitales en el vendedor no supone ningun cuello de botella cuando se trata de aplicaciones de compra de páginas Web, pudiendo, por tanto, dar servicio a un gran número de compradores.

Las entidades y protocolos en *Minipay* se ilustran en la **figura 3**. Los *broker*s de comprador y vendedor se le designa **IAP (Proveedor de Acceso a Internet)** e **ISP (Proveedor de servicio Internet)**, aun cuando el papel de *broker* puede ser desempeñado directamente por bancos, compañías telefónicas, grandes compañías de servicios, etc.

Protocolo de Registro. Inicialmente, el **IAP** proporciona al comprador, de forma *off-line*, una cuenta *acct_C* y un código secreto *code_C*. El registro tiene lugar cuando el comprador quiere asociar una clave pública a su cuenta *acct_C*. Para ello el comprador genera primero la pareja de claves pública y privada (*PKc, SKc*), y luego ejecuta el siguiente protocolo con el **IAP**:

$C \rightarrow IAP: K_c, Sig_c (reg\_request, H(code_c, salt1, Kc, acct_c, t)), salt_1, t$
$C \leftarrow IAP: Sig_{IAP} (reg\_reponse, code\ error, acct_c, K_c, t, fees)$

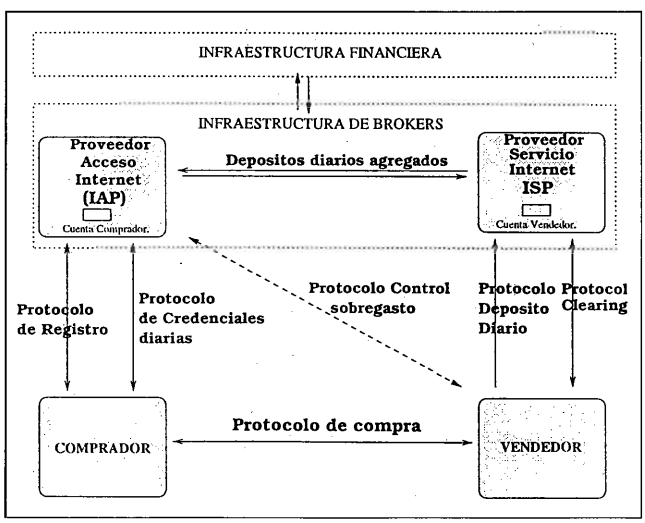


Fig 3. Sistema Minipay de BM

donde *salt_1* es un valor aleatorio usado para proteger al secreto *code_C* de ataques de adivinación; t es el tiempo en el reloj local del comprador, y su uso, al igual que en el resto de protocolos del *Minipay*, es el típico de protección, basada en sellos de tiempo, contra la reactuación; y *fees* son las tasas por transacción impuestas por el **IAP** las cuales son añadidas automáticamente, por el agente de cartera, al coste del servicio del vendedor, en el momento del pago.

Obtención diaria de credenciales. Este protocolo es lanzado por el comprador una sola vez al principio de cada día y tiene por objeto el proporcionar al usuario un certificado diario de credibilidad de pago, autorizandole a (re)utilizar la clave SK_c para firma de compras. La información intercambiada es:

$C \rightarrow IAP: K_c, Sig_c (Daily\_Request, balance, Kc, acct\_C, t)$
$C \leftarrow IAP: total\_lim, salt, real\_bal, Daily\_Cert$
donde *Daily_Cert_C* es el certificado diario de autorización de compra, dado por:

$Daily\_Cert_c = Sig_{IAP} (Daily\_resp, Kc, T, rec\_offline\_lim, H(total\_lim, salt, real\_bal))$

donde *balance* representa la cantidad total gastada el dia anterior por el usuario, *total_lim* el maximo gasto diario (entre todos los vendedores) que el usuario puede hacer y usado para controlar gastos extra del usuario, y *rec_offline_lim* el gasto máximo por vendedor. Tanto *real_bal* como *total_lim* no se incluye en el certificado por privacidad evitando que los vendedores (a quienes se envía el certificado) conozcan el gasto real de los compradores.

Compra. Comprador y vendedor intercambian a la compra la información siguiente:

$$\overbrace{\qquad\qquad}^{Orden\ Pago}$$
$C \rightarrow V: Daily\_Cert_c, Sig_c (Order, amount, day\_total, acct_c, t, Url, acct_V)$
$C \leftarrow V: pagina / error$

donde *day_total*, es la cantidad total gastada por el comprador durante el día, con ese vendedor, incluyendo la compra en curso. Si la cantidad *amount* es superior al saldo en la cartera, el agente de cartera no realiza el pago. *t* es el instante de la compra y sirve también como identificador de la transacción.

El vendedor: 1) Verifica la validez del certificado *Daily_Cert* (se supone que el vendedor ha obtenido previamente la clave pública del IAP), comprobando la firma del IAP en el certificado, y la validez del certificado de clave pública del IAP; 2) Verifica la firma del comprador en la orden de compra *OrdenPago*; 3) Chequea el tiempo *t* como protección contra reactuación de mensajes; y 4) Comprueba que el gasto diario total del comprador con el vendedor, sea menor que el limite *offline_lim*. Si no es así, ejecuta el protocolo de control de sobregasto.

Control de sobregasto. Este protocolo es lanzado por el vendedor bajo dos situaciones: (1) si el comprador gasta por

encima del valor *offline_lim* con ese comprador durante el día, y (2) si el importe del pago supera un cierto valor, por ejemplo 100 pts.. La información que se intercambian V e IAP es:

$V \rightarrow IAP: Sig_V(Extra\_req, OrdenPago)$
$V \leftarrow IAP: Sig_{IAP}(Extra\_resp, error\_code, acct_c, K_c, amount, acct_V$

donde *amount* es la cantidad extra autorizada por el IAP para ese vendedor específico.

Deposito de los pagos. Cuando el vendedor desea realizar el depósito de las ordenes de pago ejecuta:

$V \rightarrow ISP: Sig_V(t, OrdenPago_1, OrdenPago_2, ...)$
$V \leftarrow ISP: Sig_{ISP}(t, OrdenPago_1, OrdenPago_2)$

La firma de vendedor sirve de prueba, para el banco, de que el vendedor ha realizado el depósito. Recíprocamente, la firma del ISP en el mensaje de respuesta es una prueba para el vendedor de que el mensaje de depósito se ha recibido y de que es válido, evitando de esta manera repudiaciones de depósito por parte del ISP.

Compensación de pagos. Cuando el vendedor desee proceder al cobro de los pagos ejecuta el siguiente protocolo:

$V \rightarrow ISP: Sig_V(Clear\_req, t, time\_of\_last)$
$V \leftarrow ISP: Sig_{ISP}(Clear\_resp, t, amount, rejeted_1, reason_1, ...)$

siendo time_of_last es el instante de la última petición de cobro (con respuesta aceptada); *amount* la cantidad total realmente abonada al vendedor; *rejected_1*, *reason_1* ..., las órdenes de pago rechazadas con la razón de rechazo (p.e., el comprador no tiene mas crédito disponible); y *pending_1*,... la lista de ordenes aún pendientes de aprobación.

Certificación y distribución de claves públicas. *Minipay* no depende de ninguna infraestructura externa de clave pública, definiendo, en su lugar, una organización casi plana de confianza. Las claves de los compradores son certificadas por su *broker*. Por su parte, las claves de cada *broker* son enviadas a los demás *broker*s y a los vendedores, por medio de un protocolo especial denominado protocolo de encaminamiento de claves públicas. Este protocolo se ejecuta periódicamente en cada *broker* y distribuye todas las actualizaciones y nuevas claves públicas que haya registrado. Cara a los micropagos, la ventaja de este esquema es clara, pues permite eliminar la ineficiencia en el vendedor derivada de las consultas en tiempo real a la infraestructura cuando un vendedor recibe una clave pública desconocida.

3.3. Evaluación del Minipay. Algunas caracteristicas relevantes del Minipay son:

· *Anonimidad media.* La anonimidad del comprador depende en última instancia, de la calidad anónima de los *valores acct_C, Kc* y certificado asociado, en el sentido de que estos no guarden ninguna relación con la identidad real del cliente. Bajo estos supuestos el cliente es intrazable para observadores y vendedores. La anonimidad con *broker* IAP parece mas problematica, ya que puede romperse con el protocolo de sobregasto. Efectivamente, mantener esta anonimidad implica que el IAP no pueda obtener la identidad del vendedor ni a partir de su certificado de clave pública *Cert(Kv)* ni de su cuenta *acct_V*. Lo primero depende del esquema de certificados. Lo segundo depende de que IAP e ISP no sean la misma entidad, y de que guarden adecuados convenios de privacidad entre sí. Además esta privacidad puede ser rota por la inclusión del *Url* del vendedor (que en principio lo identifica plenamente) dentro de las ordenes de pago *OrdenPago,* ya que éstas son enviadas tal cual por el ISP al IAP. Para mejorar la anonimidad los autores proponen (1) uso de cuentas temporales, (2) privacidad ante el IAP de la identidad del vendedor en el protocolo de depósito, cuando éstas solucionan solo parcialmente el problema anterior. Por otra parte, los pagos de un comprador son totalmente enlazables, ya que todos contiene el mismo *acct_C*. Esto puede mejorarse, parcialmente, si se introduce la mejora consistente en cuentas temporales.

· *Anonimidad controlada por broker.* El control de la anonimidad se logra por el hecho de la confianza depositada en el IAP sobre la identidad del usuario.

· *Divisibilidad total.* El *Minipay* es un sistema totalmente divisible, ya que está basado en transacciones de crédito.

· *Estabilidad criptografica media.* La seguridad del *Minipay* está basada en firmas digitales RSA, por lo que en realidad la estabilidad dependerá de la longitud real de las claves usadas. Es previsible que, de acuerdo con lo que ha venido sucediendo en el pasado, cada cierto tiempo haya que variar la longitud de las claves RSA para hacer frente a nuevos avances tanto en el área de procesadores y memorias, como en el área de algoritmos de factorización. En el caso del *Minipay*, esto provocará cambios en los certificados de los participantes. Como medida preventiva mínima, todo el software que gire alrededor del sistema *Minipay* debería ser configurable en cuanto a longitud de la clave RSA. Asimismo, las longitudes de clave asociadas con los *brokers* deberían tener la longitud suficiente como para contrarrestar durante un tiempo considerable el efecto del progreso tecnológico. Por otra parte, los cambios en las longitudes de clave afectan fundamentalmente a la máquina del comprador, pues el tiempo de verificación apenas varía.

· *Exportabilidad.* El *Minipay* es totalmente exportable ya que no usa ningún mensaje encriptado, y las firmas digitales basadas en el RSA no están sujetas a controles de exportación por el gobierno USA.

· *Eficiencia aceptable.* Criptográficamente el protocolo requiere en el vendedor la verificación de una o dos firmas y del certificado de clave pública del IAP. Puesto que la verificación de firmas en un equipo normal Pentium 200 es no mayor de 4 mseg., el proceso criptográfico no supone ningún cuello de botella real en aplicaciones de envío de

paginas Web. En caso de gastos sobre el límite, en los que el vendedor ha de ejecutar el protocolo de control de sobregasto, el vendedor debe realizar una firma y verificar la firma en la respuesta del IAP. Ya que estos casos no es probable que sean abundantes, y puesto que la firma RSA-768 lleva unos 50 mseg., es poco probable que estos casos reduzcan notablemente la eficiencia en el vendedor. Por otra parte, el protocolo no requiere accesos a base de datos, salvo el necesario para la velidación del certificado del IAP que puede realizarse cada vez que se recibe por via el protocolo de distribución de certificados. Adicionalmente, y para mejorar la eficiencia en caso de gastos sobre el límite, y cuando el IAP está lejos del vendedor y cerca del comprador, se puede dotar al comprador de la posibilidad de contactar primero con el IAP para que autorize el pago, en cuyo caso el vendedor ya no tendría que lanzar el control de sobregasto.

· *Escalabilidad.* El vendedor no necesita una base de datos con los certificados de cada comprador ya que los está recibiendo permanentemente en los mensajes de compra. Por otra parte la base de datos de certificados de los brokers es relativamente pequeña y escala adecuadamente. El crecimiento de numero de *brokers* escala con complejidad de comunicaciones de $O(n^2)$, ya que cada nuevo *broker* puede que comunique con todos los demás diariamente.

Algunos inconvenientes (relativos) del *Minipay* son:

· *Bajo control de fraudes de vendedor.* El vendedor no puede alterar los importes pagados ya que van firmados por el comprador, ni realizar depósitos duplicados. Sin embargo, no se provee forma alguna de prevenir fraudes de entrega de paginas vacías o incorrectas del vendedor. Además, como las páginas no van firmadas (al menos en tiempo real), el vendedor siempre puede negar su envío. Por la misma razón, el comprador no puede quejarse a una tercera entidad pues podría difamar injustamente al vendedor. El único recurso del comprador es cancelar su relación con el vendedor.

· *Control medio de fraudes de comprador.* Aunque el *Minipay* no usa identificadores de transacción, los gastos dobles con el mismo vendedor es posible controlarlos vía el tiempo *t*. Sin embargo, un vendedor puede defraudar comprando con cada uno de por ejemplo 1.000 vendedores por debajo del valor *rec_offline_lim*. La linea de defensa contra este fraude consiste en reducirle al comprador su limite *rec_offline_lim* para el día siguiente, o simplemente no renovarle el certificado mientras no abone el gasto extra. En todo caso, el vendedor sólo perdería hasta el valor *rec_offline_lim*. El fraude total depende de si el comprador es capaz de alterar el software de cartera, ya que ésta controla que el gasto máximo diario no exceda la cantidad *total_lim*. En cualquier caso el fraude es visto por el *Minipay* como un riesgo del vendedor, es decir, el *broker* o banco no corre con el riesgo. Por otra parte, este problema es parcialmente solucionable con métodos de autorización probabilística[2].

· *Robo (o copia) de cartera (Riesgo comprador).* En este caso, y si el ladrón conoce también el PIN de acceso, el ladrón puede gastar gratis hasta el valor *total_lim* o más si es capaz de alterar el comportamiento de la cartera. El ladrón podría obtener certificados diarios directamente del IAP. En el caso de copia de cartera (ésta no esta implementada total o parcialmente sobre tarjeta inteligente) el problema es menos observable para el comprador pudiendo el ladrón gastar durante varios días antes de ser detectado.

· *Protección media ante compromiso de la clave privada del comprador (Riesgo comprador).* El ladrón necesitaría adicionalmente el certificado diario, pero éste es fácil de conseguir pues no es privado (es observable por los vendedores). El gasto máximo 'gratis' realizable por el ladrón podría llegar a ser grande ya que no necesariamente está limitado por el valor *total_lim* (en algunos países este riesgo del cliente está limitado por imposiciones legales).

· *Protección media contra compromiso de clave privada de un IAP (Riesgo IAP).*En este caso el ladrón podría crear tantas cuentas *acct_T* y certificados diarios válidos como quiera. La magnitud del gasto 'gratis' que consiga dependerá de la habilidad del IAP en detectar el problema. Por otra parte, puesto que es lógico suponer que la responsabilidad en este caso sea del IAP y que los vendedores reclamen al IAP el importe de las ventas, el IAP podría llegar a sufrir una notable pérdida económica.

Implementación. *Minipay*, producto desarrollado por IBM Israel, se encuentra actualmente en fase beta experimental, esperándose una primera versión comercial a principios del tercer cuatrimestre de 1998. Su implementación así como los resultados experimentales proporcionan las siguientes características:

- Firmas digitales basadas en RSA.
- Cuentas de pre-pago o post-pago.
- Compras máximas por día limitadas por IAPs o ISPs en torno a 4000 pts. ($25-30).
- Incremento de coste por enlace para amortizar los costes introducidos por el sistema *Minipay*, estimado en torno a 1 pts. para vendedores con poca actividad y 0.001 pts. para vendedores con gran volumen de ventas de enlaces/día.
- Tarifas estimadas para el IAP e ISP de alrededor del 1% del coste de la transacción.
- Precios dinámicos. Los precios de los enlaces de pago pueden determinarse dinámicamente mediante una función.
- Protección de la propiedad intelectual mediante el esquema distribuido *Cryptolope* de IBM.
- Interfaz de usuario con enlaces de pago claramente identificados para evitar que el vendedor engañe al usuario.
- Cartera de comprador implementada como *plug-in*, en lugar de con *applets*, debido a la inseguridad que plantea el enfoque actual (java versión 1.0) de *applets* cargados desde el servidor.

4. Conclusiones

Tanto *Millicent* como *Minipay* son aproximaciones válidas para micropagos por su bajo coste y alta eficiencia. *Millicent*

destaca por su excepcional eficiencia, que le hace incluso válido para aplicaciones de 'nanopagos', y ausencia de fraudes siempre que las claves se mantengan seguras. Su punto más debil es la escasa practicidad cuando el usuario necesite contactar con nuevos vendedores y que parece difícil de extender a pagos de mayor cuantía. Por su parte el *Minipay* puede extenderse sin excesiva complejidad a pagos mayores, aunque la incorporación de un esquema ad-hoc de distribución de certificados, aún teniendo una repercusión positiva sobre la eficiencia, puede jugar en contra de esa facilidad de extensión. Por otra parte, queda por ver si la aproximación de control de sobregasto es suficiente para limitar el fraude de comprador. En cuanto a la firma de las páginas en tiempo real, ésta parece más practicable (actualmente), dado el esquema de criptografia simétrica, en *Millicent* que en el *Minipay*.

Referencias

[1] J.Tygar. B. Cox, y M.Sirbu. Netbill security and transaction protocol. *Proceedings First USENIX Workshop on Electronic Commerce*, 1995.

[2] E. Gabber y A. Silberschatz. Agora: A minimal distributed protocol for electronic commerce. Bell Laboratories. *http://www.bell-labs.com/ eran/ agora.html*, 1996.

[3] Amir Herzberg y Hilik Yochai. *Mini-pay: Charging per click on the web*. Network Computing and Security Group, IBM Research-Haifa, 1996.

[4] Mark S. Manasse. The millicent protocols for electronic commerce. DEC Systems Research Center. *http : //www.research.digital.com/SRC/ people/MarkManasse/*, 1995.

Notas

[1] Al contrario que en otros protocolos, en *Millicent*, la firma de gasto se puede aplicar a más de un *vale*. Es decir, si, para cubrir la cantidad a pagar, el comprador necesita enviar varios *vales*, no es necesario firmar cada uno de esos *vales* separadamente, sino que basta con una sola firma sobre todos los vales. El pago en este caso es, incluye un *governing_secret* en lugar de un *customer_secret*, donde el *governing_secret* se construye mediante el *hash* de los *customer_secrets* de las piezas de *scrip*, clasificados, representados de forma canónica y concatenados.

[2] Agora [2], un protocolo parecido al *Minipay,* resuelve este problema usando autorización *off-line* probabilística.

Agradecimientos

Expresamos nuestro agradecimiento a Mark Manasse de DEC y Amir Herzberg de IBM por las aclaraciones realizadas acerca del funcionamiento del *Millicent* y *Minipay* respectivamente.

/DOCS/

Rentabilidad de las inversiones en TI y complejidad *

Felipe Gómez-Pallete
Consultor
fgpallete@globalnet.es

Sobre este objeto de estudio -la renta bilidad de las inversiones en las así llamadas tecnologías de información- se han escrito, se escriben y se continuarán escribiendo innumerables trabajos de todo tipo, técnicos, económicos o filosóficos, elaborados por y para especialistas, así como en clave divulgativa. Acaso sea la dificultad que entraña el estudio de este asunto el único rasgo común a todos ellos. Por ello, esta enésima contribución comienza por indagar en las causas de esta dificultad que nadie discute, causas que aquí se presentan agrupadas en cuatro categorías o tipos.

Una dificultad contra la que nada podemos hacer

La rentabilidad de las inversiones que a diario se realizan en las TI es un asunto complejo. La *complejidad* es una característica intrínseca de este objeto de estudio y, por tanto, se trata de un rasgo *ontológico*, es decir, inherente al propio ser del objeto.

Decimos, en una primera aproximación, que un asunto es complejo cuando en él intervienen varios elementos y, por tanto, las consiguientes relaciones entre los mismos, y entre éstos y el todo que forman. Y nos topamos también con la complejidad de un objeto cuando, además de reparar en los elementos que lo constituyen, y en las relaciones entre ellos, nos interesamos por las pautas según las cuales este objeto evoluciona con el tiempo, algo de lo que nada ni nadie está exento, pues todo cuanto aparece en este mundo -así físico como conceptual- experimenta cambios. Éstas son, en suma, las dos caras de esa moneda que llamamos *complejidad*. Comprender el mundo -o un aspecto concreto de él- y su complejidad es comprender estas dos categorías de cuestiones: Las relaciones entre el todo y sus partes y los procesos de evolución y cambio.

Sucede que la mente humana parece encontrarse adiestrada mejor para discurrir secuencial o linealmente que para comprender realidades complejas, de naturaleza reticular, donde todo tiene que ver con todo en mayor o menor medida. De hecho, el ser humano, en su permanente negociación con él mismo y con su entorno, acomete decisión tras decisión. Y los directivos, en concreto, si bien han alcanzado un notable grado de maestría en esto de tomar decisiones, en lo que se refiere a comprender la complejidad son, o somos, todavía unos párvulos.

Este es el primer ejercicio de humildad que hemos de practicar cada vez que nos interesamos por la rentabilidad de las inversiones en TI. Pues se trata, sí, de una cuestión compleja, es decir, en la que intervienen innumerables elementos y, por tanto, un número exponencialmente mayor de relaciones entre los mismos. Y esto es así, muy especialmente, cuando se eligen la información como nexo, y las decisiones como elementos, para analizar en clave sistémica nuestras organizaciones humanas, en lugar de aceptar -como habitualmente se hace- la autoridad como el lazo que hilvana y recorre los departamentos de una empresa.

Y la rentabilidad de las inversiones en TI es, al mismo tiempo, un objeto de estudio que está en permanente evolución, especialmente en esta época que nos ha tocado vivir, donde el ritmo de cambio que experimentan las empresas, y los instrumentos técnicos de que éstas se dotan, es tal que produce vértigo.

En suma, esta característica intrínseca del objeto -su *complejidad*- representa, ya de por sí, una *dificultad* a la hora de acometer su estudio. Se trata de un obstáculo cuya causa no reside en nosotros, sino en el objeto de estudio por el que nos interesamos.

Existen, además, otras fuentes de dificultad. Pero para emprender la búsqueda e identificación de estos nuevos focos habremos de cambiar el destino de nuestra mirada. Tendremos que dejar de observar el objeto propiamente dicho, y empezar a interesarnos por nosotros mismos, es decir, por los analistas deseosos de conocer cómo puede evaluarse la rentabilidad de las inversiones en TI.

Una dificultad instrumental

Con el fin de comprender una segunda categoría de razones que hacen difícil nuestra tarea, recurriré a una conocida comparación entre varios instrumentos inventados por el hombre. Repárese en lo siguiente. Para adentrarse en lo infinitamente pequeño y poder observar la intimidad de la materia, el ser humano ideó el microscopio. Para acercarse a lo infinitamente grande e intentar comprender lo que sucedió, sucede, y acaso ocurra en el cosmos, el hombre construyó el telescopio. Mas para hacerse con lo infinitamente complejo -complejo como la vida misma, así individual como empresarial o social-, no disponemos de instrumento físico alguno. Por este motivo, entre otros, los seres humanos seguimos sin comprender muchas cosas. (Entre otras -y dicho sea entre paréntesis-, el propio concepto de complejidad que acabo de enunciar, noción ésta que la ciencia moderna no ha conseguido aún definir por completo. Por eso nos tenemos que conformar -según acabamos de ver- con hacer referencia al todo y sus partes, y a los procesos de evolución y cambio).

* Este artículo es la transcripción íntegra de la ponencia impartida por el autor en la IV Conferencia Internacional ComputerWorld y se publica con los oportunos permisos de los organizadores de dicha conferencia y del autor, que tienen el copyright de la misma.

El hecho es que no disponer de un instrumento *ad hoc* para comprender la complejidad constituye, por tanto, un segundo e importante obstáculo, achacable éste a las limitaciones humanas. Pero no es el último que deberemos superar a golpe de ingenio. Ni quizá se trate de la traba más seria.

Una dificultad epistemológica difícil de sortear

Para comprender esta nueva fuente de dificultades propongo establecer una nueva comparación al amparo de la primera. Ahora se trata de cotejar no instrumentos físicos, sino ideas. Del siguiente modo. Para estudiar el mundo físico -bien infinitamente pequeño, bien infinitamente grande- no sólo los respectivos instrumentos han evolucionado una enormidad en los últimos 100 años; también lo han hecho las ideas y teorías con que intentamos comprender estos dominios. Y sin embargo, en el caso de la comprensión de la complejidad de la vida humana, ni hemos conseguido inventar artilugio alguno, ni -lo que es aún más grave- hemos evolucionado gran cosa en el terreno de las ideas, hipótesis y teorías con que pretendemos adentrarnos en las cuestiones sociales.

Los postulados básicos de la Economía, así como de la Sociología, son ahora sustancialmente los mismos que los acuñados por sus fundadores. Lo cual no deja de constituir una intrigante paradoja, muy del agrado de numerosos pensadores. Pues así como la naturaleza de los átomos o del cosmos no ha debido de evolucionar gran cosa en las últimas décadas (pero sí -y mucho- los instrumentos, y no digamos ya la Física o la Biología), en el caso de la organización social y empresarial ocurre, en cierto modo, lo contrario, es decir, mientras la sociedad y la empresa han experimentado -y experimentan a diario- cambios sustanciales, seguimos huérfanos de utensilios e ideas nuevas para abordarlos.

Al genuino carácter complejo de la cuestión; a la inexistencia de instrumentos físicos que amplíen nuestras escasísimas facultades innatas para observar tal complejidad y, en tercer lugar, al envejecimiento de las ideas con que intentamos interpretar la condición humana y social, habremos de añadir una cuarta y última fuente de dificultades, imputables estas últimas -al igual que las citadas en segundo y tercer lugar- al ser humano. Me refiero al siguiente hecho que creo tan cierto como los anteriores.

Una última fuente de dificultades ... asequibles, fáciles de sortear

En nuestros análisis mezclamos con frecuencia categorías o conceptos para nada homogéneos, al tiempo que ignoramos otros, por creerlos quizá irrelevantes. Pues tantas, y tan amplias, son las nociones que lleva explícitas el propio rótulo -rentabilidad, inversiones, TI-, así como las que de ellas se derivan implícitamente, como son la naturaleza de las decisiones, el ámbito de éstas, o los criterios de evaluación, por citar tan sólo algunas de las más importantes.

De no aceptar de antemano estas cuatro categorías de obstáculos, corremos el riesgo de afrontar el asunto que hoy nos ocupa provistos de una insensata arrogancia. Con el fin de intentar llegar a algunas conclusiones que merezcan un mínimo crédito, me propongo en lo que sigue desandar el camino recorrido, es decir, partir de las ideas que hoy utilizamos, situar cada una de ellas en el lugar que le corresponde, aderezarlas con algunas dosis de actualidad y, quizá, de futuro y, por último, ver cómo podemos paliar la falta de ese utensilio físico que tanto echamos de menos, y que bien podríamos bautizar como "*complexcopio*". De este modo nos volveremos a encontrar en el lugar del que partimos, es decir, nos hallaremos de nuevo, frente a frente, ante la complejidad intrínseca y al desnudo, pero desprovista ya de nuestras propias torpezas analíticas que -así lo espero- se habrán ido quedando en la cuneta. Éste es el plan o discurso para el que pido su atención y paciencia.

Comencemos, pues, por la tarea que se encuentra más a nuestro alcance, y recordemos las diferencias que existen entre las *decisiones* a que inevitablemente conduce un análisis de inversiones (sus distintos tipos y ámbitos) y los *criterios* por los que, finalmente, el decisor opta por una u otra alternativa de entre todas las consideradas. Bien entendido que repasar los diferentes tipos, los distintos ámbitos, así como los variados criterios que caben distinguirse en todo proceso de toma de decisiones, no es el propósito de este trabajo, sino la disculpa utilizada para ir identificando las dificultades que acabamos de enunciar.

Tipos de decisiones de inversión

Sean éstas las principales categorías de decisiones que cabe imaginar:

1. Puede una empresa -o un individuo- querer decidir entre: (a) adoptar un nuevo utensilio o bien (b) no adquirirlo; entre, por ejemplo, acceder al así llamado ciberespacio o continuar enterándose de lo que ocurre por esos mundos y mercados mediante procedimientos tradicionales. Es la decisión entre X y no-X.

2. También puede suceder que el decisor se encuentre ante la necesidad de evaluar entre (a) una herramienta en particular y (b) otra que ofrece prestaciones equivalentes; entre, pongamos por caso, Netscape y otro navegador cualquiera. Es la decisión entre X_1 y X_2, dos posibilidades de naturaleza muy similar.

3. Quizá el individuo -o la empresa en cuestión- se esté planteando optar entre dos posibilidades, ambas técnicas pero de diferente naturaleza: bien (a) introducir definitivamente el uso del Internet en su actividad profesional o bien (b) dejar esta necesidad para más adelante y, primero, dotarse de un moderno sistema de bases de datos con el que gestionar mejor su catálogo de productos, por decir algo. Es la decisión entre X e Y.

4. O acaso el decisor esté dudando entre invertir en (a) tal o cual avance tecnológico o (b) dar prioridad al diseño de un nuevo logotipo institucional de su empresa. Es la decisión entre dos categorías harto diferentes; digamos que entre X y otro trazo cualquiera de un universo distinto, por ejemplo, la última y definitiva letra del alfabeto griego, omega (Ω).

Este esquema ni es novedoso ni es el único posible ni quizá sea del todo correcto o completo. Pero, en cualquier caso, es suficientemente adecuado a los fines que persigue este trabajo. Y de él, además, puede decirse lo mismo que sobre cualquier otro, de los muchos al uso: se trata de un discurso muy aburrido, romo y frío. Pues ¿dónde se encuentra el ser humano que es, al fin y al cabo, quien ha de decidir entre X y la otra alternativa? ¿Dónde están la persona y los sentimientos que le animan a pronunciarse por una u otra opción? Reparemos por un momento en los dos actores clásicos de la ya vieja historia que arrastra tras de sí la justificación de las inversiones en TI: el señor que compra -y que quiere asegurarse de que lo hace bien- y el señor que vende y que, como su cliente, también pretende alcanzar sus propios objetivos con la transacción mercantil que les ocupa a ambos. Los sentimientos de uno y otro están presentes en el ejercicio de justificar la operación, aunque en nuestros esquemas tradicionales dicho componente

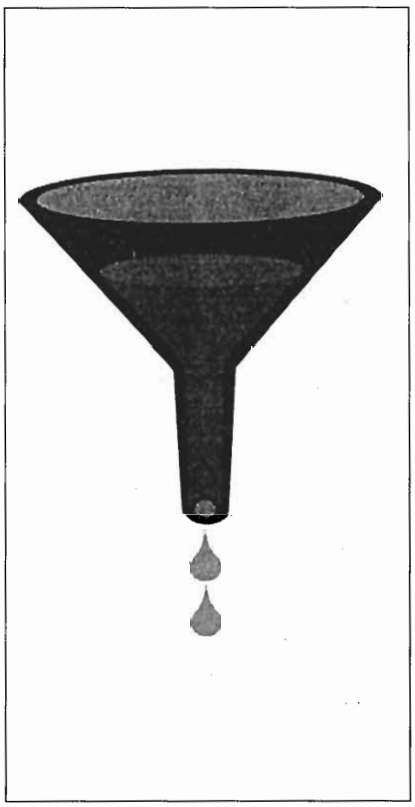
brille por su ausencia. Inteligencia y sentimientos no habitan, no, en dos compartimentos estancos, algo que en los tiempos actuales está mereciendo creciente atención.

Es necesario, por tanto, añadir el ingrediente de la *inteligencia emocional* a la fría y escueta lógica de los estudios de rentabilidad de las inversiones en TI. No hacerlo así, por temor a que los sentimientos y la tasa interna de rentabilidad sean dos entidades inmiscibles, equivaldría a aceptar que la vida y nuestros afanes humanos son una maquinaria de relojería, lo que a todas luces dista mucho de ser así. Ingenieros todos, creo importante que nos preguntemos ¿a qué estamos jugando? ¿Por qué escindimos, o abrimos en canal, la vida? Pues no es otra cosa lo que hacemos cuando hablamos, por una parte, de los aspectos que se avienen a nuestra forma de razonar y, por otra, de aquéllos otros que -como los sentimientos- creemos propios de otro planeta y ajenos a nuestra profesión, cuando no asunto de mujeres. ¿Por qué, por ejemplo, la profesión TI es, casi exclusivamente, masculina?

Ámbitos de las decisiones de inversión

Los ejemplos utilizados para ilustrar estos cuatro tipos de decisiones son, más o menos, del mismo pelaje o envergadura. Son todos reales, tomados de la experiencia cotidiana, pero son también todos muy concisos y, por tanto, fáciles de imaginar, e incluso llegado el caso, de cuantificar. Pero evidentemente, no todas las decisiones de inversión versan sobre asuntos tan concretos. Así, esta característica común a todos ellos invita a dar un segundo paso, es decir, a preguntarse por el *ámbito* o amplitud de las decisiones a tomar, con independencia del *tipo* o naturaleza (X vs. Y; X vs. Ω) de que se trate. Para estructurar esta segunda dimensión del objeto de trabajo que nos ocupa puede uno acogerse a las principales etapas que se distinguen en la reciente historia de la progresiva tecnificación de las empresas y organismos de todo tipo. Utilizar los hitos de las últimas décadas -los que se levantan en este territorio por todos nosotros conocido aunque sólo vivido por los más viejos- es una forma como otra cualquiera de establecer una clasificación que sea útil a los efectos que perseguimos. Este es el esquema propuesto, uno de los muchos que se han descrito. Consta de cuatro puntos, a los que en lo sucesivo me referiré repetidas veces mediante las cuatro primeras letras de nuestro abecedario:

1. Decisiones de inversión acerca de un utensilio o artefacto en particular: tal o cual sistema operativo, o cualquier otro dilema concreto en el plano no del software, sino del hardware. Este era el territorio duro y puro donde se desenvolvían como pez en el agua los en su día denominados jefes de mecanización. Su universo mental empezaba y acaba aquí: en sustituir tal máquina (CPU, se decía entonces) por



tal otra.

2. Decisiones de inversión que atañen ya no a un elemento del sistema sino al diseño del sistema o infraestructura tecnológica en su conjunto, lo que en mi época se dio en llamar el sistema de información físico, es decir, el conjunto de utensilios (software y hardware) que era responsabilidad de los jefes de proceso de datos y, más tarde, de los directores de informática. Este era el reto -el ámbito de las decisiones- de aquellos colegas que al sentirse superados por el desarrollo de los acontecimientos, decían ver en la red de terminales -cada vez más tupida- los tentáculos de la muerte.

3. Decisiones de inversión en un ámbito aún más amplio: aquéllas que se refieren no ya a los utensilios (aislados o en su conjunto) sino al objeto de trabajo o razón de ser de éstos, es decir, las informaciones de todo tipo que circulan a lo largo y ancho de las organizaciones. Hace cierto tiempo, a este dominio se le conocía como el sistema de información lógico de la empresa. No distinguir este nuevo ámbito del inmediatamente anterior sería tanto como confundir los medios para gestionar la información, con la gestión propiamente dicha de la información. Este era, más o menos, el espacio donde germinaron, y vivieron sus esplendor, siglas hoy tan rancias como el MIS (*Management Information Systems*).

4. Decisiones de inversión, por último, que versan sobre el sistema empresarial en su conjunto, uno de cuyos recursos (la información) era -y es- responsabilidad de quienes se daban -y se dan- a conocer como los CIO de las empresas, a imagen y semejanza de la consabida etiqueta -CEO- con que se designan a las máximas autoridades ejecutivas.

Respecto a esta forma de clasificar los *ámbitos de las decisiones* cabe repetir lo ya dicho con relación a las categorías o *tipos de decisiones*: Ni es novedosa ni la única posible ni, acaso, sea del todo acertada ni -como cualquier otra clasificación al uso- tiene en cuenta la condición humana del decisor. Pero, de todos modos, se ajusta lo suficiente a los fines que aquí se persiguen. Y así como los sentimientos humanos constituyen una categoría ausente -se hable de *tipos* o de *ámbitos* de las decisiones-, en lo que se refiere a esta última clasificación cabe mencionar, además, dos nuevos ingredientes que aún luchan por alcanzar la mayoría de edad en los análisis con que se intenta justificar la rentabilidad de las inversiones en TI, a saber: la gestión no ya de la información sino, además, del conocimiento (*knowledge management*) y, en segundo lugar, la conceptualización de la propia empresa, o de la institución de que se trate, como sistemas que procesan información y conocimiento con el fin de alcanzar sus objetivos (*information & knowledge based organizations*), perspectiva ésta a la que habré de referirme de nuevo más adelante.

No deja de llamar la atención (por decirlo de alguna forma, y a modo de inciso o digresión) que para facilitar la comunicación entre ustedes y yo haya de referirme a estos conceptos en lengua inglesa, cuando lo cierto es que se trata de nociones que echaron sus primeras y más fecundas raíces entre nosotros, aquí, en el viejo continente. Sea ello como fuere, para que estas dos nociones superen con éxito su apariencia de meras expresiones alambicadas -fruto ambas de la imaginación de consultores y

ejecutivos-, es menester incluirlas a todos los efectos en los cálculos que hagamos: ¿Cuál es la rentabilidad de las inversiones en la gestión del conocimiento?, ¿y la de las inversiones que se necesitan para, de verdad, gobernar una empresa basada en la información y el conocimiento? Ahora bien, la incorporación de estas nociones pone sobre la mesa importantes y nuevos retos, así conceptuales como prácticos. Y esto es así, entre otras razones, porque se trata de cuestiones -información, conocimiento- que, por su propia naturaleza, no obedecen -no pueden obedecer- a las leyes que sí rigen -y con probada eficacia- la gestión de los factores clásicos, Trabajo y Capital. Por ello, dicha propuesta de incorporación rodea de interrogantes a las proverbiales funciones de producción, ejes diamantinos de un pensamiento económico aún hoy vigente.

Aquí la pregunta debe dirigirse, no a los ingenieros, sino a los economistas: ¿A qué estamos esperando? A mi modo de ver, la respuesta en este caso es inmediata. La incorporación de la información y el conocimiento a las funciones de producción clásicas implicaría poner en cuestión, entre otras cosas, las relaciones de poder.

Por eso, esta dificultad es sorteable, sí, pero ¿por quién, ¿a qué precio?, ¿cuándo?, ¿qué circunstancias habrán de darse para que el pensamiento económico se atreva de dar el paso que significa interesarse -además de por el sustento, el cobijo y demás motivaciones básicas- por las motivaciones más elevadas del ser humano, es decir, por la necesidad de saber, de alimentarse de nuevos conocimientos?

Criterios para decidir las inversiones

Cualquiera de los cuatro *tipos* de decisión pueden darse -de hecho, se dan- en cualquiera de los cuatro *ámbitos* mencionados. Aun siendo ambas clasificaciones escuetas y simples en extremo, su combinación nos ofrece un rico abanico de posibles escenarios, todos ellos situados bajo el amplio rótulo de la rentabilidad de las inversiones en TI. Este espectro de posibilidades verá aumentado aún más su tamaño desde el momento en que reparemos en lo siguiente: Es imprescindible acordar de antemano cuáles serán los *criterios* por los que nos vamos a inclinar por una u otra opción (X vs. Y ; X_1 vs. X_2, etcétera) en cualquiera de los ámbitos (utensilio, sistema físico o lógico, o la propia empresa en su conjunto).

Para pasar revista a los posibles criterios de decisión resulta útil agruparlos en categorías. Sin que -una vez más- pretenda en modo alguno agotar la cuestión, he aquí los tres tipos de criterios que propongo. Hablaré de criterios relacionados con los fines, que podríamos denominar criterios teleológicos; de criterios estrictamente financieros y, por último, de criterios basados en análisis comparativos entre empresas

1.Criterios relacionados con los fines

Como es sabido, el fin último de las decisiones de inversión de capital es proteger y aumentar la capacidad de quien realiza la inversión para alcanzar unos determinados objetivos. Cualquier propuesta de inversión que no garantice tal fin (proteger y aumentar la capacidad para cumplir unos objetivos) no merecerá ser aprobada. Este es, pues, *"el" criterio* genérico por excelencia con que deberán ser juzgadas las inversiones que se sometan a estudio.

Al igual que en los apartados precedentes, también aquí propongo una clasificación con la que ahormar los razonamientos que siguen. Con este fin, parece obligado indagar en los diferentes tipos de objetivos cuya consecución se pretenda garantizar mediante una inversión. Y para ello no hace falta ir muy lejos; es suficiente con adoptar como guía de nuestro discurso los distintos ámbitos de decisión recientemente expuestos. De este modo -lo veremos de inmediato-, acabaremos por distinguir entre criterios u objetivos *instrumentales* y criterios u objetivos *empresariales*. Dos nuevas categorías que vienen, no "a sumarse a", sino a "multiplicarse por" los cuatro tipos y otros tantos ámbitos de decisiones hasta aquí descritos.

Puede darse la circunstancia -de hecho se da con frecuencia- que, con la inversión cuya rentabilidad nos preocupa, se pretenda alcanzar fines tan concretos como el de aumentar la capacidad de efectuar determinadas transacciones por unidad de tiempo, para lo que el decisor se dispone a evaluar la adquisición de un determinado equipo de entre todos los que el mercado ofrece, o bien a desecharla.

O puede suceder que con la inversión en estudio se desee conseguir objetivos técnicamente más amplios: no ya mejorar las prestaciones de un determinado elemento del sistema físico sino de la propia infraestructura tecnológica en su conjunto, ampliando así su complejidad. Estos dos supuestos se corresponden con los ámbitos **a.** y **b.** ya expuestos.

Pues bien, predecir el grado de cumplimiento de ambos tipos de objetivos gracias a una determinada inversión es una labor que no comporta serias dificultades. Este es el terreno de las conocidas pruebas de *benchmarking*. El resultado de las mismas -de ser positivo- puede dejar muy satisfechos tanto al ofertante como a su cliente, e incluso puede convencer a propios y extraños, pero siempre y cuando no se vaya demasiado lejos en la búsqueda (muchas veces desesperada) de relaciones causa efecto. Pues si bien resulta cierto que las inversiones en un elemento del sistema de información físico (**a.**), o en el diseño del propio sistema en su conjunto (**b.**), pueden justificarse sin problemas -con mucha naturalidad-, siempre y cuando el criterio que para ello se utilice no rebase los límites de su propio ámbito de actuación, no es tan evidente y demostrable deducir que, como consecuencia de lo anterior, se mejora el sistema de información lógico de la empresa -ámbito **c.** de nuestra escala-, es decir, que se mejoran los sistemas de gestión de la información de la empresa propiamente dichos.

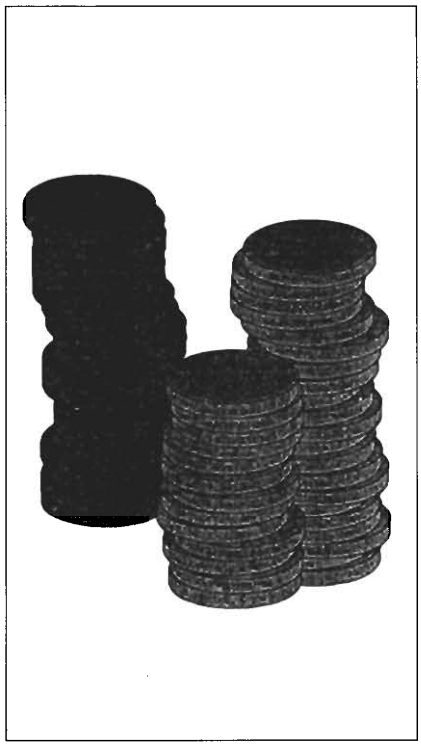
En resumen, traspasar las fronteras del plano físico al lógico, es decir, marcarse un objetivo en el ámbito **a.** o **b.**, estudiar una inversión *ad hoc* para "proteger y aumentar" la capacidad de alcanzarlo, pero evaluar su idoneidad con criterios del ámbito **c.**, puede representar un salto en el vacío, quizá muy bien ensayado, pero siempre arries-gado, se disponga o no de la consabida red entre nosotros y el duro suelo. Y esto es así, entre otras razones, porque mientras los ámbitos, objetivos y criterios de tipo **a.** o **b.** son de naturaleza mecánica (aceptemos como símbolo un reloj), en la gestión de la información de una empresa intervienen, además, personas y un buen número de otras circunstancias que obligan a equiparar este nuevo ente, no ya a un reloj, sino a un organismo vivo. Y así como una máquina, o incluso un conjunto de instrumentos, puede desmontarse y volverse a montar sin que sobre ni falte un tornillo, de un organismo vivo -individual o colectivo- no puede decirse lo mismo: una vez desarmado, sólo un milagro puede devolverle la vida.

No los ingenieros, ni los economistas tampoco, ahora los destinatarios de la pregunta obligada son, en concreto, los expertos en los análisis financieros -o de cualquier otro tipo- con que se pretende justificar las inversiones en TI: ¿De qué

estamos hablando? Siendo tan dispares las naturalezas de uno y otro plano, **a.** y **b.**, ¿cómo es posible invertir en el primero de ellos y justificar dicho empeño mediante criterios que son únicamente válidos en el segundo?

Los problemas que se derivan del cruce indiscriminado de fronteras pueden incluso acentuarse cuando lo que se pretende es hacer frente a este nuevo desafío: invertir en los sistemas de gestión de información **c.** (re-ingeniería de procesos es un ejemplo) y justificar dicha iniciativa mediante criterios del siguiente territorio o ámbito **d.**, es decir, con criterios de naturaleza empresarial. Aquí, no se vulnera la naturaleza de los ámbitos (ambos -sistema de información y sistema empresarial- gozan del mismo carácter o condición: son sistemas vivos, no físicos) pero sí se incurre en una simplificación de dudosa solvencia, a saber, la que supone equiparar *una interpretación del todo* -la empresa como sistema de información- con *el todo* propiamente dicho, es decir, con esa unidad compleja que llamamos empresa. Pues avalar inversiones en el campo de los sistemas de gestión de información aduciendo para ello que la empresa ve así "protegida y aumentada" su capacidad para alcanzar sus objetivos empresariales, es tanto como admitir una nueva relación de causa efecto que, cuando menos, puede ser calificada de atrevida. Y es que la mentalidad mecanicista invade nuestro pensamiento. Repárese, por ejemplo, en la expresión que acabamos de mencionar: re-ingeniería de procesos. Se trata de una etiqueta atroz donde las halla, pues el mero hecho de aplicar la noción de ingeniería a procesos donde intervienen seres humanos da justa medida de la miopía intelectual de quienes de este modo se pronuncian.

Utilícense, en suma, los criterios que se deseen, pero sin traspasar fronteras alegremente. Sin saltarse a la ligera los límites que se interponen entre lo que son sistemas físicos y aquellos otros de naturaleza orgánica o viva. Y sin cruzar con desmedida audacia la distancia que separa lo que son instrumentos de lo que son fines, es decir, recorriendo con las necesarias cautelas el espacio que se interpone entre los *objetivos instrumentales* y lo que son *objetivos empresariales*. Los primeros (por muy válidos y supremos que sean dentro de sus respectivos ámbitos, **a.**, **b.** o **c.**) están al servicio de los segundos (**d.**), es decir, son instrumentos para alcanzar los objetivos empresariales. Lo cual no debe invitarnos a utilizar éstos para justificar aquéllos. Pues, al fin y al cabo, es la empresa quien invierte y no tal o cual director de informática, o de organización, aunque la práctica presupuestaria de sus empresas les haya delegado la gestión de una determinada partida para invertir dentro del ejercicio. Son, en efecto, los objetivos empresariales -de los que me ocuparé a continuación- no los únicos, pero sí los árbitros supremos a la hora de tomar decisiones sobre las inversiones de capital, así en TI como de cualquier otra naturaleza.



En el contexto de este trabajo parece conveniente adentrarse en el campo de los objetivos empresariales de la mano de nociones tan conocidas como son la eficacia y la eficiencia. Se es eficaz si se cumplen los objetivos propuestos, y eficiente cuando el foco se pone en la gestión de los recursos y medios de que se dispone para alcanzar dichos objetivos. Desde el punto de vista de la *eficacia*, puede hablarse de objetivos empresariales genéricos (crear valor para el accionista; asegurar la con-tinuidad de la empresa y, con ello, los puestos de trabajo, etcétera) y de objetivos empresariales coyunturales (aumentar la cuota de mercado, lanzamiento de un nuevo producto, etcétera). Desde la perspectiva de la *eficiencia*, las palabras clave son, entre otras muchas, coste, tiempo, materias primas, procesos, información, etcétera. Pues bien, las inversiones en TI -como cualquier otra inversión de capital- se acometen con el propósito último de proteger y aumentar la capacidad de la empresa para alcanzar este tipo de objetivos: tanto de eficacia como de eficiencia; genéricos o coyunturales. Es fácil imaginarse la gama tan grande de criterios con que pueden las máximas autoridades ejecutivas exigir que le sean justificadas las inversiones en TI. La presión que los responsables del recurso información sienten ante tamaño compromiso les lleva, en ocasiones, a asegurar que las inversiones en TI ahorran a su empresa tantos millones de pesetas lo que, dividido por el número de acciones, equivale a tantos céntimos por acción, "demostrando" de este modo cómo las TI colaboran al fin último de la entidad, es decir, a la "creación de valor para el accionista".

Al margen del rigor que puedan albergar o no estas aseveraciones, sí resulta cierto el que la creación de valor para el accionista -fórmula ésta consagrada en el reciente Código Olivencia como la principal función de la empresa- no es un objetivo supremo y válido para todos los casos y circunstancias. ¿Quiénes son, por ejemplo, los accionistas de las cajas de ahorros, sector éste que representa, más o menos, la mitad del sistema financiero español?

En cualquier caso, es fácil suponer cuán alto se colocaría el listón, en esto de justificar las inversiones en TI, si un empresario transmitiera el siguiente mensaje institucional: la autorrealización del empleado en el mundo del trabajo (su plenitud como seres humanos y su capacidad de decidir con autonomía) es una premisa irrenunciable para el rendimiento y el progreso de la economía. Por eso, nuestra empresa -basada en la cooperación- se caracteriza por el hecho de que todos los interesados, desde el accionista, pasando por la dirección, hasta los empleados, se consideran un grupo de trabajo con una misma finalidad y responsabilidad: aportar un servicio a la sociedad. ¿Cómo podríamos llegar a relacionar la causa -una inversión en equipos y/o procedimientos- con el efecto u objetivo último deseado, es decir, con la utilidad social de la empresa? Este ejemplo no es imaginario, sino real. Son palabras de Reinhard Mohn, hasta hace poco presidente de una de las grandes multinacionales de la comunicación -el grupo Bertelsmann-, quien acaba de merecer el premio Príncipe de Asturias de Comunicación y Humanidades.

Y es que son tantos, y de tan variada índole, los factores que intervienen en el asunto que hoy nos ocupa; tantas, y de tan dispar naturaleza, las circunstancias que se interponen entre los meros instrumentos tecnológicos y los fines últimos

de la empresa que, cuando menos, hemos de admitir que tras la etiqueta "Rentabilidad de las inversiones en TI" se esconde todo un mundo complejo y variopinto de casos muy diferentes y en los que, de una forma u otra, intervienen siempre cuestiones técnicas, estrategias empresariales, intereses personales, relaciones de poder, etcétera.

Aun recuerdo con agrado -y no creo que hayan perdido vigor alguno- las conclusiones del estudio que realicé para la Asociación del Progreso de la Dirección a mediados de los años 80. Tras el riguroso análisis realizado sobre 204 empresas españolas, no pudo encontrarse evidencia alguna que permitiera afirmar la existencia de relaciones causa efecto entre las inversiones en TI y los resultados económicos de estas compañías.

2. Criterios de carácter financiero

A las dos categorías de criterios hasta aquí descritas -instrumentales y empresariales- cabe añadir una tercera: criterios estrictamente *financieros*. Es ésta una fórmula vieja y acrisolada mediante la cual todo se traduce a clave económica. ¿Se traduce o se reduce? Sea ello como fuere, y puesto que el propósito de este trabajo no es otro que el de seguir restando *dificultad* a la ya por sí inherente *complejidad* de nuestro objeto de estudio, me limitaré a recordar unas cuantas nociones básicas. Pues la exposición detallada de los grandes avances experimentados por las técnicas de justificación financiera es algo que debemos dejar en manos de los expertos.

Tanto se trate de decidir entre X y no-X como, en el extremo opuesto, entre X y Ω, y en no importa cuál de los ámbitos enunciados (**a.**, **b.**, **c.** o **d.**), bueno será tener presente cuatro conceptos mal contados y, en ocasiones, peor comprendidos. He elegido aquéllos que en mi época -no tan lejana, si se me permite- manejábamos con más torpeza; los que, a pesar de su aparente sencillez, o quizá precisamente por ello, resultaban más escurridizos. Helos aquí:

- *La naturaleza cronológica del dinero*, algo que puede asimilarse a la inflación cuando, en rigor, si el dinero es función del tiempo ello se debe, en primera instancia, a nuestra capacidad habitual para operar con él. Y por esta razón, es decir, para no caer en el error que supondría manejar cantidades de dinero de diferentes "edades", resulta obligado, como es sabido, reducir el valor de todas las partidas y conceptos a un único momento, pasado, actual o futuro.

- *El propio concepto de inversión* (ora de activo puro -de caja a inmovilizado- ora de pasivo, vía ampliación de capital), como catalizador o bomba cebadora de un proceso del que se espera obtener más beneficios que costes. Algo que a los no iniciados les invita a conceptualizar la bondad de una inversión como una balanza entre costes y beneficios cuando, en rigor, en la metafórica balanza, la

inversión cuya rentabilidad nos interesa conocer ocupa uno de los platillos -con sus costes y sus beneficios previstos-, mientras que en el otro ha de situarse un proyecto inversor alternativo.

- *Los diferentes tipos de coste* (de explotación -o costes operativos- y de instalación, también llamados de implantación o de primer establecimiento), *así como de beneficio*, entendido éste no como entrada de dinero en caja sino, precisamente, como reducción de costes. Lo que permite categorizar los posibles beneficios según su grado de cuantificabilidad, a saber, de más a menos: costes desplazados, costes evitados y beneficios intangibles. En cada uno de estos tipos de beneficios se puede, a su vez, hacer distingos según sea la probabilidad de ser obtenidos, pues una cosa es el problema de su cuantificación y otra, bien distinta, es el grado de certeza con que se estima pueden ser obtenidos. La combinación de ambos criterios da pie a las consabidas *matrices de riesgos*, donde la cantidad ha de convivir forzosamente con la calidad, y los juicios objetivos -si los hubiere- deben cohabitar con las omnipresentes e inevitables valoraciones subjetivas.

En fin, cuando se ha elegido el dinero como patrón supremo, es con éstos y otros elementales mimbres como se construyen las diferentes varas de medir la rentabilidad financiera de las inversiones. En este resumen telegráfico de la cuestión caben mencionarse los siguientes patrones o criterios, ordenados de menos a más sofisticación: (1) La comparación de costes, lo que puede entenderse como un ejercicio elemental de evaluación al peso; (2) La recuperación de la inversión, más conocido, quizá, por sus siglas inglesas: ROI, y su inverso, conocido como (3) El período de recuperación (*payback period*). Como es sabido, ninguno de estos tres patrones tiene en cuenta el valor cronológico del dinero, no así los dos siguientes: (4) El valor actual neto y (5) La tasa interna de rentabilidad. Como resulta lógico, cuanto más sencillo es el parámetro, más engañosa puede resultar su utilización, sean cuales fueren las dimensiones utilizadas: un período de tiempo, un porcentaje, o bien una unidad monetaria cualquiera -la celtibérica peseta, el arrinconado escudo portugués o el bisoño euro, que tantas luces económicas -así como sombras sociales- arroja sobre nuestra existencia inmediata.

Sobre este esqueleto así pergeñado, se han ido construyendo con los años más y más sofisticados aparatos matemáticos, bien de inspiración europea, bien con genuino sabor americano. Sin por supuesto restar mérito alguno a tan notables avances, creo oportuno resaltar en este punto que las creencias y los valores sobre los que aquéllos se sustentan no han evolucionado tanto. De ello, así como de la adecuación de su uso al caso que nos ocupa, quiero llamar su atención por si resulta merecedor como tema de debate.

3. Criterios basados en los análisis comparativos entre empresas

Asegurarse de que las inversiones en TI que viene realizando nuestra empresa son razonables, por estar en línea con lo que hace la competencia, es una forma indirecta, y no menos frecuente que las anteriores, de presumir la rentabilidad de aquéllas. En este tercer y último grupo de criterios me limitaré a compartir con ustedes las tres ideas -a cual más obvia o elemental- que siempre fueron mi norte, cada vez que me veía ante la necesidad de establecer este tipo de comparaciones para convencer a mis clientes.

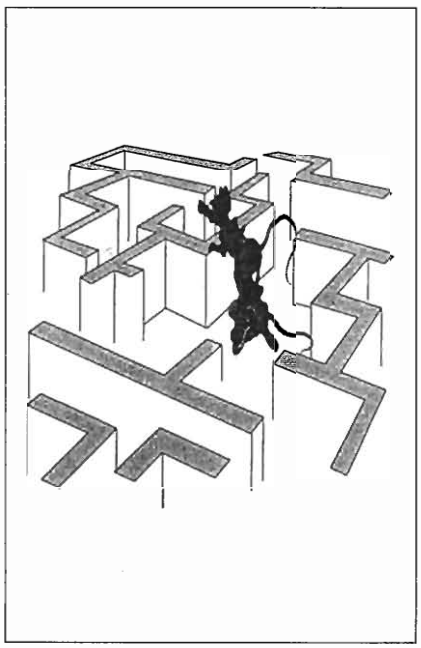
- Las comparaciones han de establecerse entre actividades productivas cuya "intensidad en información" resulte

equivalente. Entendiendo por este índice -intensidad en información- el porcentaje que sobre el valor añadido generado por la empresa (es decir, sobre su Haber) representa esta partida del Debe: la remuneración al factor Información en todas sus formas y grados de elaboración imaginables, sobre no importa qué tipo de soporte (desde el cerebro humano hasta una hoja de papel) y referente a todos y cada uno de los aspectos que componen la empresa y su entorno. La intensidad en información -índice que en la sociedad postindustrial viene a ocupar el lugar que tiene la intensidad en capital dentro de un orden industrial- depende de tres factores: (1) la diversidad de salidas, productos y servicios, que elabora la empresa; (2) su grado de integración vertical -a mayor integración, más necesidades de coordinación, y (3) las exigencias de operación y control. El problema aquí radica en el escaso hábito que tienen las empresas de examinarse así mismas en estos términos, por lo que las comparaciones en ocasiones no resultan adecuadas.

· Evitar, en la medida de lo posible, copiar a los políticos, quienes por lo común hacen o dejan de hacer en función de lo que ocurre en "los países más avanzados", expresión ésta que tiene el dudoso honor de haberse convertido en irritante coletilla de sus discursos. Abrirse sin ninguna reserva a cuanto se piensa, se habla y se hace en cualquier parte del mundo es cada vez más posible, necesario y aun inevitable. Pero reflexionar sólo de prestado es vivir en precario, sin derecho bien fundado; es una forma de renuncia o dejación que acabará por falsificar el modo de entender la vida (o la propia empresa) de quien así se comporta. Quizá la mejor forma de complementar -¡no de sustituir!- este hábito sea utilizar, además, el viejo proverbio castellano que, a estos efectos, aconseja seguir don Carlos Fernández Esteban: "Cada maestrillo tiene su librillo".

· Cuando miramos al competidor que va por delante de nosotros, con el fin de planificar nuestras inversiones futuras, no hacemos otra cosa que acogernos a la conocida técnica de planificación basada en el estudio de los posibles escenarios alternativos. Lo cual puede resultar útil en determinadas circunstancias, en asuntos concretos y muy bien acotados, pero que como técnica de gran alcance no parece ser la más adecuada hoy en día. Esto es así -al menos a mí me lo parece- porque vivimos en una época en que es el azar -más que unas leyes que están empezando a desobedecernos- el que gobierna el curso de los acontecimientos.

Por tanto, creo acertado invitar a las máximas autoridades ejecutivas de nuestras empresas y organismos de todo tipo a que, además de utilizar tales o cuales criterios para evaluar la rentabilidad de sus inversiones en TI, permanezcan atentas a lo que podemos llamar el signo de los tiempos. Frase conocida ésta que, en el presente contexto, procuraré dotar de contenido mediante dos artículos de prensa. Uno, aparecido hace ya casi 4 años, y otro recientemente publicado. El 19 de



septiembre de 1994 el vicepresidente Al Gore publicaba en *Financial Times* un interesante artículo en el que, entre otras muchas cosas, decía: "La infraestructura de información global será la clave del crecimiento económico para las economías nacionales e internacionales. En Estados Unidos, la infraestructura de información ya es para la economía estadounidense de la década de los 90 lo que fue la infraestructura del transporte para la economía de mediados del siglo XX". Hace apenas 15 días, un periódico español se hacía eco de los resultados de un reciente informe elaborado por la Secretaría de Comercio de los Estados Unidos. En este estudio, entre otras cosas, se exponen las causas clásicas de la buena salud económica del país (reducción del déficit, bajos tipos de interés, entorno macro-económico estable, reducción de barreras comerciales) y agrega: "Muchos observadores creen que los avances en las tecnologías de información, impulsados por el crecimiento de Internet, han contribuido también a crear esta economía más saludable de lo previsto". Si evitamos que estos resultados nos deslumbren -aunque sólo sea por ser coherentes con lo que acabamos de exponer, y porque la realidad de aquel país es una, y la nuestra es otra, en tantas cosas diferentes-, es posible admitir con acierto y sin reparos que, de espaldas a la evolución de las TI, el horizonte parece poco halagüeño. Tradúzcase, pues, esta evidencia al interior de nuestras empresas y organismos de todo tipo.

Resumen hasta regresar al comienzo: la rentabilidad de las inversiones en TI y su inherente complejidad

Son pues muchas, y muy variadas, las dificultades que hemos de soslayar para acometer con acierto la inherente complejidad del objeto de estudio que hoy nos ocupa. De todas las que he recordado en este trabajo, elijo ahora, al momento de resumir mis opiniones, las dos siguientes:

1. La necesidad de redefinir el núcleo del pensamiento económico todavía hoy vigente, dando entrada a la información y el conocimiento en las funciones de producción clásicas. Sin atreverse a dar este paso, los análisis para evaluar la rentabilidad de las inversiones en TI permanecerán faltos de verdadero fundamento, al centrar sus esfuerzos en los instrumentos y no en la razón de ser de éstos. Es preciso, por tanto, complementar:

- la economía centrada en los *factores causales* (Trabajo y Capital) mediante los cuales creamos riqueza,

- con un nuevo concepto de progreso, el que se deriva de entender la actividad económica en términos, no de factores, sino de *actividades causales* (decisiones y acciones) mediante las cuales la humanidad produce conocimiento.

Lo que, además, proporcionará la oportunidad de situar al ser humano y a su entorno natural en la diana misma de las preocupaciones económicas. Que buena falta nos hace.

2. La necesidad de no traspasar fronteras sin las obligadas precauciones. En especial, aplicar criterios de evaluación que sean *propios* de los ámbitos (instrumental, físico o lógico) en que se prevé hacer las inversiones, evitando así la tentación de acudir al ámbito superior de la empresa para, de este modo, establecer relaciones de causa efecto de dudoso fundamento. Pues hemos de aceptar sin paliativos de ningún

género lo difícil que resulta siempre conceder en exclusiva a un sólo factor -las TI- el mérito que supone el que la empresa alcance sus objetivos, sean éstos de la naturaleza que fueren. Por mucho que los procesos productivos, así como los propios productos o servicios que la empresa elabore, dependan de estas tecnologías, el factor humano siempre estará presente. E incluir éste -y cuantos de él se derivan; las relaciones de poder, por ejemplo- en una supuesta métrica financiera, o de cualquier otro tipo, no parece ser empeño fácil.

Si a pesar de estas y otras precauciones por el estilo, las máximas autoridades ejecutivas de nuestra empresa insisten en que les sea demostrada la rentabilidad de las inversiones en TI que les proponemos, entonces, hemos de sospechar que nos encontramos situados en el siguiente escenario: El directivo pretende enmascarar el temor que le produce decidir sobre cuestiones que se escapan a sus conocimientos. Lo cual, hemos de reconocerlo, es una reacción muy humana, pero que presta dudosos servicios a los fines -y, quizá, a la supervivencia- de su empresa.

En la recta final de este trabajo, les relataré muy brevemente cómo actuábamos mis colaboradores y yo cada vez que nos encontrábamos en semejantes circunstancias. Primero, exponíamos la cuestión con toda crudeza, es decir, presentábamos la *complejidad* de la cuestión al desnudo. Para, a renglón seguido, poner a la disposición de nuestros clientes un instrumento no físico, sino epistemológico: el ansiado "complexcopio", de los cuales repartimos entre 1980 y 1993 unas 150 unidades.

Se trata de un instrumento óptico, a través del cual puede apreciarse, por una lado, la empresa, sus elementos, y las relaciones entre unos y otros, lo que permitía a nuestros clientes comprender las ventajas de analizar su negocio como un sistema que procesa información y conocimientos, tanto se tratara de una empresa siderúrgica, un ayuntamiento o un banco. Este primer cristal del instrumento tiene un nombre muy antiguo y bien contrastado: La *Teoría General de Sistemas*. Y, en segundo lugar, les invitábamos a que entendieran su empresa, así concebida, como un organismo vivo sujeto, por tanto, a continuos cambios. Para ello poníamos a su alcance los *Modelos Evolutivos* que explican cómo una empresa, por ejemplo, camina desde sus orígenes hasta, o bien el éxito -siempre efímero, o bien el fracaso, muchas veces definitivo. Y para ello tuvimos que indagar, por extraño que pueda parecer, en áreas tan ajenas a la administración de empresas como son la biología, la física o la termodinámica.

En suma, ante la exigencia de justificar la rentabilidad de unas inversiones en TI, nuestra respuesta fue siempre la misma: Invitar a las máximas autoridades ejecutivas a que invirtieran en su propia formación. Nuestra hipótesis de trabajo era ésta: un directivo avezado en la comprensión de la *complejidad* de su empresa es la mejor garantía para que sus inversiones en TI acaben siendo rentables.

Los resultados obtenidos durante más de 20 años fueron excelentes, tanto económica como humanamente hablando. El resumen de esta experiencia -que quizá siga siendo válida hoy día- es lo que he pretendido plasmar en este enésimo trabajo sobre la rentabilidad de las inversiones en tecnologías de información.

Conclusiones

1. Sin introducir la información y el conocimiento en las funciones de producción clásicas (Capital y Trabajo), los análisis para evaluar la rentabilidad de las inversiones en TI (Tecnologías de la Información) seguirán careciendo de auténtico fundamento.

2. Ha de admitirse, sin paliativos de ningún género, que resulta ilusorio adjudicar a una única causa -las TI- el mérito que supone el que la empresa alcance sus objetivos, sean éstos de la naturaleza que fueren.

3. Ha de admitirse, con igual rotundidad, que sin el uso inteligente de las TI cada vez resulta más difícil asegurar la supervivencia de un creciente número de actividades económicas.

4. Las proposiciones 2. y 3. no son contradictorias ya que las TI constituyen una condición necesaria (incluso en muchos casos, *sine qua non*) pero no suficiente para garantizar el éxito empresarial.

5. Exigir, mediante los métodos disponibles, que se justifiquen las inversiones en TI es, en ocasiones, una actitud con la que las máximas autoridades ejecutivas de las empresas intentan esconder el temor que les produce tener que decidir sobre cuestiones que se escapan a sus conocimientos.

6. La mejor forma que tiene una empresa para asegurarse de que sus inversiones en TI acaben siendo rentables es contar con un equipo directivo avezado en la comprensión de la *complejidad* de la propia empresa y su entorno.

Lengua y Tecnologías de la Información

Una modelización del mecanismo dinámico de construcción de la significación de expresiones complejas

Pablo Gamallo, Michel Chambreuil
Laboratoire de Recherche sur le Langage, Université Blaise Pascal - Clermont 2 (Francia)

{gamallo,chambreuil}@lrl.univ-bpclermont.fr

Resumen: *El predicado es la entidad semántica fundamental del espacio de interpretación de los lenguajes formales no ambiguos y, por extensión, del lenguaje natural. Ahora bien, la rigidez y el estatismo de esta entidad impiden una modelización adecuada del polimorfismo gramatical, de la polisemia léxica y del proceso de desambiguación de las expresiones del lenguaje natural. Este artículo propone, tras un análisis de la organización interna de la noción de predicado, una reestructuración del espacio semántico. En concreto, la hipótesis que se defiende estipula que el objeto central alrededor del cual se estructura el espacio semántico no es el predicado, sino la operación de asignación de una entidad a un papel predicativo.*

La operación de asignación, junto a las condiciones que se le asocian, se presenta como un mecanismo composicional que permite construir de manera dinámica el significado de las expresiones complejas. La flexibilidad de este mecanismo, por lo demás, se adapta convenientemente al polimorfismo gramatical y a la polisemia léxica de las expresiones combinadas. El objetivo de este artículo es precisamente el de esbozar un modelo formal del mecanismo de construcción de expresiones complejas a partir del análisis de la operación de asignación.

Palabras clave: *semántica formal, procesamiento semántico del lenguaje natural, ambigüedad, composicionalidad.*

1. Introducción: ambigüedad y proceso de desambiguación

Uno de los problemas esenciales del procesamiento semántico del lenguaje natural reside en que, a diferencia de los lenguajes formales no ambiguos, la significación de las unidades lingüísticas varía en función de los enunciados en los que se insertan.

La ambigüedad[1] está directamente ligada a una propiedad fundamental de las expresiones lingüísticas: la polivalencia o flexibilidad sintáctico-semántica. Toda expresión es polivalente (o flexible) en el sentido que puede reconfigurar su categoría y precisar su contenido conceptual en función del contexto discursivo en el que se integra. La polivalencia de las expresiones se manifiesta tanto en el nivel sintáctico (lo que llamaremos **polimorfismo gramatical**) como en el nivel léxico (lo que llamaremos **polisemia léxica**). El proceso de construcción de la significación de expresiones complejas permite caracterizar categorialmente y precisar conceptualmente la polivalencia sintáctico-semántica de las expresiones constituyentes. En otros términos, la interpretación dinámica de expresiones complejas desambigua el contenido de las expresiones constituyentes.

1.1. Polimorfismo gramatical

Una misma expresión lingüística (o varias formas lingüísticas aparentadas) puede reflejar categorías gramático-sintácticas diferentes y distribuirse en diferentes contextos sintácticos: 'Juan *corre*' / 'la *carrera* de Juan' / 'que Juan *corra*' / '*correr*'...

Uno de los objetivos principales de los enfoques actuales de la semántica cognitiva, especialmente de la cognitiva de R.W. Langacker (1987, 1991), es el de configurar un espacio semántico que pueda dar cuenta de la riqueza y flexibilidad de la polimorfia gramatical. Las entidades básicas de este espacio son abstracciones conceptuales, caracterizadas como mecanismos complejos de estructuración de la información, que representan el contenido semántico de las formas gramaticales y sintácticas del lenguaje. Tales abstracciones son operaciones de conceptualización ligadas a una capacidad particular perceptivo-cognitiva, llamada *imagery*, cuya función es la de organizar una misma escena visual de diferentes maneras. Basándose en este tipo de abstracciones conceptuales, Langacker propone una nueva caracterización del sistema de categorías lingüísticas.

El polimorfismo gramatical es también el objeto de teorización de la teoría de propiedades (Chierchia G. & Turner R. 1988), cuyo enfoque no es de naturaleza cognitiva sino lógico-formal. La teoría de propiedades no asocia a las formas verbales temporales (por ejemplo a la forma de presente de indicativo 'corre') y a las diferentes formas nominalizadas ('que Juan corra', 'correr', 'carrera'...) el mismo tipo de entidad en el espacio semántico. Una forma verbal temporal denota una función predicativa, mientras que una forma nominalizada denota una entidad individual.

La teoría de propiedades llama **modos de ser** a las dos manifestaciones conceptuales de una predicación: la función predicativa (que es una estructura predicativa incompleta o no saturada) y la entidad individual nominalizada (que corresponde a una estructura predicativa saturada). En el marco nocional de la gramática cognitiva, estos dos modos de ser representan en realidad dos conceptualizaciones abstractas particulares. El espacio semántico de la teoría de propiedades, sin embargo, no está adaptado a la modelización de la polisemia léxica.

1.2. Polisemia léxica

Una misma expresión léxica puede vehicular informaciones diferentes pero aparentadas. Todo lexema posee un grado más o menos elevado de polisemia. Por poner algunos ejemplos, el verbo 'cargar' puede significar : *desplazar obje-*

tos ('cargar sacos en el camión'), *llenar un espacio* ('cargar el camión de sacos') ; el nombre 'botella' puede significar: *objeto que sirve como recipiente* ('llena esta botella'), *substancia contenida en un recipiente* ('prueba esta botella').

Uno de los intentos de teorización formal de la polisemia léxica más en boga corre a cargo de J. Pustejovsky (1995). En su modelo, una entrada léxica se asocia a una compleja estructura informativa compuesta de un conjunto de facetas conceptuales, facetas que representan las diferentes significaciones posibles de la entrada.

El mecanismo composicional opera en el interior de la estructura informativa para seleccionar una faceta conceptual (es decir un significado posible) de la entrada léxica.

El enfoque de Pustejovsky hereda, sin embargo, la rigidez y las limitaciones del sistema de categorías semánticas montagoviano. En efecto, la rigidez de la semántica de Montague no permite en ningún caso modelizar los fenómenos de polimorfismo gramatical (Gamallo P. 1998).

1.3. La construcción dinámica de la significación de expresiones complejas: la desambiguación

Existen numerosos trabajos sobre el procesamiento sintáctico-semántico de enunciados complejos desde el punto de vista de un agente-receptor en comprensión. Estos trabajos analizan la relación entre en el proceso de construcción de la estructura sintáctica del enunciado y el acceso a las informaciones léxicas de las expresiones constituyentes. Entre éstos, se pueden distinguir esencialmente dos tipos de enfoques: el primero (basado en el modelo *garden path* de Frazier L. 1989) se caracteriza por dar una mayor preeminencia a la sintaxis. Inspirándose en el generativismo chomskyano, postula que el proceso de construcción de la estructura sintáctica de una oración se efectúa tomando en cuenta únicamente informaciones de naturaleza morfosintáctica.

La resolución de los fenómenos de ambigüedad se relegan de esta manera a una segunda etapa, donde se da acceso a la información léxica de las expresiones constituyentes; el otro enfoque (McRae et al., 1997), por el contrario, presenta el procesamiento de la oración como un mecanismo que da acceso simultáneamente a informaciones de naturaleza morfosintáctica, léxica y, eventualmente, pragmático-discursiva: la situación de enunciación, los conocimientos compartidos por el locutor y el/los oyente(s)... Este enfoque rechaza por tanto la autonomía de la sintaxis. La construcción de la estructura sintáctica depende de informaciones léxico-pragmáticas. En otros términos, la interpretación de un enunciado se efectúa en el proceso mismo de construcción de su estructura sintáctica. Es lo que se conoce por el procesamiento *on line*.

Teniendo en cuenta que el polimorfismo gramatical y la polisemia léxica son dos fenómenos de naturaleza semántica, la desambiguación de expresiones polimórficas y polisémicas se debe llevar a cabo en un proceso de construcción de la significación en el que se dé acceso simultáneamente a informaciones morfosintácticas y léxicas, es decir en un procesamiento *on line*.

El objetivo de la parte constructiva de este artículo será el de modelizar en el espacio lógico-semántico el proceso de construcción *on line* de la significación. Para ello, analizaremos, en el interior de la estructura de argumentos de un predicado, el mecanismo de saturación de los papeles de un predicado, en particular, nos centraremos en la operación de asignación de una entidad a un papel predicativo.

2. Un esbozo[2] de modelización del procesamiento *on line* de expresiones complejas

Basaremos la modelización de este procesamiento en la concepción formal de un predicado como una operación de saturación de sus papeles internos. Tal concepción es el eje central en torno al cual se caracterizan las entidades del espacio semántico en las versiones actualizadas de la teoría de situaciones (FRACAS 1994, Chambreuil M. et al. 1998).

2.1. Saturación de los papeles de un predicado

Un predicado puede ser analizado como una operación que, asignando un conjunto de entidades a sus papeles, da como resultado una entidad integradora de orden superior. En el proceso de resolución de esta operación, se pueden distinguir, por tanto, tres tipos de objetos: (i) el operador predicativo y sus papeles, que conforman la operación (o función) predicativa ; (ii) las asignaciones de entidades a los papeles predicativos : los argumentos de la función ; (iii) y la entidad integradora, valor de la función. La entrada verbal 'descargar', por ejemplo, podría denotar[3] en el espacio semántico una función predicativa con, al menos, dos asignaciones: **(1)** $\lambda(X)^{\text{sujeto}}\,\lambda(Y)^{\text{objeto}}\,(DESCARGAR\ ;\ (X)^{\text{sujeto}},\ (Y)^{\text{objeto}})$

Nótese que en (1), los objetos lambda (resultantes de las operaciones de l-abstracción) no son parámetros de entidades, sino asignaciones de parámetros a papeles predicativos. La interpretación de la oración 'Chema descargó el camión' puede asociarse por tanto al proceso de saturación de los papeles de la función predicativa de (1). La aplicación de esta función a las asignaciones $(chema)^{\text{sujeto}}$ y $(camión)^{\text{objeto}}$, donde *chema* y *camión* representan las entidades denotadas respectivamente por 'Chema' y 'el camión' , da como resultado, no un valor de verdad V o F (como en la lógica de predicados), sino una entidad individualizada, *descargar-chema-camión*, donde se integran las entidades asignadas. La entidad integradora designa el evento en el que Chema descarga el camión. Como en la teoría de propiedades, una expresión verbal temporal puede asociarse a la función predicativa, función que representa el **modo de ser** composicional del verbo, mientras que una nominalización verbal se asocia al resultado de la función, es decir a la entidad individualizada como el evento designado por la expresión. Esta doble caracterización objeto -composicional y evento- permite tratar el polimorfismo de las expresiones de naturaleza verbal.

Sin embargo, queda todavía un problema por resolver. Un mismo lexema verbal puede asociarse a un gran número de funciones predicativas. Por ejemplo, el lexema 'descargar' en las oraciones 'Chema descargó el camión de sacos' y 'Chema descargó el camión sobre la empalizada' se asocia a dos funciones predicativas diferentes : *DESCARGAR1* (acción de modificar un espacio-lugar) y *DESCARGAR2* (desplazamiento de un objeto). Se trata por tanto de un lexema polisémico que contiene, al menos, dos significados, es decir dos procesos de composición diferentes. Como cada significado representa en realidad un proceso composicional, la

elección de uno u otro (es decir la desambiguación) se efectúa antes de que se inicie el proceso composicional de saturación de los papeles predicativos. En otros términos, antes de comenzar el proceso de interpretación de la oración, es necesario elegir uno de los significados composicionales del verbo. La desambiguación no se realiza por tanto al mismo tiempo que se precisa el significado de las expresiones que se combinan en el interior de la oración: no hay procesamiento *on line*. Este análisis de la noción de predicado nos lleva al postulado siguiente: el eje del mecanismo composicional no es el pro-ceso de saturación de los papeles predicativos; la composicionalidad se configura más bien a un nivel inferior en el análisis de la predicación, concretamente en el interior de la operación de asignación. El análisis de esta operación nos permitirá: caracterizar las subcategorías básicas de entidades individuales de nuestro modelo, subcategorías por medio de las cuales podremos tratar el fenómeno del polimorfismo gramatical; caracterizar un mecanismo composicional basado en la precisión gradual del significado de las expresiones (polisémicas) combinadas.

2.2. Asignación de una entidad a un papel predicativo

La operación de asignación puede definirse como una función con dos argumentos -la entidad asignada al papel predicativo y la entidad que individualiza la predicación- que los combina e integra en una entidad de orden superior: la entidad compleja resultado de tal combinación. Formalmente, una operación de asignación es un caso particular de función predicativa. La asignación de *chema* al papel sujeto del operador predicativo *DESCARGAR* puede representarse como una función cuyos argumentos son $(descargar)^{sujeto^-}$ y $(chema)^{sujeto-}$, y cuyo resultado es la entidad *descargar-chema*, que integra en una unidad individualizada la entidad *chema*, asignada al papel sujeto, y el evento *descargar*. La entidad compleja *descargar-chema* es el evento asociado a la expresión verbal 'Chema descargó...' (los tres puntos representan el hecho que puede haber otras asignaciones que saturen la expresión verbal). La flecha descendente simboliza el hecho que la entidad que desempeña ese papel **busca** los elementos constituyentes que van a venir a integrarse a su estructura: la entidad *descargar* es el evento donde se integra *chema*. La flecha ascendente simboliza el hecho que la entidad que desempeña ese papel **busca** la entidad que pueda integrarla: la entidad *chema* se integra en el evento *descargar*.

En el caso de los predicados verbales, las operaciones de asignación representan en realidad los objetos semántico-composicionales asociados a las funciones sintácticas. De esta manera, el sujeto puede caracterizarse a partir de la función predicativa (2): **(2)** $\lambda(X)^{sujeto^-}\ \lambda(Y)^{sujeto-}\ (SUJETO\ ;\ (X)^{sujeto^-},\ (Y)^{sujeto-})$. La aplicación de esta función a las asignaciones $(descargar)^{sujeto^-}$ y $(chema)^{sujeto-}$, donde *descargar* y *chema* representan las entidades denotadas respectivamente por 'descargar' y 'Chema', da como resultado la entidad compleja *descargar-chema*, asociada a 'Chema descargó...'.

2.2.1. Caracterización de dos subcategorías de entidades individuales

Los diferentes papeles de los operadores de asignación caracterizan dos tipos de entidades individuales:
- la entidad asignada al papel descendente se conceptualiza como el todo integrador con respecto a sus entidades constituyentes. A este tipo le llamaremos **dominio**.
- la entidad *descargar* denotada por el verbo 'descargar' en 'Chema descargó...' se conceptualiza como el dominio de la expresión. La anotaremos *$descargar*.
- la entidad asignada al papel ascendente - se conceptualiza como un constituyente inserto en el dominio. A este tipo de entidad, le llamaremos **átomo**. La entidad *chema* asociada al nominal 'Chema' en 'Chema rompe...' se conceptualiza como el átomo de la expresión. La anotaremos *#chema*.

El resultado de la función de asignación es una entidad compleja categorizada como un dominio o como un átomo. En la expresión verbal 'Chema descargó...', el resultado de la operación es una entidad caracterizada como un dominio complejo: *$descargar-chema*. La caracterización de la categoría de la entidad compleja depende de las propiedades composicionales del tipo de función de asignación. La función de sujeto verbal no posee las mismas propiedades composicionales que, por ejemplo, la función de modificador nominal.

Los objetos composicionales no solamente se asocian, por tanto, a las marcas de funciones sintácticas verbales, sino también a toda marca de relación morfosintáctica: modificadores nominales (adjetivos, complementos preposicionales, relativas...), modificadores verbales (adverbios, complementos preposicionales...), etc.

2.2.2. Caracterización interna de los objetos composicionales

Los mecanismos de composición semántica de los que disponemos son las funciones que designan las operaciones de asignación a los papeles predicativos. A estas funciones se le pueden asociar condiciones semánticas que restringen la naturaleza de las entidades combinadas. Distinguimos dos tipos de condiciones semánticas:
- las condiciones categoriales que restringen la subcategoría de las entidades combinadas : dominio o átomo.
- las condiciones conceptuales que delimitan la clase conceptual específica de las entidades combinadas : eventos, situaciones estáticas, objetos físicos, localizaciones, seres humanos, dimensiones físicas...

Las condiciones categoriales se precisan en gran parte por medio de marcas lingüísticas de naturaleza morfosintáctica. Las condiciones conceptuales, en cambio, se precisan por medio de marcas de naturaleza léxica.

En la expresión compleja 'Chema descargó...', las marcas morfosintácticas relativas a la función de sujeto pueden asociarse al objeto composicional siguiente: **(3)** $\lambda(\$X)^{sujeto^-}\ \lambda(\#X)^{sujeto-}(SUJETO\ ;\ (\$X)^{sujeto^-},\ (\#X)^{sujeto-})$

Este objeto especifica, con respecto a (2), las condiciones categoriales de las entidades combinadas, en concreto pone en relación un dominio con un átomo para obtener como resultado un dominio complejo integrador.

Las expresiones léxicas 'descargar' y 'Chema', por su parte, añaden a (3) las restricciones conceptuales adecuadas: (i) la operación *SUJETO* pasa a ser *AGENTE*, operación específica que designa la integración de una entidad agentiva en una acción ; (ii) el dominio *$X* pasa a ser una acción agentiva

$ACTION, que queda todavía indeterminada con respecto al hecho de si se trata de un desplazamiento de objetos, o bien de una acción de modificación de un espacio-lugar ; (iii) el átomo *#X* pasa a elaborarse como un ser agentivo *#ENT-AGENTIVA*.. El objeto composicional específico así constituido es: **(4)** l(*$ACTION*)$^{agente^-}$ l(*#ENT-AG*)$^{agente^-}$ (*AGENTE* ; (*$ACTION*)$^{agente^-}$, (*#ENT-AG*)$^{agente^-}$). Este objeto representa la función que se aplica a las asignaciones (*$descargar*)$^{agente^-}$ y (*#chema*)$^{agente^-}$, para construir la entidad integradora *$descargar-chema*, entidad que pertenece, por un lado, a la categoría de los dominios, y por otro lado, a la clase conceptual de las acciones agentivas, clase todavía indeterminada.

2.3. Polimorfismo gramatical y categorización semántica

En la separación entre categorización semántica y clasificación conceptual se encuentra la clave para poder caracterizar y modelizar el polimorfismo gramatical; las expresiones '...descargó...' y 'la descarga...' se asocian a dos entidades que se categorizan respectivamente como un dominio y como un átomo: el dominio *$descargar* y el átomo *#descargar*. Estas dos entidades, a pesar de categorizarse de diferente manera, pertenecen a la misma clase conceptual: las dos designan una acción de descarga (Gamallo P. 1998).

2.4. La desambiguación de expresiones polisémicas y la construcción dinámica de la significación

El procesamiento *on line* de expresiones complejas se basa en la evolución progresiva del discurso. El resultado del procesamiento de una expresión puede aportar nuevas condiciones conceptuales que restringen y precisan el procesamiento de la siguiente expresión. O a la inversa, si la primera expresión procesada da lugar a una entidad todavía polisé-mica, las restricciones aportadas por el procesamiento de la siguiente expresión pueden permitir la determinación de una significación precisa de la primera expresión. La dinámica del procesamiento *on line* se basa precisamente en la herencia de restricciones en el proceso de elaboración de los objetos composicionales que combinan las entidades constituyentes.

Analicemos brevemente el procesamiento de la expresión 'la harina', una vez procesada la expresión compleja 'Chema cargó...'. La combinación entre 'Chema cargó...' y 'la harina' se lleva a cabo a partir de la explotación de las marcas sintácticas de objeto directo, marcas que determinan la elaboración del objeto composicional siguiente: **(5)** l(*$X*)$^{odirecto^-}$ l(*#X*)$^{odirecto^-}$ (*ODIRECTO* ; (*$X*)$^{odirecto^-}$, (*#X*)$^{odirecto^-}$)

En cuanto a las condiciones léxicas, el resultado del procesamiento de 'Chema cargó...' y la explotación del nombre 'harina' precisan el contenido conceptual de las entidades combinadas, en concreto las condiciones de 'harina' determinan que el átomo asignado designe una substancia física y no un espacio localizador. Tal restricción impide que el evento de descargar sea clasificado como una acción de modificación de un espacio-lugar. Por consiguiente, la descarga se precisa como un desplazamiento de objetos. La función composicional definida en (5) se elabora en consecuencia como una operación de integración de un átomo designando una substancia física en un dominio designando un desplazamiento directivo: **(6)** l(*$DESPL*)$^{desplazado^-}$ l(*#OBJ-FIS*)$^{desplazado^-}$ (*DESPLAZADO* ; (*$DESPL*)$^{desplazado^-}$ (*#OBJ*)$^{desplazado^-}$)

La aplicación de este objeto composicional a las asignaciones (*$descargar-chema*)$^{desplazado^-}$ y (*#harina*)$^{desplazado^-}$, da como resultado el dominio complejo *$descargar-chema-harina*, entidad no polisémica denotada por 'Chema descargó la harina...', que pertenece a la clase conceptual correspondiente a las acciones de desplazamiento de objetos.

3. Conclusión

La originalidad de nuestro modelo formal del espacio semántico radica en la caracterización de los objetos composicionales a partir del análisis de la operación de asignación de una entidad a un papel predicativo. Tal caracterización viene motivada por el hecho de que permite dar cuenta, en un marco teórico coherente, del polimorfismo gramatical de las expresiones lingüísticas y del proceso de desambiguación (o de determinación) de la polisemia (o indeterminación) léxica. La brevedad de este artículo nos impide, no sólo mostrar detalladamente la coherencia interna de nuestra modelización, sino también profundizar de manera crítica en las hipótesis y nociones fundamentales en las que basamos tal modelización. No en vano, la reflexión crítica que nos ha llevado a formular este conjunto de hipótesis ha sido y es el producto de un estudio pluridisciplinar donde se abordan diferentes tipos de fenómenos lingüísticos desde el menos tres enfoques complementarios : el enfoque de la semántica formal (o logicista), el enfoque de la semántica cognitiva, y el enfoque ligado al procesamiento informático del lenguaje natural.

4. Referencias bibliográficas

Chambreuil M., Ben Gharbia A., Bernigot C., Gamallo Otero P., Panissod C., Reinberger M-L. (1998). *Théories sémantiques pour la langue naturelle*. Paris, Hermès en prensa.

Chierchia G. & Turner R. (1988). Semantics and Property Theory. *Linguistics and Philosophy*, vol 11, n° 3, (pp. 261-302).

FRACAS (1994). *Describing the Approches* (D8). Informe interno del proyecto Framework for Computational Semantics.

Frazier L. (1989). Against lexical generation of syntax. En William Marslen-Wilson (ed.), *Lexical representation and Process*, pp. 505-528.

Gamallo Otero P (1998). *Construction conceptuelle d'expressions complexes: traitement de la combinaison "nom-adjecif"*. Tesis doctoral de la universidad Blaise Pascal Clermont 2.

Langacker R. (1987, 1991). *An introduction to Cognitive Grammar*. Vol I y II, Standford University Press.

McRae K., Ferreti T.R. & Amoyte L. (1997). Thematic Roles as Verb-specific Concepts. En M. C. MacDonald (ed.), *Lexical Representations and Sentence Processing*, pp. 137-176.

Pustejovsky J. (1995). *The Generative Lexicon*. MIT Press: Cambridge.

Notas

[1] Como el objetivo de este artículo no es el de describir y caracterizar los diferentes tipos o grados de ambigüedad, situados en la escala gradual que va de la homonimia a la indeterminación pasando por la polisemia, no marcaremos ninguna diferencia significativa en el uso de los términos "ambigüedad", "polisemia" o incluso "indeterminación".

[2] En Gamallo Otero P. (1998), se realiza una elaboración detallada de esta modelización.

[3] A lo largo del artículo, los términos "denotar" y "asociar" son empleados indistintamente para referirse a la relación entre una expresión o índice lingüístico y el objeto semántico correspondiente.

Seguridad

Desarrollo de politicas de seguridad en entornos de red con cortafuegos

Javier Areitio Bertolín, Julián Marcelo
**Redes y Sistemas. ESIDE, Facultad de Ingeniería, Universidad de Deusto (UD); ** Riesgos y Seguridad en los Sistemas de Información. Universidad Politécnica de Valencia (UPV)*

Jareitio@orion.deusto.es
julian.marcelo@sema.es

1. Seguridad en entornos de red

Los mecanismos de salvaguarda de las redes de comunicaciones 'no locales' entre sistemas-nodos de parecido o distinto nivel han de tener en cuenta que los canales de transporte contratados a proveedores externos pueden tener problemas de seguridad (acceso de terceras partes) fuera del dominio propio. Estas redes suelen presentar ese y otros problemas especiales de seguridad, pues:

- son más complejas que los equipos individuales tanto por estructura como por coordinación;
- comparten medios físicos, dispositivos de enlace y equipos accesibles;
- su perímetro es difuso, con recursos y usuarios locales que se prolongan a entornos remotos;
- los puntos de amenaza se distribuyen en múltiples sitios del viaje de la información;
- el acceso remoto permite a usuarios desconocidos acceder anónimamente a las 'puertas' de los equipos, camuflando su identidad tras varios equipos y medios; los controles de autenticación y acceso han de funcionar así en un entorno más agresivo e incierto;
- la multiplicidad de rutas posibles entre dos equipos deja su elección fuera del control de los usuarios o las aplicaciones, incluso en redes de complejidad media.

Este escenario conlleva la posibilidad de amenazas de los siguientes tipos:

- ***Intercepción (lectura) de datos en tránsito,*** accediendo a su contenido o a su sola existencia (análisis de tráfico).
- ***Modificación de datos en tránsito***, con aparición de un 'tercero interpuesto' *man in the middle* que actúa de repetidor neutro durante la mayor parte del tiempo, pero que eventualmente puede retransmitir variantes alteradas de lo que recibe.
- ***Acceso (lectura)*** no autorizado a programas y/o datos en equipos remotos.
- ***Modificación*** de programas y/o datos en equipos remotos.
- ***Ejecución de programas*** en equipos remotos.
- ***Suplantación*** de la personalidad de un usuario autorizado.
- ***Reproducción ciega de transacciones*** registradas anteriormente.
- ***Bloqueo de tráfico*** (total, parcial o selectivo) realizado de forma pasiva (deja perder paquetes en tránsito) o activa (se inyecta ruido en la red).

El concepto de 'cortafuegos' se ha popularizado con la difusión de Internet. Muchas organizaciones han conectado o se plantean la necesidad de conectar sus redes internas privadas (Intranets, para seguir la terminología en auge) a redes externas. La falta de dominio sobre la seguridad de éstas no debe privar a sus usuarios de dominar la seguridad de la Intranet propia y de acceder a la amplia panoplia de servicios externos, gobernados por todo tipo de protocolos, que por ejemplo proporciona Internet; sean en este caso servicios de consulta y transferencia como *ftp, tftp, telnet, www/ http, rlogin, network file system NFS, network news transfer protocol NNTP*; sean servicios de correo como SMTP/ POP3/IMAP4 (*post office protocol v.3 / Internet message access protocol v.4*).

Conviene recordar que Internet se diseñó para ofrecer gran seguridad sobre su disponibilidad global (frente a grandes catástrofes), pero no sobre la confidencialidad, autenticidad e integridad que han de garantizar muchas organizaciones privadas. Partiendo del principio de que la seguridad absoluta es una asíntota no alcanzable, las versiones actuales de TCP/IP tienen problemas técnicos de seguridad como éstos:

- ***Escucha clandestina y falsificación fáciles.*** La mayor parte del tráfico Internet no está cifrado. El correo, las con-traseñas y las transferencias de ficheros se pueden monitorizar y capturar utilizando fácilmente el software disponible.
- ***Servicios TCP/IP muy vulnerables,*** particularmente los de prueba y testeo.
- ***Complejidad de configuración*** de los controles de acceso de seguridad a los computadores; si se configuran involuntaria pero incorrectamente, permiten peligrosos accesos no autorizados.

Pero la inseguridad en la conexión a las redes externas de las organizaciones se debe sobre todo a que muchas de éstas carecen de política de seguridad, entendida como un conjunto de decisiones racionales respecto a las medidas adecuadas para protegerse eficazmente. Muchas organizaciones configuran el acceso a Internet sin tener en cuenta los posibles abusos desde ésta; abren más servicios TCP/IP de los que requieren sus operaciones, con el consiguiente acceso de información de y sobre su red interna a los intrusos. De acuerdo con un informe de Datapro, sólo el 46% de las empresas españolas (frente al 69% de la media europea) disponen de una política de seguridad para sus sistemas de información (los datos serían aún más pesimistas si se refirieran a las redes).

2. Filtros y Cortafuegos

Los dos mecanismos básicos para afrontar las amenazas a la red interna desde las externas son:

- Filtros para control de los flujos de información (acceso, rutas y accesibilidad de terceras partes)
- Cortafuegos para proteger la información en sí (de su confidencialidad e integridad).

Los **Filtros** se establecen para controlar los flujos de información en los nodos siempre que sea posible. Conviene recordar que los nodos-conectores de una red se suelen clasificar en tres niveles:

·Un conector de nivel 1 o ***repetidor*** se emplea dentro del mismo edificio para enlazar equipos cuya comunicación directa supere las características físicas del medio; no puede contener filtros, lo que tiene escaso impacto pues la zona debe estar controlada con otras políticas de seguridad.

·Un conector de nivel 2 o ***puente*** *(bridge)* enlaza dos subredes y reproduce el tráfico de una en otra si su origen y destino están a cada lado del puente; éste suele aprender dinámicamente qué equipos hay en ambas subredes a base de escuchar las emisiones y se suele emplear para distribuir tráfico y atajar la saturación del medio también dentro del mismo edificio, por lo que la carencia de mecanismos de filtrado también tiene escaso impacto.

·Un conector de nivel 3-4 o ***enrutador*** *(router)* suele enlazar dos redes unidas por canales externos al edificio atendiendo a direcciones de red y por tanto suele poder clasificar los paquetes por tipos de protocolo. Esta topología siempre tiene al menos dos puertos (más si la conexión se estructura en forma de estrella).

La política de seguridad de un ***enrutador*** exige mecanismos de filtrado específicos que han de tomar en consideración tres parámetros: las direcciones de red del remitente y del destinatario; así como el tipo de servicio (que puede inferirse del puerto al que va dirigido y/o del que procede, ya que el par 'dirección-puerto' permite identificar con relativa solvencia qué servicio soporta el paquete). En base a estos parámetros, el filtro autorizará o denegará el tránsito de un paquete desde un puerto a otro de los controlados por el enrutador, con una política de seguridad del tipo 'todo denegado salvo autorización expresa' que se plasmará en el control de configuración del sistema. Para implantar una política de seguridad en el enrutador se siguen estos pasos:

·Identificar al responsable de autorizar nuevas reglas y dar de baja reglas antiguas.

·Identificar al responsable de configurar los equipos.

·Asociar direcciones de red a puertos del enrutador de forma estricta para inhibir la posibilidad de que un nodo en una red enmascare a un nodo de otra (*spoofing*).

·Desarrollar una batería de pruebas -tests de regresión- que valide la implantación de la política de seguridad elegida (las pruebas se ejecutan cada vez que se altere la configuración por nueva política, inclusión o eliminación de reglas, cambio de equipo o versión de *software* o *firmware).*

·Registrar en el libro de operación del sistema las actuaciones y los resultados de las pruebas.

Un Cortafuegos (*firewall*) es un mecanismo de filtrado que aisla una 'ciudadela segura', tratando de identificar los puntos de acceso vulnerables en el 'perímetro' y de concentrar en ellos la política de seguridad en tránsito que se desee. En el caso más típico, el cortafuegos aísla una red privada del entorno constituido por la red pública externa; pero el modelo sirve también para aislar dos redes privadas entre sí cuando las características de seguridad de ambas difieren notablemente.

El cortafuegos (mejor se llamaría puente levadizo) impone una política de acceso desde/hacia la red exterior, lo que parece poder relajar la política interna de seguridad de la red protegida (se deja circular dentro con más libertad). Pero el cortafuegos no influye en la política de seguridad interna y no reduce los riesgos de ataques originados internamente y dirigidos a los equipos internos.

La política de acceso que soportaría un cortafuegos es incluso la única posible en ciertos casos:

·en entornos donde la implantación de controles de acceso estrictos no es viable en todos y cada uno de los equipos; o donde la información transita 'en claro' (sin cifrar) por segmentos comunes

·en redes complejas cuya cantidad de equipos desborde la capacidad de administrar la seguridad por su responsable; éste sólo podrá imponer, mantener y monitorizar una política de seguridad con solvencia centralizando su materialización en un sólo punto y en forma de cortafuegos.

El cortafuegos se materializa con un equipo único que proporciona toda la funcionalidad o con equipos separados (software, enrutador, servidor e incluso red) cuya combinación ofrece el efecto deseado. Se puede así requerir un cortafuegos multinivel, es decir una mini-red interna que se conoce como 'red de nadie' o 'desmilitarizada'. Alrededor de este segmento de red se disponen enrutadores de acceso y/o servidores ('bastiones') que hospeden los *proxies* o programas correspondientes. Esta arquitectura dota al cortafuegos de una capacidad de concentrador, muy útil cuando hay que disponer varias puertas bajo su control. La arquitectura multinivel dota al sistema de niveles de defensa en profundidad: un ataque con éxito a uno de los componentes no conlleva la penetración inmediata; los mecanismos de alarma deben detectar la intrusión y avisar al administrador, que dispone de cierto tiempo para reaccionar antes de que se logre penetrar la siguiente barrera. Así, un cortafuegos no es un componente único, sino un concepto estratégico diseñado para proteger los recursos de la organización que pueden alcanzarse a través de Internet.

3. Tipos de cortafuegos

El cortafuegos es un dispositivo con funciones de separación, limitación y análisis, que al menos dispone de dos puertas y controla en todo caso el flujo de información entre dos de las posibles puertas. Su principal función es el control de acceso centralizado, cuya efectividad excluye poder acceder sin cruzarlo de/a las redes internas por usuarios internos/exteriores/remotos. Así, si un viajante de una empresa puede llamar mientras viaja a su PC de la oficina por medio de línea pública y modem, con ese PC conectado a la red interna protegida de la organización, un atacante puede llamar a ese PC directamente y se salta así el cortafuegos que protege la red interna de la organización. Si un usuario accede, desde su PC de la oficina utilizando el modem y la red telefónica conmutada, a su cuenta Internet abierta en un ISP (Proveedor de Servicios Internet), está abriendo una conexión no segura con Internet que se salta la protección del cortafuegos.

Un cortafuegos proporciona diversos tipos posibles de protección:

·registra el tráfico que sale o llega a la red privada;

·bloquea tráfico no deseado;

·dirige el tráfico entrante a sistemas internos preparados para tal fín, más confiables;

·oculta identificadores (topología y dispositivos de red, sistemas y usuarios internos de Internet);

·oculta sistemas vulnerables que no pueden hacerse fácilmente seguros de Internet;
·proporciona una autentificación más robusta que la de las aplicaciones estándar.

Pero conviene también aclarar otras protecciones que NO proporcionan los mitificados cortafuegos:
·no protegen contra amenazas 'inteligentes' intencionales internas (en el dominio de la intranet);
·no protegen contra amenazas derivadas de conexiones con el exterior que no pasan por él;
·no protegen contra virus ni amenazas no catalogadas.

Para protegerse de estas amenazas habrá que combinar el cortafuegos con otros mecanismos de salvaguarda.

Como en todo mecanismo de protección, el cortafuegos es un compromiso entre conveniencia y seguridad. Se llama transparencia a la visibilidad del cortafuegos tanto para los usuarios de dentro como los de fuera que lo atraviesan. Un cortafuegos es 'transparente' para los usuarios si éstos no se dan cuenta de su presencia ni deben detenerse en él para poder acceder a la red. Los cortafuegos normalmente se configuran para ser transparentes a los usuarios de la red interna (mientras no se encuentren fuera del cortafuegos), pero no transparentes para todas las redes externas que deseen atravesar el cortafuegos. Esta política proporciona generalmente un nivel muy alto de seguridad sin cargar excesivamente a los usuarios internos.

El cortafuegos puede trabajar en tres niveles:
·*al nivel de la red,* controlando el trasiego de paquetes individuales (se denomina ***'apantallado'***).
·*al nivel de aplicación,* controlando el acceso a servicios individuales (se denomina ***'proxy'***).
·*al nivel de agente* activo, entrando a controlar el contenido de los accesos a los servicios (evitando virus, impidiendo el acceso a servicios de carácter no profesional, imponiendo límites al volumen de información en tránsito, etc.).

El cortafuegos debe tener características y capacidades distintas según trabaje en uno u otro nivel:
·*volumen de tráfico* a gestionar, creciente desde el nivel de red al de aplicaciones que controlan el contenido.
·*capacidad de control:* muy superior para el nivel de aplicación que para el nivel de red.
·*registro de uso:* indiferenciado al nivel de red y con clasificación por servicios al de aplicación.
·*identificación del usuario:* prácticamente imposible al nivel de red, pero posible al de aplicación (se llega a delegar en el cortafuegos toda la política de control de acceso, desde el exterior o el interior).

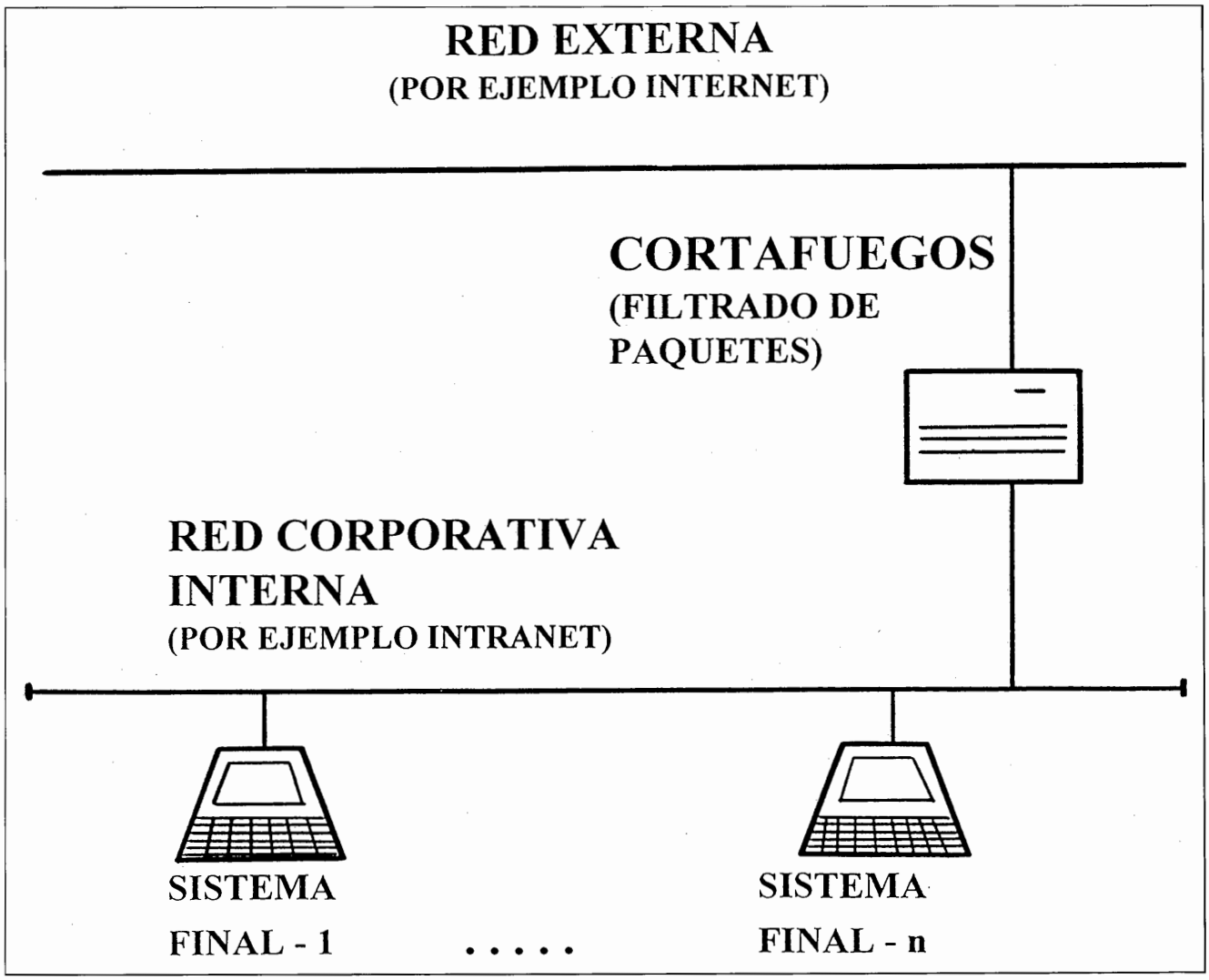


Figura1: Localización típica de un cortafuegos en un Entorno de Red

En definitiva, el cortafuegos consiste en un dispositivo informático (un enrutador o un computador) que separa físicamente un dominio de red de otro. Los enrutadores pueden controlar el tráfico en el nivel de red/transporte permitiéndolo o denegándolo selectivamente en base a la dirección fuente/destino y al número de puerto. Los computadores pueden controlar el tráfico en el nivel de aplicación. Los cortafuegos aplican un conjunto de operaciones de filtrado de paquetes del nivel red/transporte, tomando así decisiones de seguridad basadas en la información (dirección fuente y número de puerto). que proporcionan por ejemplo las cabeceras IP y TCP.

4. Cortafuegos al nivel de Red

El propósito de este cortafuegos, también llamado de ***Filtrado de Paquetes,*** es proporcionar un punto de defensa y de acceso controlado y auditado para servicios, desde dentro y desde fuera de una red privada de la organización, permitiendo y/o denegando el flujo de paquetes a su través, con lo que proporciona control de acceso a dicha red. La **figura** muestra un cortafuegos instalado entre dos redes para encaminar el tráfico entre ellas a su través.

Este cortafuegos suele materializarse por medio de un enrutador con filtros que proporcionan el control solicitado, utilizando reglas de filtrado de paquetes para conceder o denegar el paso de éstos al interior en base a la dirección fuente, a la dirección destino y al puerto. Ofrecen una seguridad mínima, pero su costo es muy bajo y pueden ser una alternativa apropiada para entornos de bajo riesgo. Son rápidos, flexibles y transparentes. Las reglas de filtrado no suelen poder mantenerse fácilmente en el enrutador, pero se dispone de herramientas para simplificar las tareas de crear y mantener esas reglas.

Los riesgos de los cortafuegos basados en el filtrado de paquetes son:

- El enrutador cuenta sólo con las direcciones origen y destino y los puertos contenidos en la cabecera del paquete IP para permitir o no el acceso de tráfico a la red interna.
- Un atacante tendrá acceso directo a cualquier equipo de la red interna una vez que el cortafuegos le haya concedido acceso.
- El enrutador no protege contra el *'spoofing'* -engaño- de direcciones DNS ó IP.
- El enrutador proporciona poca o nula información útil de registro -*'logging'*.
- Algunos cortafuegos de filtrado de paquetes no soportan la autentificación fuerte de usuarios.

El Cortafuegos de Filtrado de Paquetes no es aceptable para Entornos de Alto Riesgo (por ejemplo hospitales); ofrece una seguridad mínima para Entornos de Riesgo Medio (por ejemplo, Universidades); y puede ser la elección recomendable para Entornos de Bajo Riesgo.

5. Cortafuegos al nivel de Aplicación

Estos cortafuegos ejecutan programas servidor denominados *proxies* (apoderados) que, como su nombre indica, tratan con los servidores externos -de Internet- en nombre de clientes internos -que solicitan servicios. O bien examinan las peticiones externas y las reenvian peticiones legítimas al servidor interno para que proporcione el servicio apropiado.

Estos cortafuegos se consideran más seguros que los simples filtros y ofrecen ventajas a una organización que tenga riesgos medio-altos como las siguientes:

- Este cortafuegos puede configurarse como la única dirección de computador visible para la red externa, requiriendo que todas las conexiones hacia/desde la red interna se realicen a su través.
- La utilización de *proxies* para los diferentes servicios impide el acceso directo de la red interna a servicios externos, protegiendo a la organización incluso contra las vulnerabilidades de los computadores internos mal configurados o no seguros.
- Este cortafuegos también soporta funciones de autentificación fuerte del usuario.
- Los *proxies* pueden proporcionar registro (*logging*) detallado en el nivel de aplicación. Los cortafuegos del nivel de aplicación deberían configurarse de modo que el tráfico de red externo aparezca como si lo originasen ellos (es decir, sólo el cortafuegos es visible para las redes externas). De esta forma, no está permitido el acceso directo a los servicios de red de la red interna y así mismo todas las peticiones entrantes para los diferentes servicios de red (telnet, ftp, http, rlogin, etc.) deben ir a través del *proxy* apropiado (uno por servicio) sin tener en cuenta cuál será el computador de la red interna destinatario final del servicio.

Si se requiere un servicio que no esté soportado por un *proxy*, se tienen tres posibilidades:

- denegar el servicio Internet hasta que el fabricante del cortafuegos desarrolle un *proxy* seguro (alternativa preferida cuando los nuevos servicios poseen vulnerabilidades no aceptables);
- desarrollar un *proxy* a medida (opción difícil que sólo puede emprenderse con técnicas sofisticadas);
- pasar el servicio directamente a través del cortafuegos con un filtrado más reducido de paquetes, usando 'configuraciones', lo que puede limitar algunas de las vulnerabilidades pero puede comprometer la seguridad de los sistemas internos situados tras el cortafuegos.

Cuando el servicio Internet no soportado por un *proxy* sea interno (dentro de la frontera de seguridad), también se pasa a través del cortafuegos, después que el administrador de éste defina el *plug* que permita el servicio pedido. Cuando esté disponible un *proxy* del fabricante del cortafuegos, se inhabilitará el *plug* y el *proxy* se hará operativo. Todos los servicios Internet internos deben procesarse por software *proxy* del cortafuegos. Si se pide un nuevo servicio, éste se denegará hasta que se disponga de un *proxy* del fabricante del cortafuegos y se verifique por el administrador del cortafuegos. Se puede desarrollar un *proxy* a medida por la propia organización o por otros fabricantes, pero sólo se podrá utilizar tras aprobarse por el responsable de seguridad.

Los Cortafuegos del Nivel de Aplicación son una opción efectiva para Entornos de Alto Riesgo; la elección recomendada para los de Riesgo Medio; y una elección aceptable pero costosa para los de Bajo Riesgo.

6. Cortafuegos Híbridos

Muchos Cortafuegos combinan los tipos anteriores y los implementan en serie -lo que mejora la seguridad total- más que en paralelo -porque el perímetro de seguridad de red sólo será tan seguro como el menos seguro de los tipos utilizados.

La combinación híbrida depende de los servicios que requieran los usuarios y del nivel de riesgo que acepten. Por ejemplo el filtrado de paquetes maneja con más efectividad ciertos protocolos (Telnet, SMTP) y los servidores *proxy* otros (FTP, WWW).

Cada tipo de cortafuegos puede asumir mejor unas u otras funciones. Así un enrutador puede asumir bien éstas dos:

- *Gestión de direcciones.* Internet tiene rangos de direcciones reservados para redes privadas; dichas redes no se anuncian públicamente y se aísla así efectivamente el encaminamiento, que queda reducido al nicho local; se utiliza un mecanismo de traducción dinámica de direcciones (NAT, *Network Address Translation*) para que se puedan establecer enlaces entre el interior y el exterior (habitualmente en ambos sentidos).
- *Cifrado entre enlaces.* El dispositivo que actúa de cortafuegos tiene la ubicación idónea para establecer canales seguros de comunicaciones con otros cortafuegos remotos separados de aquél por redes no confiables.

Por su parte con un cortafuegos al nivel de aplicación ni se plantea la problemática de direcciones privadas aisladas pues no tiene canales directos y todo tiene que pasar por la aplicación *proxy* que hace de intermediario. Sin mebargo la problemática de los canales cifrados entre aplicaciones se puede implantar cómodamente dentro de la funcionalidad *proxy,* lo que además puede eliminar el requerimiento de alterar las aplicaciones cliente y servidor en sí mismas.

En entornos de medio a elevado riesgo, un cortafuegos híbrido puede ser la elección ideal. Sería así la elección recomendada para Entornos de Alto Riesgo; una opción efectiva para los de Riesgo Medio; y una elección aceptable para los de Bajo Riesgo.

7. Amenazas a los cortafuegos

El cortafuegos se diseña para que sea el punto de ataque donde se concentren las amenazas. Un cortafuegos de nivel red/transporte puede estar sometido a dos grandes grupos de amenazas, unas genéricas y otras operacionales (o sea, referidas al entorno de las operaciones):

El ***Grupo de Amenazas Genéricas*** comprende las causadas por los siguientes agentes:

- Personas no autorizadas pueden ganar acceso lógico al cortafuegos.
- Personas no autorizadas de una red externa pueden suplantar a un sujeto de la red interna, llevando a cabo ataques de *spoofing* -'engaño'- en direcciones de red, por ejemplo *spoofing* IP desde una conexión de red a otra, atravesando el cortafuegos.
- Personas no autorizadas pueden realizar ataques a los servicios siempre que puedan ser accedidos desde fuera de la red interna. Las amenazas específicas encontradas dependen de los protocolos que se permiten pasar a través del cortafuegos.
- Personas no autorizadas pueden realizar ataques de encaminamiento fuente en el nivel de red; Varios protocolos del nivel de red permiten al emisor de un paquete especificar el camino que el paquete seguirá desde la fuente al destino: si el encaminamiento fuente está indicado en la cabecera de protocolo, la función que procesa éste se saltará cualquier comprobación de reglas, ofreciendo así un camino no deseado para cruzar "por un tunel" el cortafuegos.
- Personas no autorizadas pueden realizar intentos de penetración no detectados (si no existe personal en la red atacada que se dé cuenta de que tales ataques estan teniendo lugar).
- Un atacante puede no ser detectado mientras realiza intentos de penetración repetidos si falta revisión del registro o de los datos de auditoría, bien por la cantidad de datos generados o por falta de herramientas de revisión adecuadas.
- Un atacante puede modificar/degradar el registro de auditoría, bien directamente (manipulándolo a través de un interface del cortafuegos, como un protocolo de control específico soportado por la red); bien enmascarando sus acciones (por ejemplo averiando el cortafuegos tras realizar una penetración o intento para que pueda perderse el registro de auditoría si no está bien protegido.
- Un atacante puede modificar la configuración del cortafuegos y otros datos de seguridad relevantes (esta amenaza es similar a la anterior, salvo que los datos que elige un atacante son esa configuración y otros datos de seguridad críticos).
- Ciertos defectos en el cortafuegos pueden generar brechas de seguridad que los agentes amenazadores pueden descubrir por accidente o búsqueda dirigida y utilizar para trastornar el funcionamiento de las funciones de seguridad y cambiarlas en su provecho (tanto en la entrega e instalación del cortafuegos como durante su funcionamiento normal, con métodos de 'minado' de las funciones de seguridad).

El ***Grupo de Amenazas aplicadas al Entorno de Operación*** implican las causantes de riesgos potenciales del sistema por el entorno o por medios procedimentales como:

- Personal de administración del sistema descuidado, negligente o intencionalmente hostil puede saltarse fácilmente los mecanismos de seguridad del cortafuegos puesto que es responsable de establecer las reglas de control de acceso y de monitorizar el registro de auditoría.
- Ciertos usuarios de una red protegida (situados detrás del cortafuegos) pueden querer compartir información con usuarios de la red externa, enviando información de forma ilegítima a sabiendas que este tipo de cortafuegos generalmente será inefectivo contra esta clase de ataques pues está diseñado específicamente para proteger las redes internas de las redes externas sin tratar de comprobar el contenido del paquete.
- Ciertos usuarios de una red protegida pueden atacar máquinas de esta red protegida, sin que el cortafuegos las pueda proteger, al no ser un ataque a información que pase por el cortafuegos.
- Ciertos usuarios de una red protegida pueden realizar ataques sofisticados a los servicios y protocolos de alto nivel, eligiendo defectos de los niveles de protocolo (y los servicios que utilizan dichos protocolos) por encima del nivel de transporte; el cortafuegos puede denegar el paso de paquetes a servicios específicos, pero una vez que los permite pasar, no les defiende de posibles ataques a los servicios elegidos, pues no verifica el contenido del paquete.

En un entorno operacional con cortafuegos de filtrado de paquetes del nivel red/transporte, se asumen condiciones de utilización segura de diverso tipo (físicas, de personal , de conectividad).

Condiciones físicas:
- El cortafuegos y la consola asociada directamente conectada son seguros: es decir, su acceso se limita sólo al personal autorizado.
- El personal autorizado de administración interactúa con el cortafuegos sólo a través de consolas directamente conectadas; es decir, no se permite ningún "login de red" a los administradores.
- El cortafuegos no requiere para funcionar cambios de las propiedades operativas (por ejemplo, aplicaciones de software, hardware) de la red interna o de la red externa.

Condiciones de tipo personal:
- El cortafuegos sólo está diseñado para actuar como tal y no para proporcionar servicios adicionales de usuario (por ejemplo, "*login*") a cualquiera de la red interna o externa.
- Sólo los administradores poseen acceso directo.
- Se supone que los administradores no son hostiles y son de confianza para realizar sus funciones correctamente.

Condición de tipo de conectividad:
- El cortafuegos es el único dispositivo de interconexión entre las redes. No se permite una configuración con dos redes -una pública y otra privada- conectadas a la vez por un cortafuegos y por una conexión directa.

8. Política de seguridad para implantar un cortafuegos

Hay que especificar los siguientes extremos:
- Se identifica cada 'isla' de seguridad (o sea una red físicamente diferenciable a la que se aplica una política de seguridad sea única o común para todos los equipos con un mínimo de excepciones).
- Tras identificar varias islas, se decide si se dispone cortafuegos entre ellas y se determina la política de tránsito (lo habitual es prohibir todo tipo de tránsito entre redes y sólo autorizar explícitamente los flujos permisibles). Si no hay tráfico entre dos islas, no se requiere cortafuegos entre ellas. Si el tráfico entre ambas es voluminoso, se puede justificar un cortafuegos explícitamente dedicado a esta interfaz.
- Es habitual disponer varias islas de seguridad en forma de estrella alrededor de un cortafuegos único con varias puertas (cortafuegos que suele estructurarse internamente como multinivel). Esta estructura en estrella no puede convertirse en cuello de botella ni limitar el número de niveles de defensa en profundidad.
- Tras determinar la arquitectura (topología y nivel de actuación del cortafuegos) hay que plasmar la política de seguridad explicitando los flujos permitidos de información y las condiciones de autorización para cada uno de esos flujos.
- Se especifica el responsable de diseñar y mantener dicho plan de seguridad, de implantar las reglas pertinentes y de gestionarlas (dando altas y bajas de rutas y de servicios).
- Se diseña una batería de pruebas que permita verificar la operación correcta del cortafuegos, con pruebas de caja negra (verificación global de servicios) y de caja blanca (satisfacción de cada una de las reglas individuales).
- Se corren las pruebas y se valida la implantación. Se ejecutarán pruebas de regresión cada vez que se altere la configuración: nueva política, nuevas reglas, eliminación de reglas, cambio del equipo o de versión de *software* o *firmware*, etc.
- Se registran todas las actuaciones en el libro de operación del sistema, junto con los resultados de la aplicación de la batería de pruebas. Hay que disponer de varios planes: de registro de actividad del cortafuegos de respuesta a incidencias; de contingencia.
- Se identifica/n el/los responsable/s de prestar atención a las alarmas que se produzcan

9. Autentificación e Integridad de la información de configuración en los cortafuegos

Los cortafuegos basados en enrutador no proporcionan autentificación de usuario. Los cortafuegos de tipo *proxy* pueden proporcionar las siguientes categorias de autentificación:
- Uso de "*username/password*"; la menos robusta pues puede monitorizarse usando *sniffers*.
- Uso de OTPs (*One-Time Passwords*), con *tokens* software ó hardware que generan una nueva palabra de paso para cada sesión (como no se pueden reutilizar las palabras de paso anteriores se reduce el riesgo si se monitorizan (utilizando *sniffers*), pierden, prestan o roban.
- Uso de "Certificados Digitales" que involucran Autoridades de Certificación y permiten firmar electrónicamente aplicando algoritmos de cifrado de clave pública, por ejemplo RSA.

Para impedir modificaciones no autorizadas de la configuración del cortafuegos, se debe utilizar alguna forma de proceso que garantice la integridad de su información. La decisión de permitir o denegar a un paquete su paso a través del cortafuegos se basa en atributos del sujeto, del objeto, de la información de estado generada por el cortafuegos y de las reglas de control de acceso configuradas administrativamente. Normalmente se realizan checksums CRC (*Cyclic Redundancy Checks*) o funciones *hash* criptográficas (por ejemplo, MD5) de la imagen *run-time* (en tiempo de ejecución) y se guardan en medios protegidos. Cada vez que modifica la configuración del cortafuegos un individuo autorizado (normalmente el administrador del cortafuegos) se ha de actualizar la base de datos "en-linea" de integridad del sistema y guardarla en un sistema de ficheros en la red o en soporte removible. Si la comprobación de la integridad del sistema muestra que los ficheros de configuración del cortafuegos se han modificado, se avisará que el sistema ha visto comprometida su seguridad. La base de datos de integridad del sistema del cortafuegos se actualizará cada vez que se modifica la configuración del cortafuegos. Los ficheros de integridad del sistema deben guardarse en soporte de sólo lectura o de almacenamiento "fuera de linea". El administrador debe comprobar regularmente la integridad del sistema obteniendo un listado de todos los ficheros que se han modificado, reemplazado o borrado. Es importante que los procedimientos operacionales y sus parámetros de configuración se encuentren documentados, actualizados y guardados en lugar seguro a salvo.

10. Alternativas en el cortafuegos: encaminar frente a reenviar

La política de seguridad de un cortafuegos es diferente si actúa como un enrutador o como un reenviador *proxy* de paquetes Internet. Un cortafuegos basado en un enrutador, al actuar como un dispositivo de filtrado de paquetes, no tiene más opción que encaminar paquetes. En un cortafuegos

del nivel de aplicación todas las conexiones internas y externas deben realizarse a través de *proxies* de aplicación, sin encaminar ningún tráfico entre interfaces de las redes interna y externa que puedan saltar los controles de seguridad, como permiten estos dos mecanismos:

Encaminamiento fuente. En este mecanismo de encaminamiento, la fuente, no los enrutadores intermedios, determina el camino a una máquina destino. El encaminamiento fuente se utiliza principalmente para depurar problemas de red pero también permite ataques a un computador. Si un atacante conoce alguna de las conexiones seguras entre sus computadores, el encaminamiento fuente se puede usar para aparentar que los paquetes dañinos vienen de un computador confiable. Esta amenaza puede neutralizarse fácilmente, configurando un enrutador de filtrado de paquetes para rechazar los que contienen la opción de encaminamiento.

De este modo una organizacón que desea evitar el problema del encaminamiento fuente escribirá una política de seguridad consistente en eliminar paquetes de encaminamiento fuente.

'Spoofing IP'. Este enmascaramiento del atacante que hace pasar su máquina como un computador de la red destino (engañando a una máquina destino con que los paquetes vienen de una máquina confiable de la red interna destino) exige especificar claramente la política de seguridad que trata el encaminamiento de paquetes. El *spoofing* IP utiliza diversas técnicas para trastornar el control de acceso basado en IP suplantando a otro sistema utilizando su dirección IP. Para protegerse contra los ataques de *spoofing* IP, la autentificación basada en direccionamiento fuente ha de combinarse con otro esquema de seguridad.

11. Arquitecturas de cortafuegos

Los cortafuegos se pueden materializar en diferentes arquitecturas que proporcionan diversos niveles de seguridad con diferentes costos de instalación y operación. Las organizaciones deben hacer corresponder su perfil de riesgo con el tipo de arquitectura de cortafuegos seleccionada. Las principales arquitecturas de cortafuegos son:

El cortafuegos con ***computador multi-puerto (multi-homed host)*** tiene más de una interfaz de red (dos es el caso más común). Cada interfaz se conecta a segmentos de red física lógicamente separados. Un cortafuegos de doble puerto tiene dos tarjetas de red (NIC, *Network Interface Cards*) y cada interfaz conecta a una red diferente. Para impedir que el tráfico de paquetes IP procedente de la red no segura se encamine directamente a la red segura y no a través del cortafuegos -que actúa como intermediario-, incluso se inhabilitará el encaminamiento del cortafuegos.

El cortafuegos con ***computador pantalla (screened host)*** utiliza obliga a conectar todos los computadores de fuera a un computador denominado "bastión", en vez de permitir su conexión directa a otros computadores internos menos seguros. Para realizarlo, se configura el enrutador de filtrado de paquetes para que todas las conexiones a la red interna desde la red externa se dirijan al computador "bastión" .

El cortafuegos con ***subred pantalla (screened subnet)*** tiene una arquitectura similar a la del "computador pantalla", pero le añade una capa extra de seguridad creando una red -denominada "perimetral"- que reside en el computador "bastión" y se encuentra separada de la red interna. Se crea una "subred pantalla" añadiendo una red perimetral que separe la red interna de la externa. Si existe un ataque con éxito en el computador bastión, el atacante está restringido a la red perimetral por el "enrutador pantalla" que se conecta entre la red interna y la red perimetral.

12. Mecanismos de respaldo en cortafuegos

El cortafuegos, al igual que cualquier sistema de la red, debe tener alguna política que defina su respaldo o *backup* para conseguir la recuperación tras un fallo o un desastre natural. Así mismo los ficheros de datos y los de configuración del sistema necesitan tener algún plan de respaldo en caso de fallo del cortafuegos.

El cortafuegos y el conjunto del sistema que dependen de él (software, datos de configuración, ficheros de base de datos, etc.) deben contar con sistemas de respaldo; por ejemplo un proceso de copias de seguridad periódico (cada pocas horas, a diario, semanalmente, mensualmente, etc.), cuyas copias deben almacenarse de forma segura en un soporte de sólo lectura para que los datos no se sobreescriban inadvertidamente y deben protegerse para que el soporte sólo sea accesible por el personal apropiado.

Otra alternativa de respaldo consiste en tener un mecanismo de tolerancia a fallos llamado "replicación del cortafuegos de grado dos", es decir otro cortafuegos configurado como el primero y guardado de forma segura para que en caso de fallo del actual, el cortafuegos de respaldo se conmute automática o manualmente mientras se repara el averiado. Con esta alternativa la degradación del servicio es menor, pero a costa de un mayor costo por la duplicidad del cortafuegos y el mecanismo de conmutación.

Toda la administración del cortafuegos se debe realizar desde el terminal local, cuyo acceso físico debe limitarse sólo al administrador del cortafuegos y al administrador de respaldos. No debe permitirse ningún acceso remoto al software operativo del cortafuegos. Éste nunca debe utilizarse como servidor de propósito general y sólo debe contener como cuentas de usuario las del administrador del cortafuegos y las del administrador de respaldos o copias de seguridad.

13. Cortafuegos para Intranets y con capacidad VPN

Aunque los cortafuegos se colocan habitualmente entre una red corporativa y la red no segura del exterior (Internet), se utilizan a menudo en grandes organizaciones para crear subredes distintas dentro de la Intranet. Un cortafuegos para Intranet permite aislar una subred o segmento de red particular de la red corporativa total (por ejemplo la del departamento de nóminas o de contabilidad de la organización), con dos objetivos posibles:

- evitar que todos los usuarios internos puedan acceder a la información de la subred guardada (que estará disponible sólo para los quela tengan que manejar por necesidad)
- conseguir un alto grado de responsabilidad en el acceso y utilización a subsistemas con información sensible, confidencial o crítica para la organización, con un control de acceso fuerte que soporte auditoría y registro.

Estos sistemas y controles deberían utilizarse para dividir la red corporativa interna a la hora de soportar políticas de acceso desarrolladas por los propietarios de información designados.

Por otra parte, las llamadas redes privadas virtuales o VPN (*Virtual Private Networks*) permiten a redes seguras comunicarse con otras redes seguras apoyándose en redes no seguras como Internet. Puesto que algunos cortafuegos proporcionan esta "capacidad VPN", es necesario definir una política de seguridad para establecer dichas VPNs. Cualquier conexión entre cortafuegos por medio de redes públicas habrá de utilizar VPNs cifradas para asegurar la confidencialidad y la integridad de los datos que pasan a través de la red pública. Todas las conexiones VPN deben ser aprobadas y gestionadas por el administrador de servicios de red, quien debe establecer los medios apropiados para distribuir y mantener claves de cifrado antes del uso operacional de los VPNs.

14. Configuración de cortafuegos como servidor DNS

En Internet, el DNS (*Domain Name Service*) proporciona la correspondencia y la traducción de los nombres de dominio a direcciones IP (por ejemplo: 130.206.100.1 representa la dirección IP del computador orion.deusto.es). Algunos cortafuegos se pueden configurar como servidores DNS dde distintos niveles (primarios, secundarios o caché).

Debe observarse que no suele ser una decisión del ámbito de la seguridad la forma de gestionar los servicios DNS. Muchas organizaciones utilizan para gestionar su DNS una "tercera parte" -un ISP (*Internet Service Provider*): en este caso, el cortafuegos puede utilizarse como un servidor DNS caché que mejora el rendimiento pero que no necesita mantener su propia base de datos DNS. Si la organización decide gestionar su propia base de datos DNS, puede ser ventajoso que el cortafuegos actúe como servidor DNS, pero en este caso es necesario tomar otras precauciones de seguridad. Así, si se implementa como servidor DNS, el cortafuegos puede configurarse para ocultar la información de los computadores internos de la organización: o sea, los computadores internos obtienen una visión no restrictiva de los datos DNS internos y externos, mientras que los computadores externos no tienen acceso a la información relativa a las máquinas internas. Para el mundo exterior, todas las conexiones a cualquier computador de la red interna parecerán haberse originado desde el cortafuegos. Con la información sobre los computadores internos oculta desde el exterior, un atacante no sabrá los nombres y direcciones de los computadores internos que ofrecen servicios a Internet. Por tanto una posible política de seguridad para ocultar el DNS puede consistir en que el cortafuegos opere como un servidor DNS y se configure para ocultar la información relativa a la red interna al mundo exterior (Internet).

15. Administración de cortafuegos

Un cortafuegos, como cualquier dispositivo de red, debe ser gestionado por alguien. La política de seguridad debe especificar quién es el responsable de la gestión del cortafuegos. El administrador de la seguridad de la información debe designar dos administradores de cortafuegos (uno primario y otro secundario) como responsables de las tareas de conservación y mantenimiento del cortafuegos. El administrador primario debe encargarse de realizar los cambios en el cortafuegos, mientras que el administrador secundario sólo deberá actuar en ausencia del primario para que no existan accesos simultáneos y/o contradictorios en el cortafuegos. Cada administrador de cortafuegos debe proporcionar sus datos (teléfono del trabajo y de casa, teléfono celular, dirección de correo electrónico, www, buscapersonas, etc.) en los que puede ser contactado cuando se necesiten sus servicios.

16. Consideraciones finales sobre políticas de seguridad

El establecimiento de una política de seguridad debe sincronizarse con el de otras políticas de la organización relacionadas con aquélla y suele presentar tres etapas:
- la estrategia general que establece el enfoque que la organización da a la seguridad
- las reglas que especifican la política concreta de seguridad del dominio a proteger (la red o redes internas); dichas reglas definen lo que está ó no permitido y pueden completarse con procedimientos y otras guías
- el análisis o enfoque técnico que soporta la política general y las reglas específicas.

Para que la política de seguridad sea efectiva sus diseñadores deben tener en cuenta que han de realizarse compromisos/ concesiones. Así, muchas soluciones limitan la funcionalidad para poder incrementar el grado de seguridad (a mayor seguridad mayor dificultad de uso, etc.).

En definitiva, hay varios niveles de la política de seguridad según su destino y grado de robustez, con lo que suele tenerse que estructurar subpolíticas de seguridad:
- para los usuarios
- para los administradores/gestores
- para dominios con requisitos técnicos de bajo riesgo
- para dominios con requisitos técnicos de riesgo medio y alto, etc.

Bibliografía

Areitio, J. *Estrategias de Cortafuegos para Proteger Servicios Web.* Congreso Internacional Mundo Internet'97. Madrid. Febrero 1997.

Areitio, J; Garay, L.M. Gestión de Red: Consideraciones en torno a la Seguridad. ME. *CEP Communications*, nº 263. Enero, 1996.

Areitio, J.; Lewis, S. Auditoría Telemática Automatizada: Una Necesidad Urgente. AEI. *CEP Communications*, nº 276. Julio, 1997.

Areitio, J.; Marcelo, J. Arquitectura de Servicios y Mecanismos de Seguridad para Redes OSI. *Novatica*, nº 125. Enero/Febrero 1997.

Chapman, B.; Zwicky, E.D. *Building Internet firewalls.* O'Reilly & Associates, Inc. 1995 (versión española de McGraw Hill Interamericana, 1997).

Hughes, L. *Actually Useful Internet Security Techniques.* New Riders Press. 1995.

Kaufman, C.; Perlman, R.; Speciner, M. *Network Security: Private Communication in a Public World.* Prentice- Hall. Englewood Cliffs. NJ. 1995.

Oppliger, R. *Internet and Intranet Security.* Artech House. Norwood. Massachusetts. 1998.

Watne, D.; Tuerney, P. *Auditing EDP Systems.* Prentice-Hall. Englewood Cliffs. NJ. 1990.

Sistemas de Tiempo Real

Aviónica y Software del programa CAPRICORNIO

José E. Rico, José M. Gallego
Instituto Nacional de Técnica Aeroespacial

Resumen: *Este artículo hace una somera presentación del Programa Capricornio describiendo los requisitos del vehículo, la arquitectura y la filosofía del guiado así como las instalaciones de tierra necesarias para su operación. Seguidamente, de una forma más detallada, se revisan la Especificación de Requisitos y el Diseño de Alto Nivel del Sofware del Lanzador CAPRICORNIO, haciendo referencia al comportamiento estático y dinámico de la arquitectura escogida. Se han omitido los aspectos de interacción con el hardware. Respecto al Software del Ordenador de Control y Chequeo, se hace repaso de la técnica de prototipado rápido con LabVIEW® analizando los primeros resultados. El objetivo es mostrar cómo se está desarrollando un software de bajo coste con un alto grado de modularidad y flexibilidad que permita migrar fácilmente entre los vehículos demostradores (ARGO) y el lanzador CAPRICORNIO.*

2. Lista de símbolos y acrónimos

t	tiempo
θ	ángulo de cabeceo
ψ	ángulo de guiñada
X'	velocidad horizontal en el plano de la trayectoria
Z	coordenada vertical
Z'	velocidad vertical

Acrónimos

AD	Arquitectural Design
ARTK	Alsys® Real-Time Kernel
BIT	Built-In Test
DD	Detailed Design
E/S	Entrada/Salida
MCC	Módulo de Control de Comunicaciones
MPCC	Multi-Protocol Communication Controller
OBC	On-Board Computer
OCC	Ordenador de Control y Chequeo
OM	Operation & Maintenance
PI	Plataforma Inercial
SR	Software Requirements
TC	Telecomando
TM	Telemedida
TR	Transfer
TVA	Thrust Vector Actuator
TVC	Thrust Vector Controller
UR	User Requirements

3. Introducción

Tras una destacada experiencia en los campos de las armas y los cohetes de sondeo [1] [2], en 1989 el INTA realizó estudios de viabilidad de un lanzador de micro-satélites: el vehículo CAPRICORNIO [3].

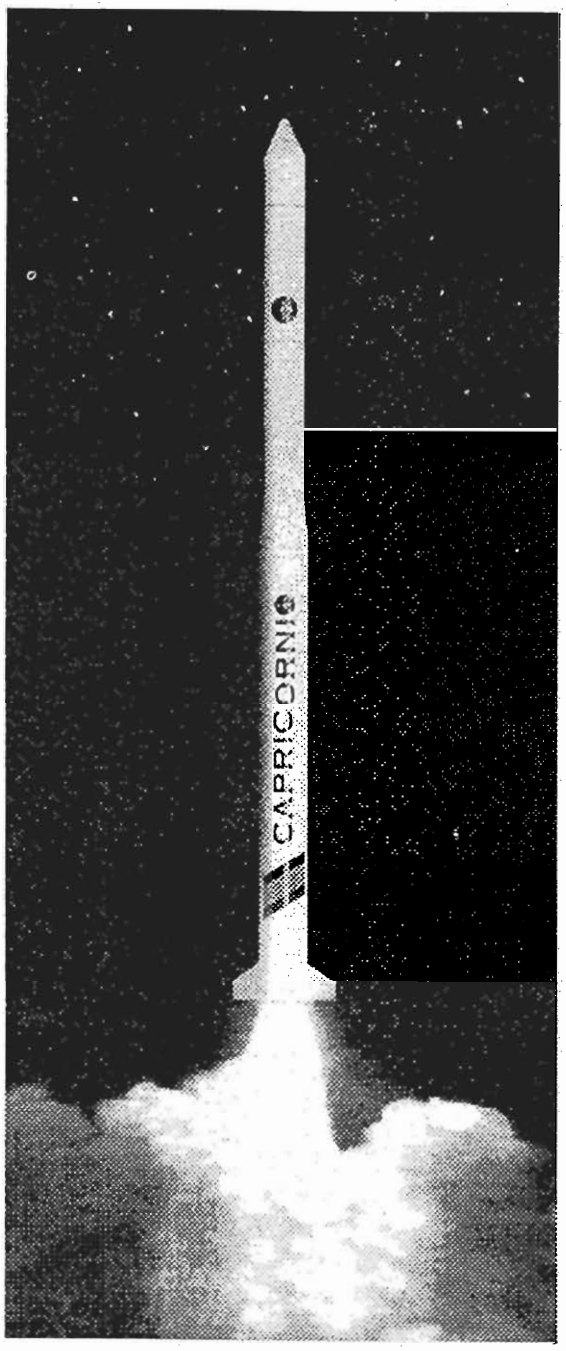


Figura 1: Vehículo Capricornio

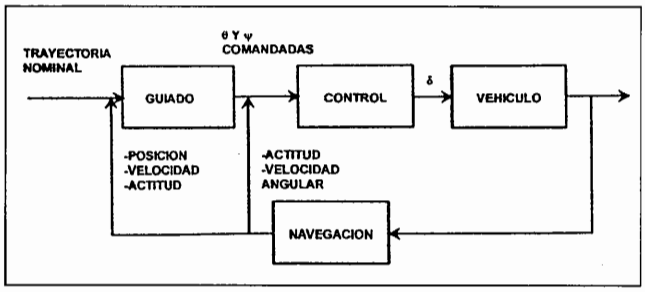


Figura 2. Navegación, Guíado y Control

El objetivo del Programa Capricornio es el desarrollo de un vehículo lanzador capaz de inyectar micro-satélites (hasta 100 kg) en órbita baja (600 km). Aparte, el programa pretende promover la capacidad del INTA y de la industria española tanto en el diseño e integración de esta clase de vehículos como en el resto de tecnologías involucradas. El vehículo constará de tres etapas de propulsante sólido con una masa total de 15 toneladas y una longitud de 18 metros.

Los requisitos básicos de este vehículo se dividieron en [4]:

Primarios:
- masa de los satélites: 50-100 kg
- órbita: 600 km, circular
- punto de lanzamiento: territorio español (costa de Huelva o Islas Canarias)

Secundarios:
- capacidad de evolución
- tanta participación nacional como sea posible

El vehículo fue denominado Capricornio y su configuración se estableció de la siguiente manera:
- Peso total: 15000 kg
- Altura total: 18 m

1ª etapa:
· motor CASTOR IVB (Thiokol corporation)
· TVC (Thrust Vector Control)
· controles aerodinámicos para limitar el balanceo.

2ª etapa:
· motor DENEB (de nuevo diseño)
· TVC (guiñada y cabeceo)
· motores de gas frío (balanceo)

3ª etapa:
· motor MIZAR (nuevo diseño)
· motores de gas frío (balanceo, guiñada y cabeceo)

t	θ	Z	X'	Z'
.01	.339664	26563.780	399.164	1128.928
1.01	.342213	27685.590	397.656	1115.042
2.01	.343804	28815.690	411.949	1145.415
3.01	.344376	29976.950	426.851	1177.370
4.01	.344580	31170.950	442.326	1210.880
5.01	.344651	32399.230	458.355	1245.921
6.01	.344676	33663.300	474.931	1282.484
7.01	.344685	34964.680	492.045	1320.551
8.01	.344688	36304.860	509.693	1360.109
9.01	.344688	37685.360	527.870	1401.153
10.01	.344688	39107.660	546.580	1443.682
11.01	.344688	40573.240	565.822	1487.702

Figura 3: Registros de la trayectoria nominal

Antes de desarrollar el Capricornio, el INTA comenzó en 1993 el desarrollo del ARGO, cuyo primer prototipo volará en 1997, un vehículo demostrador sobre el que desarrollar y probar los motores DENEB y MIZAR y tantos componentes del Capricornio como sea posible. La configuración del ARGO es la siguiente:
- Peso total: 3900 kg
- Altura total: 9 m

1ª etapa:
· motor: DENEB (sin TVC)
· controles aerodinámicos (balanceo)

2ª etapa:
· motor: MIZAR
· TVC (guiñada y cabeceo)
· motores de gas frío (balanceo)

Filosofía de Guiado

El algoritmo de guiado se concibe como un guiado en actitud (controlando la orientación del cohete) en el que el vehículo es obligado a seguir una trayectoria nominal plana preprogramada. El objetivo es alcanzar unas condiciones determinadas de altitud y velocidad en el apogeo. El guiado sólo puede llevarse a cabo durante el vuelo de aquellas etapas en las que existe TVC. Puesto que estos motores cohete no disponen de sistemas de corte de combustión, la precisión se ve muy afectada tanto por las perturbaciones externas como por la exactitud del modelo del motor en cuanto al empuje y el tiempo de combustión.

Ya que la frecuencia característica del TVC es 5 Hz, la frecuencia de control se ha fijado en 25 Hz. Cada ciclo de computación (40 ms) deben realizarse las siguientes funciones:

* adquirir t, θ, Z, X' y Z', tanto los actuales como los nominales. Los datos nominales van almacenados con un intervalo de 1 segundo por lo que se requiere hacer interpolación entre dos registros consecutivos (**Figura 3**). La adquisición de datos actuales (navegación) se efectúa mediante una PI (Plataforma Inercial) ligada.

* calcular θ y ψ comandados como funciones lineales de las desviaciones de los parámetros de trayectoria antes mencionados (guiado).

* calcular las deflexiones de tobera implementando un control proporcional derivativo, como funciones lineales de las desviaciones entre los ángulos y velocidades angulares actuales y comandados.

Sistema Completo

El programa busca tanto el desarrollo de los vehículos como de las instalaciones necesarias para operarlos, todo lo cual conforma el sistema mostrado en la **Figura 4** que consta de:

· ***Centro de Control*** con las siguientes funciones: Seguridad, Operación, Misión, Pruebas, Interruptor de disparo, Adquisición de Telemedida.

· ***Block House***, en el que se encuentra el OCC (Ordenador de Control y Chequeo) y el segundo interruptor de disparo.

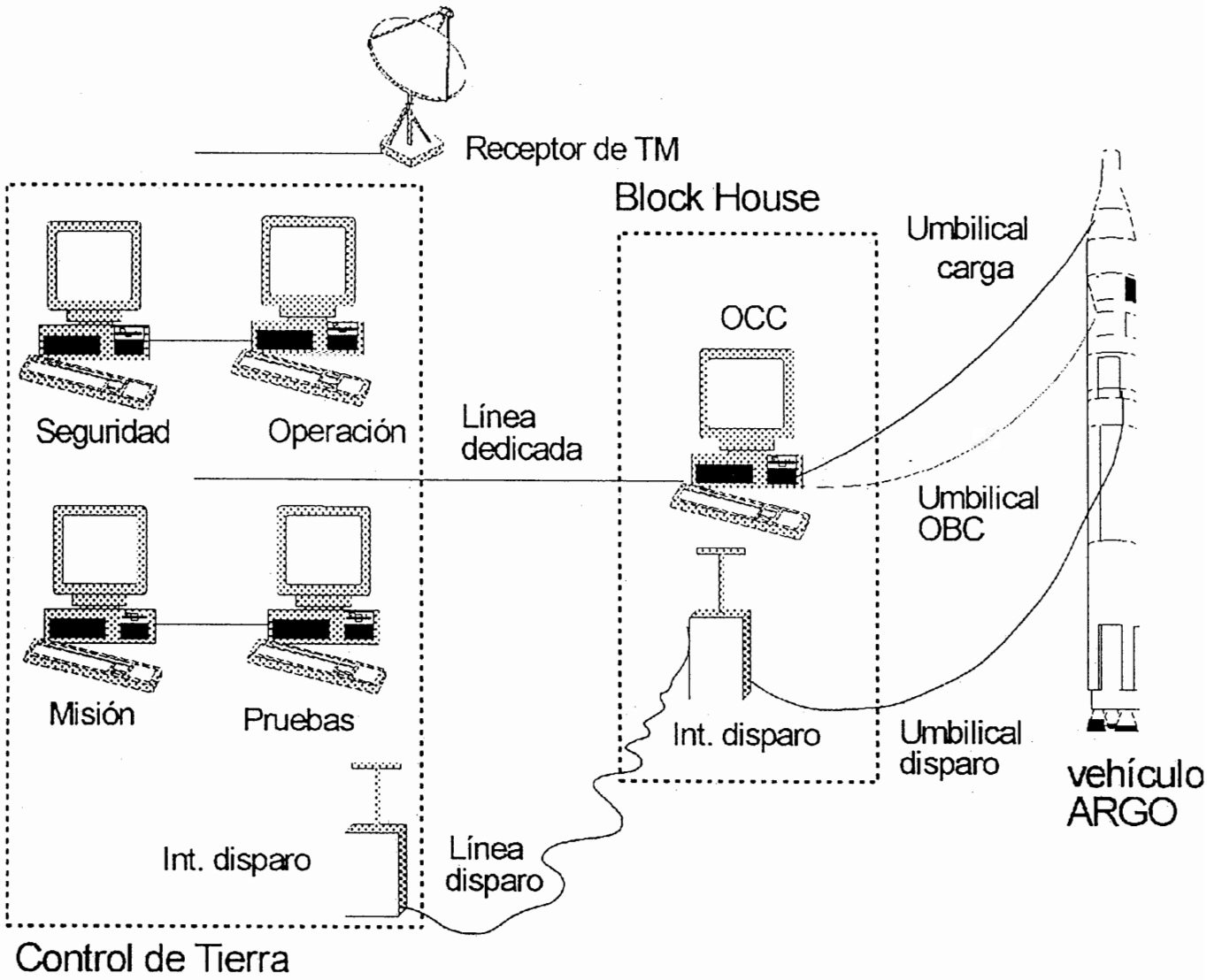


Figura 4: Esquema de campo de lanzamiento

· ***Vehículo ARGO***, en el que se encuentran el Ordenador Embarcado y las tarjetas de control de las comunicaciones.

· ***Umbilicacles de comunicación, líneas dedicadas y líneas de potencia.***

4. Aviónica

El sistema de aviónica emplea sistemas integrados específicamente desarrollados poniendo especial énfasis en el alto nivel de integración, la flexibilidad, la adaptabilidad a los distintos requisitos de misión, peso mínimo y facilidad para las pruebas y el soporte en el lanzamiento.

El elemento principal es el OBC (On-board Computer, **Figura 5**). Consta de dos tarjetas, CPU-40 y MPCC-1 (Multiprotocol Communication Controller), conectadas por un bus VME. Específicamente se trata de las tarjetas PMV 68 CPU-40 y PMV 68 MPCC-1, ambas modelo *Military Conduction Cooled*, de Radstone Technology® PLC, basadas en Motorola® 68040 y 68020 respectivamente.

La CPU-40 es la unidad procesadora principal, con un procesador de 25 Mhz y 32 bits, dos canales RS-423 y una configuración de memoria SRAM, FLASH y EEPROM que hace posible la reprogramación para parámetros específicos de cada misión.

La MPCC-1 está dedicada al control de las comunicaciones en el vehículo, descargando así a la CPU-40 de estas tareas. Proporciona 4 canales.

RS-422 *full duplex* síncronos o asíncronos (configurable), y es capaz de transmitir hasta 500 Kbits/s en cada uno de los cuatro canales simultáneamente.

Uno de los canales se conecta a la PI, leyendo de ella tramas de datos en HDLC a 100 Hz con una velocidad de 460.8 Kbits/s. El modelo de PI empleado es la SAGEM AGYLE SP-10.

Otro canal se conecta al transmisor de telemedida (TM). Este es el enlace más exigido ya que soporta la mayor cantidad de datos, suma de los restantes enlaces.

El último canal en uso (el 4º se deja libre) enlaza todos los actuadores y transductores del vehículo a través de una línea multipunto. Cada estación secundaria consiste en un MCC (Módulo de Control de Comunicaciones), un desarrollo del Departamento de Aviónica del INTA basado en el Motorola®

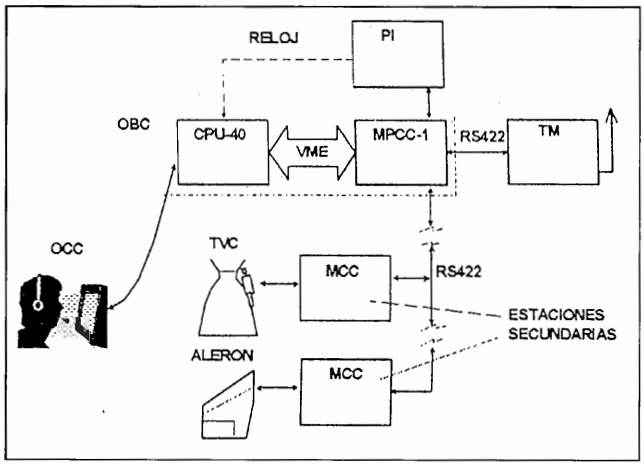


Figura 5: Arquitectura de Aviónica

68302, que incluye tanto el procesador como el control de comunicaciones, montado sobre una placa tamaño simple-Europa, configurando un computador de adquisición de datos y control de comunicaciones multi-propósito al que se adjunta otra placa simple-Europa con las E/S (Entradas/Salidas) analógicas y digitales que se requieran.

Hay varios MCCs a lo largo del vehículo, cada cuál controlando varios actuadores y transductores. Por ejemplo, el MCC-1 del ARGO está encargado de distribuir comandos a las aletas y de recoger distintos datos: posición de las aletas, temperatura de éstas, presión en la cámara del motor DENEB y temperatura en la tobera.

Sólo hay dos comandos que no son procesados por el OBC: encendido de la primera etapa, que va directamente cableado a un interruptor en el Block House, y el sistema de destrucción, que se telecomanda desde tierra. Los datos con alta frecuencia de muestreo, como son los de vibración, no son procesados por el OBC, sino que directamente se empaquetan y mandan a tierra con el resto de los datos de telemedida.

Las comunicaciones en el interior del vehículo van codificadas en HDLC, lo que proporciona enlaces muy fiables y permite una conexión fácil a las actuales redes de ordenadores. Esta es una característica muy útil durante el desarrollo. La línea multipunto del vehículo emplea, como ya se ha dicho, un interfaz RS-422. Esta configuración permite que cada MCC pueda ser conectado individualmente al puerto COM de un PC y así chequearlo antes de la integración empleando el software apropiado.

5. Metodología de desarrollo sotware

Características del desarrollo de software para sistemas de aviónica

Los ordenadores embarcados son la parte más importante de los sistemas de aviónica, cuyo desarrollo se remonta a cerca de una década. El software de aviónica se caracteriza principalmente por:

· **desarrollo incremental**: es prácticamente imposible retrasar el comienzo del desarrollo del software hasta que se complete la definición del sistema.

· **capacidad de implementar cambios**: el desarrollo y generación de sistemas de aviónica y sus componentes asociados, da lugar a peticiones de cambios en las especificaciones de software. El mantenimiento correctivo y de actualización durante la vida operacional del lanzador, deberá realizarse en periodos de tiempo razonablemente cortos.

· **fuertes restricciones técnicas** (***restricciones de tiempo real***): los sistemas de aviónica están sujetos a fuertes requisitos de tiempos (tiempos de reacción de pocos mseg.) y calidad (formalidad, eficiencia, robustez, seguridad, fiabilidad,...).

· **eficiencia económica**: la reutilización de componentes software ha llegado a ser crítica en el desarrollo de software de aviónica. Además, la evolución constante de las tecnologías hardware ha incrementado la importancia de los requisitos de portabilidad que permiten crear productos software lo más independientes posibles de los procesadores y arquitecturas hardware.

Metodología de desarrollo del software

El desarrollo de todo el software del programa CAPRICORNIO sigue los procedimientos incluidos en la propia metodología INTA. Dicha metodología está basada en los estándares de desarrollo de software de la Agencia Espacial Europea (ESA).

Inicialmente, se seleccionó el modelo de ciclo de vida en "*V*", pero se tuvo que cambiar posteriormente a un modelo de ***desarrollo incremental*** (**Figura 6**) debido a la naturaleza volátil y experimental de muchos de los requisitos. Cada paso en el modelo incremental contiene variaciones significativas respecto el anterior en cuanto a las características de la misión: número de etapas, atributos de las etapas (duración, eventos que se producen, acciones que deben ser ejecutadas, actuadores que deben ser controlados,...), cargas de pago, apogeo, etc. El diseño del software debe permitir una adaptación sencilla al siguiente incremento con el mínimo esfuerzo. Para ello, la arquitectura deberá tener un alto nivel de modularidad.

Para el desarrollo del software del OCC se seleccionó el modelo de desarrollo de *rapid prototyping* de forma que se pudieran congelar lo antes posible los requisitos de interface de usuario. La pantalla del prototipo se presenta en la **Figura 13**.

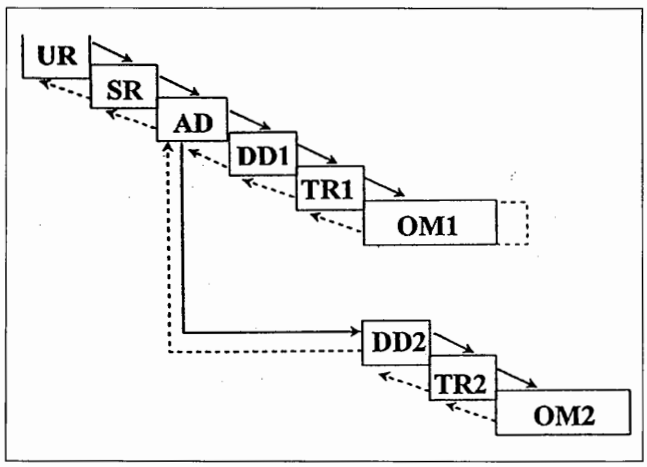


Figura 6: Modelo de desarrollo incremental

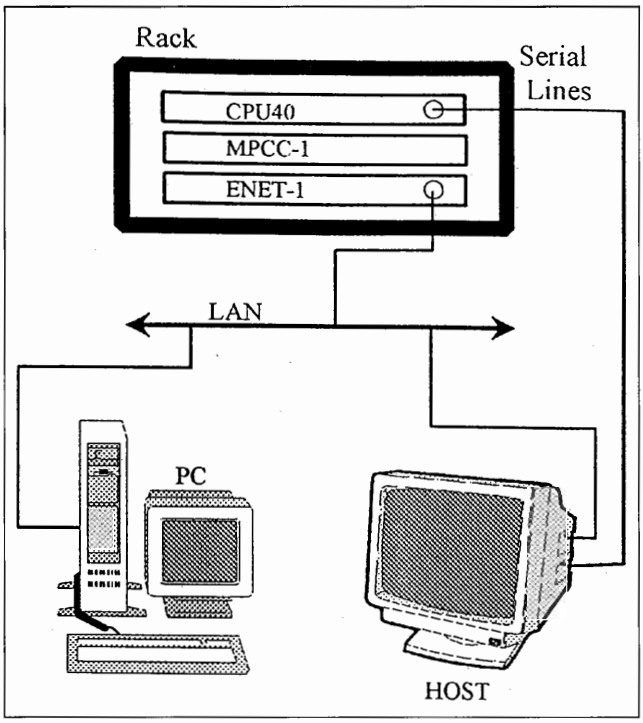


Figura 7

La fase de definición de requisitos software

En la fase de definición de requisitos software, los desarrolladores construyen un modelo independiente de aspectos físicos, en el que se reflejan los requisitos del usuario. Este modelo recibe el nombre de modelo lógico y representa la descomposición funcional del sistema. Para construir el modelo se seleccionó un formalismo de ***Análisis Estructurado*** de ***Yourdon-DeMarco*** con la extensión a tiempo real: ***Ward & Mellor*** [6].

En el formalismo de ***Ward & Mellor*** el modelo está formado por dos partes: un modelo que se centra en la definición de los elementos que interactúan con el sistema y otro que describe el comportamiento requerido. Ambos modelos se desarrollan con independencia de aspectos de implementación.

· El modelo de ***Entorno*** es una descripción del entorno en el que opera el sistema. Tiene dos partes:
- el ***Diagrama de Contexto*** que describe los límites que separan el sistema del entorno.
- la ***Lista de Eventos*** que se generan en el entorno y ante los que el sistema debe reaccionar.

· El modelo de ***Comportamiento*** es una descripción del comportamiento que se espera del sistema. Este modelo tiene también dos partes:
- el ***Esquema de Transformación***: representación gráfica de los procesos.
- el ***Esquema de Datos*** que define la información que se maneja dentro del sistema.

La fase de diseño de arquitectura

En la fase de ***Diseño de Arquitectura***, los desarrolladores definen una colección de componentes software y sus interfaces para establecer un marco de trabajo para el desarrollo del software. La técnica de diagramación utilizada para construir la arquitectura está basada en el formalismo de ***Buhr***. El software se descompone en una jerarquía de componentes de acuerdo con la filosofía "top-down" de ***Buhr***.

El lenguaje de programación

Para implementar el software embarcado en el lanzador se eligió Ada como lenguaje de programación. La elección se basó principalmente en sus propiedades modulares para definir una estructura de software robusta.

6. Entorno de desarrollo

Para la gestión del desarrollo de un software complejo, el equipo de desarrollo utiliza las siguientes herramientas:

- especificación: StP®
- diseño: Popkin® SA, LabVIEW®
- codificación: Alsys® Ada, LabVIEW® y Watcom® C
- Pruebas: LDRA TestBed®
- Gestión de configuración: CVS, RCS.
- Simuladores: Microsoft® Visual C++, librerías LabWindows®.

El entorno hardware se presenta en la **Figura 7.** Consiste en:

- *Host*: Sun® SPARCstation 20 para el desarrollo del software del ordenador embarcado.
- *PC 486* para el software del OCC.
- *Rack* de desarrollo que está formado por:
  *la *CPU40*: tarjeta embarcada de desarrollo,
  *la *MPCC-1*: tarjeta de comunicaciones embarcada de desarrollo y
  *la *ENET-1*: tarjeta de conexión ethernet.

El sistema de tiempo real

Para el desarrollo del ejecutivo de tiempo real se utilizará el proporcionado en el compilador de Ada Alsys® que consiste en un kernel de tiempo real específico (Alsys® Real Time Kernel, ARTK) que proporciona los servicios de bajo nivel que no se pueden expresar en Ada de una manera eficiente.

7. Ordenador embarcado

Los sistemas embarcados se caracterizan por tener que realizar un gran número de operaciones de entrada/salida. Una gran parte del proceso se implementa en la MPCC-1 para evitar el desbordamiento del ordenador principal (CPU40).

El ordenador principal (CPU40) es el encargado de la conducción del vehículo durante toda su vida operacional mediante el software embarcado.

Definición de los requisitos software

SE_ARGO (Software Embarcado - ARGO) proporcionará las siguientes funcionalidades [7]:

· ***Monitorización del sistema*** usando los datos de estado proporcionados por los sensores localizados en los distintos subsistemas del vehículo. Se definen funciones como:

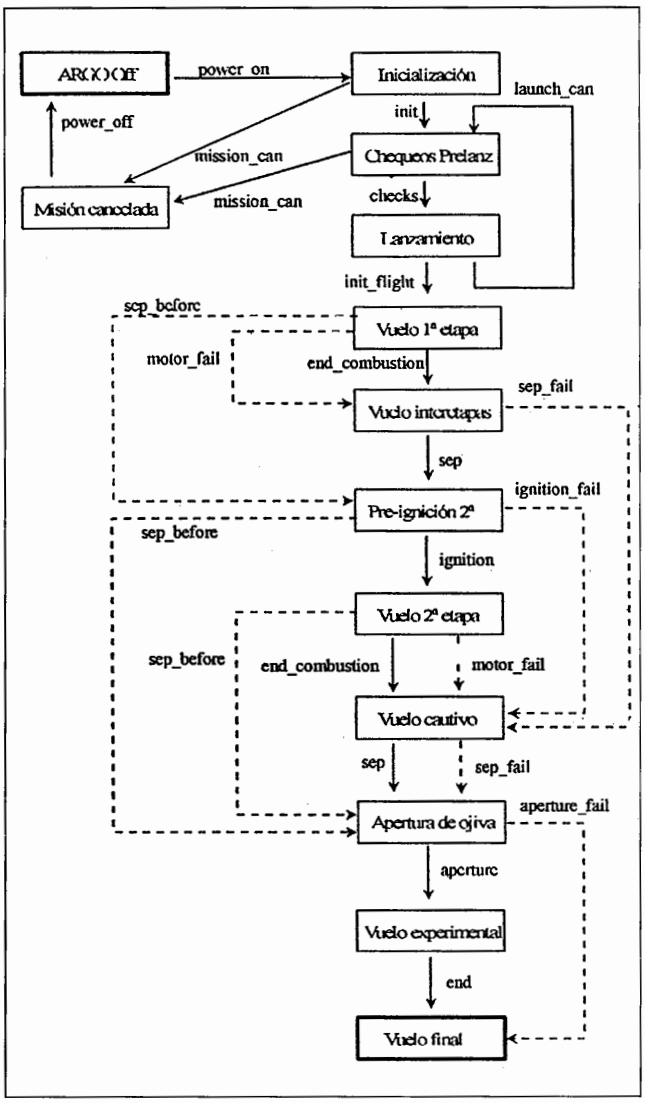


Figura 8. Diagrama de transición de estados del ARGO

- inicialización y chequeo de subsistemas durante la fase de prelanzamiento
- chequeo de las alarmas durante el vuelo

· ***Guiado y Control***: ejecución de las rutinas de guiado y generación de los comandos que se mandarán a los actuadores localizados en cada etapa para conseguir guiar el vehículo según una trayectoria nominal prefijada y para mantenerlo estable.

· ***Gestión de la misión***, ejecutar las acciones necesarias para poder llevar a cabo los objetivos de la misión. Estas acciones estarán condicionadas por los eventos o fallos producidos en el sistema y permitirán los cambios de configuración del lanzador durante el vuelo (separación de etapas, ignición de motores, pirotécnicos,...). Por tanto, serán las responsables de los cambios de modo de operación del software.

· ***Servicios de E/S***. Se definen funciones como:
- envío de la TM de ***SE_ARGO*** a la tarjeta de comunicaciones. Esta telemedida podrá contener el *estado del software, estado de la CPU, comandos de guiado y control generados, comandos de misión generados*, etc.
- adquisición de datos.

· ***Servicios de control de tiempos*** para las restricciones de tiempos del software.

El comportamiento del software se define utilizando ***un diagrama de transición de estados*** (**Figura 8**) en el que cada transición se realiza teniendo en cuenta los eventos y fallos producidos durante la misión. Se tienen los siguientes estados:

- ***ARGO Off***: representa el estado en el que el vehículo esta en la rampa de lanzamiento y todos los equipos están preparados para ser encendidos.

- ***Misión cancelada***: estado que se alcanza cuando el operador del OCC cancela la misión.

- ***Inicialización*** representa el estado en el que se van a ejecutar los procesos de inicialización de todos los equipos.

- ***Chequeos prelanzamiento*** : representa el estado en el que se realizan los chequeos (BITs) de los subsistemas requeridos por el operador del OCC.

- Durante el estado ***Lanzamiento***, se muestrean los sensores de los umbilicales y de la presión de la cámara de combustión para establecer si se ha producido el despegue.

- ***Vuelo 1ª etapa:*** estado en el que únicamente se realiza el control en balanceo

- ***Vuelo interetapas:*** estado que se alcanza cuando la combustión del motor DENEB ha finalizado. Se comanda la separación de la primera etapa.

- ***Pre-ignición 2ª*** etapa: estado que se alcanza cuando se detecta la separación de la primera etapa. Se comanda la ignición del motor MIZAR.

- Una vez detectada la ignición del motor MIZAR se alcanza el estado ***Vuelo 2ª etapa*** Se realiza control en balanceo, guiñada y cabeceo.

- ***Vuelo cautivo:*** representa el estado en el que la combustión del motor MIZAR ha finalizado. Se comanda la separación de la segunda etapa.

- ***Apertura de ojiva:*** estado que se alcanza cuando se detecta la separación de la segunda etapa. Se comanda la apertura de la ojiva y se realizan maniobras de apuntamiento.

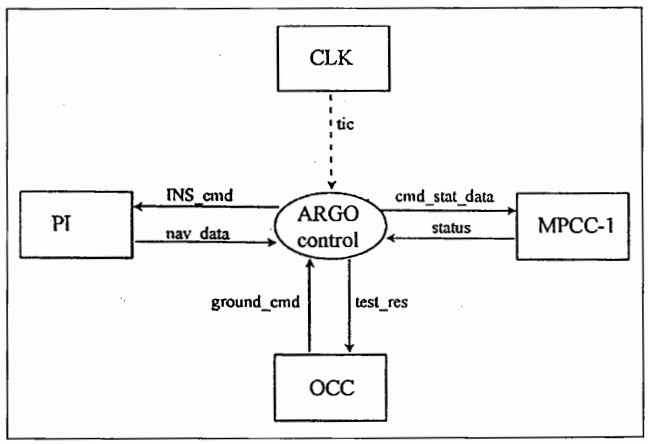


Figura 9. Diagrama de contexto

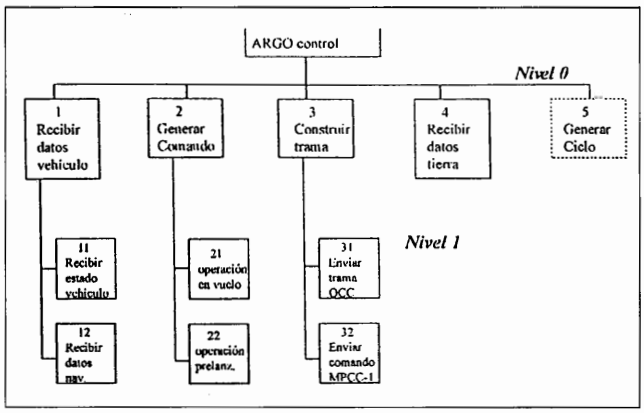


Figura 10. Diagrama de descompocición

- ***Vuelo experimental*** representa el estado en el que la ojiva se ha abierto. Se realizan las maniobras de apuntamiento requeridas por el experimento.

- ***Vuelo final:*** estado que se alcanza cuando ha finalizado el experimento.

La descripción del entorno en el que opera el sistema se describe en el modelo de entorno presentado en la **Figura 9**. Las entidades lógicas externas identificadas son:

- **PI** proporciona los datos de navegación del ARGO y recibe los comandos necesarios para controlar sus modos de operación.

- **OCC** envía los comandos necesarios para la realización de las tareas en la fase de prelanzamiento y recibe los resultados.

- **CLK.** El reloj es el responsable de guiar el comportamiento del sistema. El ciclo básico de funcionamiento es de 40 mseg. En cada ciclo se ejecutan las rutinas de guiado y control y se envían los comandos correspondientes, se comandan las acciones de misión, se realizan las actividades de chequeo y se envía la telemedida asociada a la tarjeta de comunicaciones (MPCC_1).

- **MPCC-1.** La tarjeta de comunicaciones proporciona la información del estado de todos los subsistema del vehículo. Acepta comandos para guiar el lanzador y los distribuye a los distintos subsistemas.

El *Diagrama de Contexto* se descompone en una jerarquía de procesos que forman el *Esquema de Transformación*. La **Figura 10** resume la descomposición presentándose en ella dos niveles:

«***ARGO control***» se descompone en cinco procesos:

1. Recibir datos del vehículo, obtiene y prepara la información referente al estado del vehículo.
2. Generar comandos se encarga de:
- operación en vuelo: operaciones en vuelo que incluyen el envío de comandos para guiar el vehículo y las actividades de monitorización.
- operación en prelanzamiento: operaciones en rampa que incluyen el envío de comandos para inicializar subsistemas y actividades de monitorización.
3. Construir trama, se encarga de empaquetar las tramas de TM y TC (TeleComando).
4. Recibir datos de tierra, durante la fase de prelanzamiento.
5. Generar ciclo encargado de proporcionar la señal necesaria para realizar la sincronización de tareas.

Diseño de Arquitectura

Según los resultados obtenidos en la fase de análisis, se han definido un conjunto de componentes software [8]. El primer nivel de la arquitectura (**Figura 11**) contiene una serie de paquetes encapsulados que exportan servicios y estructuras de datos (representado por flechas en el diagrama). A continuación se describen dichos paquetes.

· ***cpu-main*** contiene el programa principal y el planificador (*scheduler*). Se ha seleccionado un ejecutivo cíclico, preferible por motivos de seguridad a las tareas de Ada, con un bucle primario de 40 mseg. de duración puesto que la frecuencia de control es de 25 Hz como se vio en el apartado 3. En función del modo actual de operación se ejecuta una secuencia de llamadas a funciones para realizar las actividades de guiado y misión.

· el paquete de tiempos (***timing***), es el encargado de capturar la interrupción 'tick' de la INS y proporcionársela al planificador y al watchdog para la sincronización entre tareas.

· la librería de misión (***mission***) contiene todas las funciones necesarias para generar los comandos que deben ser enviados a los elementos de misión (por ej. los pirotécnicos) para poder lograr los objetivos de la misión. El conjunto de funciones que deben ser ejecutadas una vez por ciclo básico de funcionamiento dependerá del modo actual de operación del software.

· la librería de guiado (***guidance***) contiene todas las rutinas necesarias para la generación de los comandos que deberán ser mandados a los actuadores para guiar (siguiendo la trayectoria nominal) y controlar el vehículo durante el vuelo.

· el paquete de chequeo (***checks***) está subdividido en dos subpaquetes: monitorización durante el prelanzamiento y monitorización en vuelo.

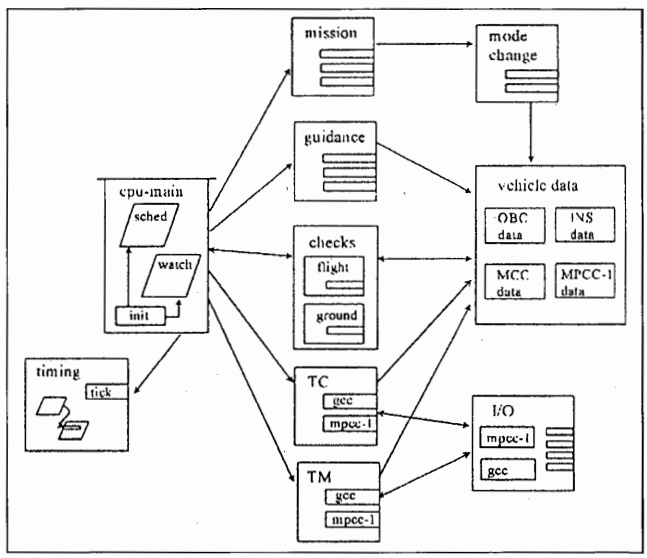


Figura 11. Diagrama de arquitectura de SW

· el paquete de ***TC*** contiene las funciones necesarias para empaquetar los comandos generados en cada ciclo de funcionamiento. Está divido en dos sub-paquetes: comandos del OCC y comandos de la MPCC-1.

· el paquete de ***TM*** contiene las funciones necesarias para empaquetar la telemedida disponible en cada ciclo de funcionamiento. Está divido en dos sub-paquetes: telemedida del OCC y telemedida de la MPCC-1.

```
package COMUNICACION_MPCC1 is

   type T_TM_MPCC1 is
      record
         ESTADO_COM_MCC_1        : TIPOS.T_SWITCH;
         TRAMA_VALIDA_MCC_1      : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_MCC_1      : TIPOS.T_UINT6;
         ESTADO_COM_MCC_2        : TIPOS.T_SWITCH;
         TRAMA_VALIDA_MCC_2      : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_MCC_2      : TIPOS.T_UINT6;
         ESTADO_COM_MCC_3        : TIPOS.T_SWITCH;
         TRAMA_VALIDA_MCC_3      : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_MCC_3      : TIPOS.T_UINT6;
         ESTADO_COM_MCC_4        : TIPOS.T_SWITCH;
         TRAMA_VALIDA_MCC_4      : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_MCC_4      : TIPOS.T_UINT6;
         ESTADO_COM_MCC_5        : TIPOS.T_SWITCH;
         TRAMA_VALIDA_MCC_5      : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_MCC_5      : TIPOS.T_UINT6;
         ESTADO_COM_TRAS_TM      : TIPOS.T_SWITCH;
         TRAMA_VALIDA_TRAS_TM    : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_TRAS_TM    : TIPOS.T_UINT6;
         ESTADO_COM_PI           : TIPOS.T_SWITCH;
         TRAMA_VALIDA_PI_1       : TIPOS.T_TRAMA_VALIDA;
         TRAMA_VALIDA_PI_2       : TIPOS.T_TRAMA_VALIDA;
         TRAMA_VALIDA_PI_3       : TIPOS.T_TRAMA_VALIDA;
         TRAMA_VALIDA_PI_4       : TIPOS.T_TRAMA_VALIDA;
         TRAMA_RETRAS_PI         : TIPOS.T_UINT6;
         ESTADO_MPCC1            : TIPOS.T_INT16;
      end record;
   for T_TM_MPCC1 use
      record
         ESTADO_COM_MCC_1        at 0  range 0..0;
         TRAMA_VALIDA_MCC_1      at 0  range 1..1;
         TRAMA_RETRAS_MCC_1      at 0  range 2..7;
         ESTADO_COM_MCC_2        at 1  range 0..0;
         TRAMA_VALIDA_MCC_2      at 1  range 1..1;
         TRAMA_RETRAS_MCC_2      at 1  range 2..7;
         ESTADO_COM_MCC_3        at 2  range 0..0;
         TRAMA_VALIDA_MCC_3      at 2  range 1..1;
         TRAMA_RETRAS_MCC_3      at 2  range 2..7;
         ESTADO_COM_MCC_4        at 3  range 0..0;
         TRAMA_VALIDA_MCC_4      at 3  range 1..1;
         TRAMA_RETRAS_MCC_4      at 3  range 2..7;
         ESTADO_COM_MCC_5        at 4  range 0..0;
         TRAMA_VALIDA_MCC_5      at 4  range 1..1;
         TRAMA_RETRAS_MCC_5      at 4  range 2..7;
         ESTADO_COM_TRAS_TM      at 5  range 0..0;
         TRAMA_VALIDA_TRAS_TM    at 5  range 1..1;
         TRAMA_RETRAS_TRAS_TM    at 5  range 2..7;
         ESTADO_COM_PI           at 6  range 0..0;
         TRAMA_VALIDA_PI_1       at 6  range 1..1;
         TRAMA_VALIDA_PI_2       at 6  range 2..2;
         TRAMA_VALIDA_PI_3       at 6  range 3..3;
         TRAMA_VALIDA_PI_4       at 6  range 4..4;
         TRAMA_RETRAS_PI         at 6  range 5..10;
         ESTADO_MPCC1            at 6  range 11..26;
      end record;                                        -- 75 bits

   type T_TC_MPCC1 is
      record
         CMD_ACTIVAR_COM_MCC_1   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MCC_1       : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_MCC_2   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MCC_2       : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_MCC_3   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MCC_3       : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_MCC_4   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MCC_4       : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_MCC_5   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MCC_5       : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_PI      : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_PI          : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_TRAS_TM : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_TRAS_TM     : TIPOS.T_SWITCH;
         CMD_ACTIVAR_COM_MPCC1   : TIPOS.T_COMANDO_VALIDO;
         ACTIVAR_COM_MPCC1       : TIPOS.T_SWITCH;
      end record;
   for T_TC_MPCC1 use
      record
         CMD_ACTIVAR_COM_MCC_1   at 0  range 0..0;
         ACTIVAR_COM_MCC_1       at 0  range 1..1;
         CMD_ACTIVAR_COM_MCC_2   at 0  range 2..2;
         ACTIVAR_COM_MCC_2       at 0  range 3..3;
         CMD_ACTIVAR_COM_MCC_3   at 0  range 4..4;
         ACTIVAR_COM_MCC_3       at 0  range 5..5;
         CMD_ACTIVAR_COM_MCC_4   at 0  range 6..6;
         ACTIVAR_COM_MCC_4       at 0  range 7..7;
         CMD_ACTIVAR_COM_MCC_5   at 1  range 0..0;
         ACTIVAR_COM_MCC_5       at 1  range 1..1;
         CMD_ACTIVAR_COM_PI      at 1  range 2..2;
         ACTIVAR_COM_PI          at 1  range 3..3;
         CMD_ACTIVAR_COM_TRAS_TM at 1  range 4..4;
         ACTIVAR_COM_TRAS_TM     at 1  range 5..5;
         CMD_ACTIVAR_COM_MPCC1   at 1  range 6..6;
         ACTIVAR_COM_MPCC1       at 1  range 7..7;
      end record;                                        -- 16 bits

   procedure  INICIALIZAR_DATOS_MPCC1 (
                 TM_MPCC1 : IN OUT  T_TM_MPCC1;
                 TC_MPCC1 : IN OUT  T_TC_MPCC1 );

   procedure  INICIALIZAR_TC_MPCC1 (
                 TC_MPCC1 : IN OUT  T_TC_MPCC1 );

end COMUNICACION_MPCC1;
```

Figura 12. Especificación del paquete JPCC-1_data

· el paquete de cambio de modo (***mode change***) es el encargado de realizar el cambio de modo de operación del software para el siguiente ciclo básico de funcionamiento del sistema. El cambio de modo se realizará teniendo en cuenta determinadas combinaciones de los datos de navegación y otros datos del estado del vehículo.

· el paquete de datos del vehículo (***vehicle data***) es el almacén principal de datos. Se descompone en cuatro subpaquetes: *OBC_data, INS_data, CCM_data* y *MPCC-1_data*. Cada uno contiene la definición de una serie de estructuras de datos y de los procedimientos que las usan.

OBC_data (datos del OBC). Define una serie de tipos que corresponden a los distintos estados de la misión presentados en la **Figura 8**. Contiene también los datos de tiempos y los referentes al estado del HW y del SW.

INS_data (datos de la INS). Especifica los datos de navegación y los tipos de comandos que pueden enviarse a la INS.

MCC_data (datos de los MCC). Especifica los datos de los MCC (temperaturas, voltajes, estado de las baterías, posición de los alerones, ángulo del TVA (Thrust Vector Actuator), alarmas, estado de los motores, etc.) y los tipos de comandos que se pueden mandar a cada uno de ellos (TVA, ignición, separación de etapas, etc.).

MPCC-1_data (datos de la MPCC-1). Define los tipos de datos manejados por la MPCC-1: estado de los MCCs e INS, tramas validadas y retransmitidas de los MCCs e INS, comandos para establecer la comunicación con las MCCs e INS, etc.

En la **Figura 12** se presenta como ejemplo la especificación del paquete Ada correspondiente a MPCC-1 data.

· en el paquete de entrada/salida (***I/O***) se definen los servicios necesarios para realizar todas las operaciones de E/S con el OCC a través del umbilical y con la MPCC-1 a través del bus VME.

Modelo incremental

El objetivo del modelo de desarrollo incremental es obtener las funcionalidades más importantes en las primeras fases del ciclo de vida, dejando para más adelante las secundarias. Las funcionalidades del software se clasifican según una jerarquía de prioridades y se agrupan coherentemente de forma que se puedan obtener incrementos que ejecuten de manera autónoma.

El desarrollo incremental se realiza en los siguientes pasos:

Primer paso:
- comunicaciones entre OCC y CPU-40.
- comunicaciones entre CPU-40 e INS.
- comunicaciones entre CPU-40 y MPCC-1
- control del vehículo en condiciones normales (separación de etapas, ignición del motor MIZAR, separación de la ojiva, etc.).

Segundo paso:
- control en balanceo durante la primera etapa del vuelo.
- guiado durante la segunda etapa del vuelo.

Tercer paso:
- control de actitud mediante los motores de gas frío desde el vuelo de la segunda etapa hasta el final de la misión.

Cuarto paso:
- filtro de los datos de navegación.
- control del vehículo bajo condiciones anormales de vuelo.

8. Ordenador de control y chequeo

Las principales funciones del OCC son [9]:

- ***Inicialización del vehículo y pruebas pre-lanzamiento***. El OCC comanda la inicialización del sistema de gas frío y el TVA abriendo las válvulas respectivas mediante mecanismos pirotécnicos. También comanda el alineamiento y comienzo de la navegación de la PI, y las pruebas prelanzamiento del TVC y las aletas.

- ***Proporcionar un interfaz adecuado al operador***. Debe mostrar los datos de una forma clara usando gráficos, tablas, etc. para hacerlos fácil de entender y simplificar los procedimientos de detección de problemas. Para enviar un comando el usuario sólo tendrá que pulsar un botón. Si el comando requiere parámetros, aparece una ventana de diálogo para pedir dichos valores y controlar la coherencia y márgenes de los mismos.

- ***Registrar las sesiones de pre-lanzamiento***. Grabar cada trama de datos recibida y proporcionar herramientas para reproducir sesiones registradas con el objeto de revisar situaciones problemáticas.

- ***Salida impresa***. Recoger los eventos principales en papel.

- ***Test de integración***. Se pretende usar el OCC no sólo para comprobar el estado del vehículo durante la fase de prelanzamiento sino para comprobar el estado de las etapas antes del ensamblado.

La solución adoptada es un sistema enteramente implementado empleando la herramienta LabVIEW® de National Instruments™ en un PC con Microsoft® Windows 3.11.

El Laboratorio de Motores Cohete del INTA ya ha evaluado un prototipo del software del OCC destacándose las siguientes ventajas e inconvenientes:

Ventajas

- desarrollo rápido
- un interfaz gráfico agradable y fácil de reconfigurar.
- interpretación sencilla y rápida de los datos
- introducción de comandos intuitiva

Inconvenientes

- Velocidad limitada. No fue fácil tratar una trama de 150 bytes a 25 hz y 38000 bits/s teniendo en cuenta que además de ser procesada debía ser grabada en disco. Sin embargo, este problema podría resolverse incrementando la potencia del PC y empleando un sistema operativo multitarea como Microsoft® Windows NT.

-Problemas de mantenimiento. Es difícil aplicar al Lenguaje de Programación Gráfica de LabVIEW las tradicionales técnicas de Ingeniería de Software y las prácticas de codificación que se aplican a los lenguajes de alto nivel escritos con un editor de textos. El leguaje Gráfico resulta ser mucho menos flexible, por lo que el diseño debe hacerse con un cuidado muy especial.

9. Referencias

1. Sanz-Aranguez P., Simón J., 1993, *Desarrollos Iniciales en España de Cohetes de Sondeo y de Vehículos con Guiado Inercial.* II Congreso Nacional de la Ingeniería Aeronáutica, Madrid.

2. Dorado R., 1992, *Estrategia del INTA en el sector de lanzadores*, Panel de Microsatélites, Año Internacional del Espacio, E.T.S.I.Aeronáuticos, Madrid.

3. Simón J., 1992, *Presentación del lanzador Capricornio*, Panel de Microsatélites, Año Internacional del Espacio, E.T.S.I.Aeronáuticos, Madrid.

4. Simón J., Mosquera G., Egea C., *Lanzadores para Microsatélites. Programa Capricornio.* II Congreso Nacional de Ingeniería Aeronáutica, Madrid.

5. *On-board Real-Time Software.* ESTEC, Noordwijk, The Nederlands. 13-15 Noviembre, 1995.

6. Ward P. T. , Mellor S. J., *Structured Development for Real-Time Systems*, Yourdon Press, New Jersey.

7. *Especificación de requisitos del software Embarcado del Sistema ARGO.* CAP/SPE/11L1/001/INTA/94.

8. *Diseño de arquitectura del Software Embarcado del Sistema ARGO.* CAP/TDO/11L1/001/INTA/95.

9. *Especificación de requisitos del software del OCC del Sistema ARGO.* CAP/SPE/11L1/002/INTA/95.

10. *Diseño de arquitectura del Software del OCC del Sistema ARGO.* CAP/TDO/11L1/002/INTA/95.

Referencias autorizadas

Sección *Arquitecturas* (Antonio González)

W. Stallings; *Computer Organization and Architecture Fourth Edition*, Prentice Hall, 1996.
D. Sima, T. Fountain, P. Kacsuk; Advanced Computer Architectures, Adiison-Wesley, 1997.
K. Hwang, *Advanced Computer Architecture. Parallelism, scalability and programmability*, McGraw-Hill, 1993.

Sección *Bases de Datos* (Mario G. Piattini Velthuis)

Johnson, J.L. (1997). *Database: Models, Languages, Design.* Oxford University Press. En este libro se presentan los tres modelos convencionales de bases de datos (jerárquico, Codasyl y relacional) junto con los modelos deductivo y orientado a objetos.

Kemper, A. y Moerkotte, G. (1994). *Object-Oriented Database Management: Applications in Engineering and Computer Science.* Prentice-Hall, Englewood Cliffs. En este libro se presentan tanto extensiones al modelo relacional como modelos orientados a objetos para bases de datos, discutiéndose los conceptos de control y seguridad de bases de datos orientados a objetos. Presenta también algunos productos comerciales.

Kim, W. (ed.) (1995). "Modern database Systems. The Object Model, Interoperability and Beyond". *ACM Press*, Addison-Wesley, Reading, Massachusetts. Esta recopilación está compuesta por interesantes artículos sobre los SGBD orientados a objetos: modelos, lenguajes, vistas, confi-dencialidad, estándares, etc. así como sobre temas relativos a la interoperabilidad de SGBD.

Kroenke, D. M. (1996) *Procesamiento de bases de datos. Fundamentos, Diseño e Instrumentación.* Mejico, Prentice-Hall. El autor ofrece una visión general de las bases de datos, incluyendo en el libro una herramienta de diseño denominada 'SALSA'.

Loomis, M.E.S. (1995). *Object Databases: The Essentials.* Addison-Wesley. Una excelente obra sobre los Sistemas de Gestión de Bases de Datos Orientados a Objetos de una de las expertas más reconocidas en este área.

Sección *Ingeniería del Conocimiento* (Federico Barber)

El número 7 de la revista *Inteligencia Artificial* (Revista Iberoamericana de IA), editada por la Asociación Española de Inteligencia Artificial, incluye un monográfico dedicado a la Inteligencia Artificial Distribuida y a los Sistemas Multiagente. De la propia presentación de esta monografía destacamos que la Inteligencia Artificial Distribuida es el área de la Informática en la que se desarrollan modelos teóricos y software específico con características atribuibles a agentes "inteligentes" que conviven en un entorno o sociedad. No existe una caracterización consensuada para la clasificación de las diferentes aproximaciones que comparten el mismo foco de atención, el diseño y desarrollo de sistemas inteligentes con una arquitectura distribuida, pero pueden identificarse tres líneas claras en este campo: la resolución distribuida de problemas, los sistemas multiagente y los agentes autónomos. Particularmente, el concepto de agente, su definición e implantación es un tema de actualidad que ha generado amplias expectativas, ya que permitiría disponer de unidades de software capaces de realizar automáti-camente tareas en un entorno en el que participan, indistintamente, agentes automáticos o personas mediante una red de comunicación digital.

Los agentes pueden concebirse como procesos informáticos con capacidad para resolver problemas no triviales relacionándose con el entorno, con cierto grado de racionalidad y autonomía en su actuación, limitada por la necesidad de interacción con el resto de agentes para la consecución de sus objetivos.

La monografía comentada, coordinada por Ana García Serrano y Sascha Ossowski, efectúa una revisión de la problemática general del área, de gran interés en una amplia gama de aplicaciones complejas de Inteligencia Artificial, así como reúne una colección de trabajos teórico/prácticos mas específicos, realizados por especialistas de reconocido prestigio. Por todo ello, la monografía resulta de gran interés, tanto para los que quieran conocer e introducirse en esta temática, como para los ya conocedores de la misma, permitiendo contrastar diferentes aproximaciones, estudios y aplicaciones que se realizan en nuestro país.

Sección *Ingeniería de Software* (Luis Fernández)

Tema: novedades sobre objetos y componentes

1. Pierre-Alain Muller, *Instant UML*, Birmingham, Wrox Press, 1997. Todavía estamos a la espera de los tres libros que Addison-Wesley publicará sobre UML de sus autores Jacobson, Booch y Rumbaugh. Dentro de las publicaciones sobre la notación UML para el desarrollo orientado a objetos, este libro traducido a inglés (el original está en francés y disponible en la editorial Eyrolles) es uno de los más didácticos y completos.
2. *IEEE Computer*, Vol. 31, nº 6, Junio 1998. En este número se incluyen algunos artículos sobre la tendencia actual (y lógicamente futura) del desarrollo de software basado en el uso de componentes software. También se aborda la problemática general del software de tercera parte.IEEE Computer, Vol. 31, nº 6, Junio 1998.

3. *Http://www.rational.com/modelingcd/* En esta dirección de la empresa Rational (fundada por los creadores de UML) se puede solicitar un CD con información sobre UML.

Sección *Lengua y tecnologías de la información* (Javier Gómez Guinovart)

Ali, S.; e Iwanska, L. (eds.), *Knowledge Representation for Natural Language Processing*. Monográfico de *Natural Language Engineering*, 3 (2-3). Cambridge University Press, 1997. Número monográfico de la revista *Natural Language Engineering* dedicado a los sistemas de procesamiento del lenguaje natural que utilizan técnicas de representación del conocimiento para la extracción de

información, el procesamiento del diálogo persona-ordenador, la adquisición de conocimiento y otras aplicaciones lingüísticas de la informática.

Pérez Guerra, J., *Análisis computarizado de textos: Una introducción a TACT.* Servicio de Publicacións da Universidade de Vigo, 1998. Manual didáctico de introducción a las técnicas y fundamentos básicos de la investigación lingüística de corpus textuales asistida por ordenador. Incluye una extensa presentación de los estándares de anotación textual SGML (*Standard Generalised Markup Language*) y TEI (*Text Encoding Initiative*), y del manejo del programa de análisis de textos electrónicos TACT (*Text Analysis Computing Tools*), con numerosos ejemplos prácticos de sus aplicaciones.

Sección *Libertades e Informática* (Alfonso Escolano)

Tema: adaptación de la LORTAD (Ley 5/1992) a la normativa europea. Se recomienda visitar: *http://www.ag-protecciondatos/datd7.htm*

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos *http.//www.senado.es/comredinf*

Muestra la actividad de la Comisión especial de Redes Informáticas del Senado Español. Visitar especialmente las secciones de presentación y actividad *http://www.congreso.es*

Ir a Buscadores Congreso / Búsquedas en el servidor del Congreso de los Diputados/ e indicar como parámetro de búsqueda 5/1992. Aparecerá la referencia A-135-1, donde aparece el proyecto de ley. Indicar que la comisión que lo estudia es la constitucional.

Sección *Seguridad* (Javier Areitio Bertolín)

Kosiur, D. *IP Multicasting. The Complete Guide to Interactive Corporate Networks.* John Wiley & Sons. Ltd. Chichester. UK. 1998.
Perkins, C. *Mobile IP: Design Principles and Practices.* Addison-Wesley Publishing Company. Reading Massachusetts. 1997.
Rosenheim, S.J. *The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet.* The Johns Hopkins University Press. 1997.
Prados, J. *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II.* Random House. 1995.
Comer, D.E. *Computer Networks and Internets.* Prentice-Hall. Upper Saddle River. New Jersey. 1997.
Longo, G. and Marchi, M. *Geometries, Codes and Cryptography.* Springer-Verlag. NY. 1990.
Albert, B. and Jayasumana, A.P. *FDDI and FDDI-II. Architecture, Protocols and Performance.* Artech House. Nordwood. Massachusetts, 1994.
Moll, L.B. *Baffling Cryptograms.* Sterling Publishing. 1996.
Stang, D. and Moon, S. *Network Security Secretes.* IDG Books. 1993.
Beker, H. and Piper, F. *Cipher Systems.* John Wiley & Sons. Ltd. Chichester. UK. 1982.
Ash, G.R. *Dynamic Routing in Telecommunications Networks.* McGraw-Hill. New York. 1998.
Rhee, M.Y. *Cryptography and Secure Data Communications.* McGraw-Hill. New York. 1994.
Riesel, H. *Prime Numbers and Computer Methods for Factorization*". Birkhauser. 1994.
Stallings, W. *High-Speed Networks, TCP/IP and ATM Design Principles.* Prentice-Hall. Upper Saddle River. New Jersey. 1998.
Escamilla, T. *Intrusion Detection. Network Security Beyond the Firewall.* John Wiley & Sons. Ltd. Chichester. UK. 1998.

Sección *Software Libre* (Jesús M. González Barahona, Pedro de las Heras)

Textos libres

No sólo el software informático puede ser libre. También los libros (o más bien la información que contienen) pueden serlo. Los autores de estos "libros libres" permiten que sus obras sean redistribuidas y copiadas libremente, y en muchos casos (cuando esto tiene sentido), también modificadas. A continuación, alguna información sobre este mundo:

- Información general, recopilada por Bertrand Lang: *http://pauillac.inria.fr/~lang/hotlist/free/text/*
- Proyecto Gutenberg, recopilación de textos clásicos cuyo copyright ya ha expirado: *http://www.gutenberg.org* o *http://www.gutenberg.net*
- Artículo de Richard Stallman, sobre la importancia de acompañar el software libre con documentación libre: *http://www.gnu.org/philosophy/free-doc.html*
- RFCs, Request for Comments, los "estándares" de Internet: *http://www.cis.ohio-state.edu/hypertext/information/rfc.html*
- Linux Documentation Project, documentación libre para GNU Linux: *http://sunsite.unc.edu/LDP/*

Por otro lado, el oscuro futuro que describía Richard Stallman en "El derecho a leer", cuento que publicó Novática (130, Nov.-Dic., 1997), sección IF, se está empezando a materializar. Por ejemplo, ya hay varios "libros digitales"' diseñados para no poder ser copiados. En algunos casos, la información sólo se "alquila"', pagando una cuota mensual. Si la cuota se deja de pagar, la información deja de ser accesible. ¿Sustituirán estos libros a los de papel? Un ejemplo de estos dispositivos puede verse en *http://www.news.com/News/Item/0,4,23614,00.html?st.ne.fd.gif.k*
Por otra parte, puede ser interesante cómo podrían usarse dispositivos de este estilo con textos libres, teniendo en cuenta que el coste "de copia" es virtualmente cero...

Noticias

En la edición WWW del número de Agosto de Sun World (*http://www.sunworld.com*) aparecen varios artículos sobre OpenSource y GNU/Linux:

- Linus on Linux, por Robert McMillan. Una entrevista con el creador de Linux.
- SPARCing up Linux, por John Little. Una guía paso a paso para la instalación y configuración de GNU/Linux en máquinas SPARC.
- Linux vs NT, por Cameron Laird. Una comparación de GNU/Linux, Windows NT y Solaris.

El Primer Foro Hispalinux de 1998 tuvo lugar este en julio, en Málaga. Más información en *http://www.hispalinux.ctv.es/cp98.html*

A mediados de Agosto tuvo lugar un seminario sobre OpenSource en California, auspiciado por O'Reilly. Más información en *http://opensource.ora.com*

En SalonMagazine (*http://www.salonmagazine.com/21st/*) se han publicado varios artículos sobre software libre, entre ellos una entrevista con Richard Stallman, impulsor del proyecto GNU.

La revista *IEEE Software* (*http://www.computer.org/software/*) va a dedicar al software libre su número de Enero de 1999. La petición de artículos está abierta hasta el 1 de Noviembre.

Cygnus ya distribuye su compilador de Java (genera código nativo a partir de código Java). Está basado en GCC, el popular compilador de GNU, y es software libre. Más información en *http://www.cygnus.com/news/gcj-980907.html*

Sección *Tecnologías para la Educación* (Benita Compostela)

Desde hace bastantes años la informática ha ido introduciéndose poco a poco entre las materias del currículo, tanto a nivel de Enseñanza Secundaria como en el nuevo Bachillerato. En ambos casos se trata de asignaturas optativas, que no son obligatorias para los estudiantes, ni tampoco los centros escolares están obligados a ofertarlas. De esta forma se salva el problema de los centros que no tienen profesorado cualificado para impartir estas nuevas materias.

En la ESO la asignatura "Informática" se imparte dos horas semanales, mientras que en el nuevo bachillerato la asignatura "Tecnologías de la Información y la Comunicación" tiene asignadas cuatro horas semanales.
Reseñaremos en esta sección algunos libros que están disponibles para la ESO (Enseñanza Secundaria Obligatoria) y para el Nuevo Bachillerato.

ESO:
Introducción Práctica a la Informática. (ESO) **Melendi Viña, Jaime**. (1995) McGraw-Hill. El libro consta de un capítulo introductorio dedicado al computador, y al entorno gráfico Windows. Dada la fecha de edición de este libro se refiere únicamente al Windows 3.1. Tras este capítulo introductorio aparece la primera parte del libro,(capítulos 2 al 8) dedicada a los procesadores de texto. Se refiere básicamente al procesador de textos WORKS. La segunda parte del libro (capítulos 9 al 12)se dedica a la hoja de cálculo. También en este caso se centra en la hoja del paquete integrado WORKS. La tercera y última parte estudia los conceptos fundamentales de las bases de datos. También tiene dos apéndices. El Apéndice A se dedica a hacer un listado alfabético, con breves explicaciones de las funciones del paquete integrado WOKS. El Apéndice B se refiere a Comunicaciones. Si bien hay que reseñar que se centra en la herramienta que WORKS dispone para conectar dos o mas ordenadores, pero no hace ninguna mención a INTERNET. Dada la velocidad con que evoluciona la informática, antes de salir al mercado este libro ya estaba prácticamente obsoleto.

Informática para la ESO.(1997). **Gracía Merayo, Felix y Alcalde Lancharro, Eduardo**. McGraw-Hill. El libro está distribuido en cinco bloques temáticos: El primer bloque es el más amplio y consta de siete lecciones: Las primeras de ellas se dedican a la descripción de las partes fundamentales de los ordenadores y sus fundamentales aplicaciones. La lección quinta se dedica al sistema operativo MS-DOS, la sexta al Entorno Operativo Windows, dedicando las cuatro últimas páginas al Windows 95. El segundo bloque temático consta de dos lecciones: la telemática y comunicaciones con WORKS. El tercer bloque temático se refiere a las bases de datos y en concreto a la base de datos de WORKS. El cuarto bloque trata de las hojas de cálculo y posteriormente la última lección se dedica al estudio de "la técnica multimedia".

Para Bachillerato:
Tecnologías de la Información Informática. **Gracía Nuñez, Pablo J. y Ferro Sánchez, María Piedad**. (1998). Este denso libro consta de diez y seis lecciones y es una revisión a los conceptos fundamentales de la cultura general informática que se supone que todo joven debería alcanzar. Trata en primer lugar sobre la sociedad de la información y las nuevas tecnologías, del Hardware, del software y los sistemas operativos, dedicando un capítulo al MS-DOS, otro al MS-DOS 3.1 y uno posterior al Windows 95. También tiene otros capítulos dedicados a los procesadores de texto, bases de datos y hojas de cálculo. Incluye además introducciones a la programación, a la robótica y a las comunicaciones. Y, como no podía faltar, el último capítulo está íntegramente dedicado a INTERNET.

Tecnologías de la Información. **Rocandio Pablo, Francisco Javier**. (1997) McGraw-Hill. El contenido del libro se ha distribuido en doce unidades, comenzando por el estudio de "la comunicación a través de la Informática" y continuando por los "componentes físicos y lógicos de un ordenador". A continuación se dedican dos unidades didácticas a los sistemas operativos: MS-DOS y Windows, tanto el 3.1 como el 95. También se estudian los sistemas multimedia y los paquetes integrados. Al tema de la escritura de textos se le dedican tres unidades: Manipulación automática de textos, Procesadores de textos y Autoedición. Termina el libro con una unidad dedicada a los gestores de bases de datos y otra a las hojas de cálculo electrónicas.

En la semana del 23 de abril de 1999, en la Comunidad de Madrid, se celebrará por primera vez en España una reunión internacional de expertos en seguridad de Tecnología de la Información. Dicha reunión se realizará en el marco de la Organización Internacional de Normalización (***ISO International Organization for Standardization***) (*http://www.iso.ch/*) ante la cual la Asociación Española de Normalización y Certificación (AENOR) representa los intereses españoles en el campo de la normalización (*http://www.aenor.es*).

La reunión cuenta con el apoyo de las organizaciones miembro del Subcomité Técnico de Normalización español CTN 71 SC27 Técnicas de Seguridad - Tecnología de la Información y dentro de ellas son patrocinadores la Fábrica Nacional de Moneda y Timbre (FNMT) donde tendrán lugar las reuniones, la Agencia de Protección de Datos de la Comunidad de Madrid, el Banco de Santander, Dimasoft, Unión Fenosa y el Ministerio de Administraciones Públicas (*http://www.map.es/csi*).

Más información en *http://www.dimasoft.es/ctn71sc27* a partir del próximo mes de septiembre.

Programar es Crear

Marcos de Ventanas

Traducción: Angel Alvarez (DIT-UPM)

aalvarez@dit.upm.es

(Este es el octavo y último programa de los planteados en la fase final del Concurso ACM de programación para estudiantes 1997)

Las interfaces gráficas de usuario incluyen elementos tales como pulsadores (*buttons*), cajas de texto (*text boxes*), barras deslizantes (*scroll bars*), menús desplegables (*drop-down menus*) y cajas deslizantes de listas (*scrollable list boxes*). Cada uno de ellos es un caso especial del tipo de objeto llamado *widget*. Y dónde se colocan estos, cuánto espacio se les asigna y cómo cambian de tamaño, es lo que constituye la geometría de una ventana.

Nuestro esquema de gestión de la geometría de una ventana usa unos *widgets* rectangulares especiales llamados marcos, que a su vez contienen y agrupan otros *widgets*. Se dice de un marco que es *padre*, si parte o todo su espacio se encuentra asignado a otros marcos, que entonces se dice que son sus *hijos*. El marco que no tiene padre se llama *marco* raíz y su tamaño viene especificado por el usuario (como parte de los datos de entrada). El problema requiere determinar la asignación de espacio y la posición de los marcos que se colocan en marcos raíz de distintos tamaños.

Dado un marco, se llama *cavidad* a la parte del mismo que no está ocupada por sus hijos. Cuando se crea un nuevo marco hijo, se le asigna bien una banda horizontal completa por arriba o por abajo de la cavidad (y entonces se llama un *hijo horizontal*), o bien una banda vertical a la derecha o a la izquierda de la cavidad (y entonces se llama un *hijo vertical*). Como resultado, cada vez que se crea un hijo la cavidad se reduce en tamaño, pero no pierde su forma rectangular. El proceso de colocar hijos dentro del marco que les engloba se llama empaquetamiento y los hijos se colocan en la cavidad según el orden en que se empaquetan.

En la **figura 1** se muestran los hijos de un marco padre. El marco 1 de la derecha se empaquetó el primero, el marco horizontal inferior 2 el segundo, luego el 3 por la izquierda y, por último, el 4 se empaquetó por la derecha. Cada marco ocupa una malla rectangular de *pixels*. Si el marco raíz ocupa *c* columnas y *f* filas, entonces el *pixel* de la esquina superior izquierda tiene la coordenada (0,0) y el pixel de la esquina inferior derecha la (*C-1, f -1*). La posición de cualquier marco viene determinada por las coordenadas de los *pixels* que están en sus esquinas superior izquierda e inferior derecha.

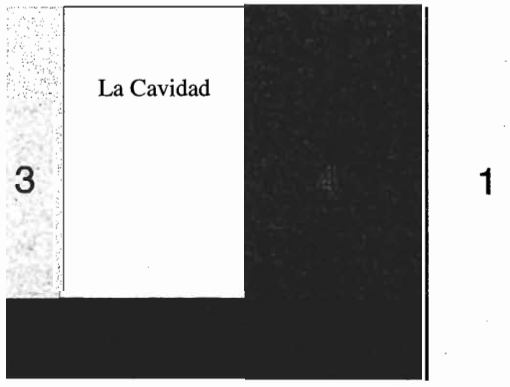


Figura 1

Cada marco tiene unas dimensiones mínimas determinadas por un parámetro de entrada *d* y las dimensiones mínimas de sus hijos. Las dimensiones mínimas de cada marco se determinan como muestra la **figura 2**. Cuando un marco es mayor que las dimensiones mínimas especificadas, el espacio interior adicional se distribuye entre sus hijos o su cavidad.

Cada marco tiene una *marca de expansión* (que es también un parámetro de entrada) que, cuando está habilitada, indica que el marco correspondiente puede crecer a lo ancho, si es vertical, o a la alto, si es horizontal. Por ejemplo, si se tiene un marco horizontal con la marca de expansión puesta, colocado en la cima de la cavidad, éste puede crecer en altura, con la altura adicional extendiéndose hacia abajo.

La distribución del espacio extra horizontal de un marco se hace como sigue. Sea *x* el número de *pixels* horizontales en los que el marco padre supera su ancho mínimo. Si *n*, el número de hijos verticales del marco que tienen su marca de expansión habilitada, es mayor que cero, entonces los *x pixels* se distribuyen entre los esos *n* hijos verticales. Sea *q* el cociente de dividir *x* por *n* y *r* el resto. Cada uno de los *n* marcos hijos verticales crece entonces *q pixels* más en anchura y los primeros *r* de ellos en ser empaquetados crecen además en anchura un *pixel* más cada uno.

Sin embargo, si *n* es cero, entonces ninguno de los hijos verticales crece a lo ancho y los x *pixels* se añaden en su lugar al ancho de la cavidad. En cualquiera de los dos casos, los hijos horizontales se ensanchan, si ello resulta necesario para que la cavidad siga manteniendo la forma rectangular.

La distribución del espacio extra vertical de un marco padre entre sus hijos y su cavidad se hace de forma similar a la que se utiliza para distribuir el espacio extra horizontal, cambiando únicamente la dirección de crecimiento (antes en anchura y ahora en altura).

Lado de empaquetamiento	Tipo de marco	Ancho mínimo	Altura mínima
Derecho o izquierdo	Vertical	Máximo de d y el ancho necesario para los hijos del marco	Máximo de 1 y la altura necesaria para los hijos del marco
Base o cima	Horizontal	Máximo de 1 y el ancho necesario para los hijos los hijos del marco	Máximo de d y la altura necesaria para los hijos del marco

Figura 2

Para distribuir los *pixels* extra en altura, sólo cuentan los hijos horizontales que tengan la marca de expansión puesta. Y, de nuevo, si no existe ninguno de ellos, todos esos *pixels* extra se utilizan para incrementar la altura de la cavidad. De manera similar a lo que ocurre en el caso anterior, los hijos verticales aumentan su altura automáticamente, si ello resulta necesario para que la cavidad siga manteniendo la forma rectangular.

En las **figuras 3 y 4**, el marco raíz de la izquierda se ha agrandado para dar el de la *derecha*. Los *marcos 6* y *7 son, respectivamente, hijos derecho e izquierdo del marco 5*. Solo los *marcos 4*, *6* y *7* tienen su marca de expansión puesta. En el marco de la derecha, el espacio extra horizontal y vertical se ha distribuido entre los hijos dando como resultado los crecimientos señalados por las flechas. Debe observarse que el marco 7 no amplía su tamaño debido a que no hay espacio extra para expansión en su marco padre, que es el 5. Por la misma razón, el marco 6 tampoco amplía su tamaño.

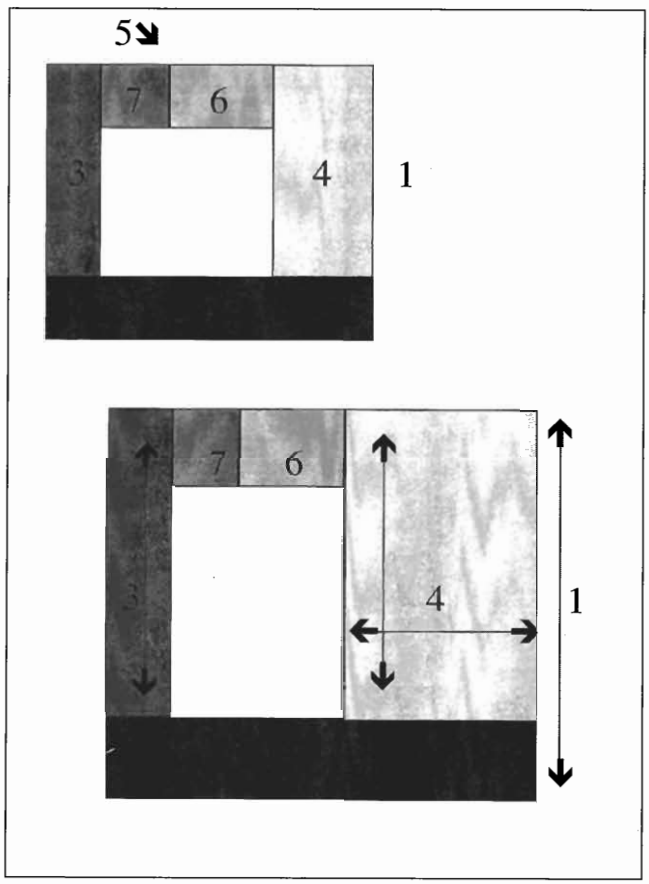


Figura 3 y 4

Datos de Entrada

La entrada consta de una secuencia de conjuntos de datos formados por tres partes: número de marcos, exceptuando el raíz, y número de tamaños posibles de éste, lista numerada de descendientes, y secuencia de distintos tamaños posibles del marco raíz. Cada elemento de la secuencia correspondiente a un único marco raíz tiene el siguiente formato:

M N M es el número total de marcos sin incluir al raíz
N es el número de distintos tamaños posibles del marco raíz (los dos son enteros positivos).
seguido de *M* líneas con la forma:
n p l d e siendo: *n* el nombre del marco (un entero positivo)
p el nombre del marco padre (siendo 0 el marco raíz)
l el lado de empaquetamiento (una de las letras "D", "I", "B" o "C": Derecha, Izquierda, Base o Cima)
d la dimensión mínima (un entero positivo)
e la marca de expansión (1 puesta, 0 no puesta)
seguido de N líneas con la forma:
c f siendo *c* el número de columnas de *pixels* y
f el número de filas de *pixels* del marco raíz (ambos enteros positivos)

Los marcos raíz no están numerados y los números de los marcos hijos de un marco raíz dado son todos diferentes. Todo hijo de cualquier marco viene en la entrada después que su padre. Los marcos se empaquetan en el orden en el que aparecen en los datos de entrada. El final de los datos de entrada viene dado por una l'inea que tiene tanto *M* como *N*, a cero.

Resultados de Salida

Los resultados para cada marco raíz comienzan escribiendo su número de orden, a partir de 1. Para cada uno de los tamaños posibles de un marco raíz, se escribe el tamaño (en filas x columnas) seguido de la lista de marcos (en el orden en que se han empaquetado dentro de sus padres), junto con las coordenadas de sus esquinas superior izquierda e inferior derecha.

Primero se escribe el primer hijo del marco raíz, seguido de sus propios descendientes, después el segundo hijo del marco raíz, seguido de sus propios descendientes, y así sucesivamente. Si el tamaño del marco raíz es demasiado reducido para empaquetar sus marcos, se escribe simplemente el mensaje "es demasiado reducido", en vez de intentar meter la lista de marcos.

Los resultados de distintos marcos raíz consecutivos se separan con líneas de guiones.

Datos de entrada de ejemplo

```
7 1
1 0 D 50 0
2 0 B 10 0
3 0 I 40 0
4 0 D 20 1
5 0 C 30 0
6 5 D 20 0
7 5 I 10 1
1000 1000
2 2
1 0 D 100 1
2 0 C 30 1
100 50
200 100
0 0
```

Resultados de salida de ejemplo

```
Marco Raiz 1
-------------------------------------------------
   Pantalla: 1000 x 1000
      Marco: 1   (950, 0)   (999, 999)
      Marco: 2   (0, 990)   (949, 999)
      Marco: 3   (0, 0)   (39, 989)
      Marco: 4   (70, 0)   (949, 989)
      Marco: 5   (40, 0)   (69, 29)
      Marco: 6   (50, 0)   (69, 29)
      Marco: 7   (40, 0)   (49, 29)
-------------------------------------------------


Marco Raiz 2
-------------------------------------------------
    Pantalla: 100 x 50 es demasiado reducida
-------------------------------------------------
   Pantalla: 200 x 100
      Marco: 1   (1, 0)   (199, 99)
      Marco: 2   (0, 0)   (0, 99)
-------------------------------------------------
```

Programación de Novática

1998

Pendiente de publicación sólo el último número del año, el tema que cubrirá su bloque monográfico será el siguiente:

Noviembre-Diciembre (Número 136)
"Informática y discapacidades"
Fecha de publicación: segunda quincena de Diciembre
Coordinador: Julio González Abascal
(*julio@si.ehu.es*)

Nota: A los autores de los artículos enviados para esta monografía les ha sido ya comunicada por el Coordinador la decisión tomada por el Comité de Revisión sobre su aceptación o no.

1999

Tras estudiar las propuestas presentadas tanto por sus propios miembros como por diversos socios, el Consejo Asesor de Medios de Comunicación de ATI (CAMCOM) ha tomado la decisión de dejar cerrada la programación de los bloques monográficos correspondientes a los dos primeros números de dicho año, que, salvo causas de fuerza mayor, serán los siguientes:

Enero-Febrero (Número 137)
"Data Mining - Data Warehouse"
Fecha de publicación: segunda quincena de Febrero
Coordinador: Joan Tort Arnau
(*jtort@mail.bcn.es*)

Nota: Para esta monografía no habrá petición de artículos.

Marzo-Abril (Número 138)
"Legislación sobre TIC"
Fecha de publicación: segunda quincena de Abril
Coordinadores: Rafael Fernández Calvo (*rfcalvo@ati.es*), Emilio del Peso (edelpeso@tsai.es)

Nota: Para esta monografía no habrá petición de artículos.

Coordinación Editorial

Novedades en las Secciones Técnicas

A partir del presente número se producen cambios de denominación de tres de las dieciocho Secciones Técnicas con las que cuenta actualmente nuestra revista. "Educación Asistida por Ordenador" pasa a denominarse "Tecnologías para la Educación", "Inteligencia Artificial" se convierte en "Ingeniería del Conocimiento" y "Seguridad y Redes" pasa a llamarse simplemente "Seguridad". Estos cambios se producen con objeto de afinar la terminología y adecuarla a los cambios que se producen el mundo de las TIC.

Asimismo la Coordinación Editorial se complace en anunciar la incorporación de Josep Sales Rufí a la sección "Tecnologías para la Educación", donde acompañará en las tareas de coordinación a Benita Compostela. Josep Sales, socio de ATI y profesor en el IES Lluch i Rafecas de Vilanova i la Geltrú, pertenece al grupo ESPIRAL, que desde hace años se dedica a impulsar el uso de las TIC en las aulas y que siempre ha tenido estrechas relaciones con ATI.

Normas de publicación para autores

Aprobadas por el Consejo Editorial y válidas a partir del 1 de Enero de 1997.

Novática agradece su contribución desinteresada a los miles de autores que han elegido y elegirán sus páginas para presentar sus contribuciónes al avance profesional y tecnológico de la Informática.

Periodicidad: Novática tiene periodicidad bimestral y aparece en los meses de febrero, abril, junio, septiembre, octubre y diciembre, salvo retrasos debidos a causas de fuerza mayor.

Normas de revisión: con los artículos no solicitados se seguirán las siguientes reglas: en el caso de los bloques monográficos, serán los Coordinadores de los mismos los que decidan sobre su publicación o no; los artículos no destinados a monográficos serán revisados por al menos un revisor.

Los artículos deberán ser enviados a su oficina de Coordinación Editorial (Novática-ATI. Calle Padilla 66, 3º dcha. 28006 Madrid, *novatica@ati.es*) y serán publicados tan pronto como sea posible, teniendo siempre en cuenta las citadas normas de revisión así como las reglas sobre tamaño, soportes, lengua, *copyright* y estilo descritas a continuación.

Tamaño: Los artículos deberán tener un máximo de 3.000 palabras, lo que equivale a entre 8 y 10 páginas DIN A4 a doble espacio (fuente Times, tamaño 12), incluyendo resumen, figuras, bibliografía y notas. Sólo en casos excepcionales se aceptarán artículos superiores a dicho tamaño. Salvo excepciones, los artículos no deberán incluir más de cinco ecuaciones ni más de doce referencias bibliográficas o notas, y deberán incorporar título, un resumen (máximo 20 líneas), nombre y afiliación del autor/a(es/as), así como su dirección postal y electrónica, y números de teléfono y fax.

Soportes: Los artículos deberán ser enviados a Novática en formato digital, bien a través de la red bien en soporte magnético (disquete) mediante correo postal. En caso de envío por correo electrónico, si el fichero tiene un tamaño superior a los 150.000 bytes, es preciso enviar el fichero comprimido con el programa *Pkzip* e indicando qué procesador de texto entre los citados a continuación se ha utilizado. Novática se edita actualmente en **PageMaker 6.0 para Windows**. En ambos casos (correo electrónico o disquete) el artículo debe llegar en uno de los procesadores de texto más habituales para PC (Word, Wordperfect, Wordstar, Write, etc.), en HTML, RTF o, en último caso, en ASCII si se teme una difícil lectura o no se dispone de un procesador de texto estándar. También en ambos casos (correo electrónico o disquete) es preciso enviar una edición completa del artículo en papel para el cotejo de texto y **gráficos**. Estos se admitirán *solamente en blanco y negro* y con una buena resolución; además cada uno de los gráficos deberá enviarse en *hoja aparte*, tamaño DIN A4.

Lengua: Aunque Novática admite artículos en todas las lenguas reconocidas por la Constitución española y los Estatutos de las diferentes Comunidades Autonómas, dado que el ámbito de difusión de la revista conlleva su publicación en castellano, como lengua oficial común, los autores deberán presentar sus artículos en la lengua oficial de su elección y en castellano. Novática enviará a los socios y suscriptores que lo soliciten una copia de la versión original de aquellos artículos que hayan sido escritos en una lengua oficial que no sea el castellano.

Copyright: Novática da por supuesto que un autor acepta las presentes normas al enviar su original y que, en caso de que esté destinado a ser publicado en otro medio ajeno a ATI (o ya haya sido publicado) debe de aportar la autorización del editor del mismo para su reproducción por Novática (incluida la autorización para realizar traducciones). Novática por tanto no asume ninguna responsabilidad sobre derechos de propiedad intelectual si un texto se ha publicado en otro medio de comunicación, sea inadvertidamente o no, por parte del autor. Todo autor que publique un artículo en Novática debe saber que autoriza su reproducción, citando la procedencia, salvo que el autor declare explícitamente que desea proteger sus derechos con © o *copyright*. Asimismo, se entiende que el autor acepta que, además de en Novática, su artículo podrá ser también publicado y distribuido electrónicamente, mediante los medios habituales de difusión de ATI (servidor WWW, listas de distribución Internet, etc.) en su totalidad o parcialmente.

Estilo: Novática respeta totalmente el estilo y contenido de cada artículo, pero da por supuesta la autorización del autor para retocar su ortografía, léxico, sintaxis, titulación y paginación, a fin de facilitar su comprensión por el lector y de subsanar posibles errores. Cualquier cambio que afecte al contenido será consultado con el autor.

novatica
Revista de la Asociación de Técnicos de Informática

HOJA DE SUSCRIPCIÓN
Rellene esta hoja y envíela a:
Novática (Suscripciones)
Vía Laietana 41, 1º, 1ª
08003 Barcelona, España
Tlfno.: (93) 412 5235 Fax: (93) 412 7713
E-mail: *novatica@ati.es*

Apellidos .... Nombre..
Empresa/Organismo..CIF/NIF..
Domicilio..
Ciudad.. Provincia..
Código Postal.. País..
Teléfono.......................... Fax.......................... E-mail ....

Nota: Rellenar los siguientes datos solamente si la dirección de envío es diferente de la anterior.
Domicilio para envíos..
Ciudad.. Provincia..
Código Postal.. País..

Deseo suscribirme a Novática (6 números al año) en las siguientes condiciones (marcar con X la opción deseada y, en su caso, la cantidad de suscripciones solicitadas):

* *España*
- ❒ 1 suscripción: 9.000 pts. +4% IVA
- ❒ __ suscripciones: 8.250 pts. cada una +4% IVA

* *Otros países de la Unión Europea y Marruecos*
- ❒ 1 suscripción: 11.000 pts.
- ❒ __ suscripciones: 10.500 pts. cada una

* *Resto del mundo*
- ❒ 1 suscripción: 95 dólares USA
- ❒ __ suscripciones: 90 dólares USA cada una

Abonaré el importe:
- ❒ Con domiciliación de cobro por entidad bancaria (deberá rellenar los datos bancarios abajo solicitados)
- ❒ Talón adjunto
- ❒ **Transferencia bancaria a la cta. 3025-0004-30-1500001500, Caja de Ingenieros, C/ Buen Pastor 5, 08021, Barcelona (España)**

Fecha .... Firma

DATOS BANCARIOS PARA DOMICILIACIÓN

Banco/Caja..

CÓDIGO CUENTA CLIENTE			
ENTIDAD	OFICINA	D.C.	NÚMERO DE CUENTA

NV 135

✂ -

AUTORIZACIÓN DE COBRO
Le rogamos repita los datos bancarios otra vez. ATI se encarga de su envío al Banco o Caja.

Banco/Caja..

CÓDIGO CUENTA CLIENTE			
ENTIDAD	OFICINA	D.C.	NÚMERO DE CUENTA

Ruego a Uds. se sirvan tomar nota de que, hasta nueva orden mía en contra, deberán adeudar en mi cuenta arriba indicada los recibos que a nombre de D./Dª.. le sean presentados por la Asociación de Técnicos de Informática (ATI), en concepto de suscripción a la revista Novática.

Fecha .... Firma

¿ Quién puede ser socio de ATI ?

- ***Socios de número***
  - Deben acreditar un mínimo de tres años de experiencia profesional informática, o dos años, si se posee un título de grado superior o medio, ***o bien,***
  - poseer un título de grado superior o medio relacionado con las Tecnologías de Información, ***o bien,***
  - haber desarrollado estudios, trabajos, o investigaciones relevantes sobre dichas tecnologías.

- ***Socios Estudiantes***
  - Deben acreditar estar matriculados en un Centro Docente cuya titulación dé acceso a la condición de socio de número.

- ***Socios Adheridos***
  - Profesionales informáticos que no cumplan las condiciones para ser Socios de Número o Socios Estudiantes, o también personas que, no siendo profesionales informáticos, quieran participar en las actividades de ATI.

- ***Socios Institucionales***
  - Personas jurídicas, de carácter público o privado, que quieran participar en las actividades de ATI.

Cuota socio (1998):

de Número ..... 9.500 ptas.
Estudiante ..... 4.000 ptas.
Adherido ..... 8.000 ptas.
Institucional (consultar con Secretaría)

(Enviar a cualquiera de las oficinas de ATI indicadas en el reverso de esta hoja)

Hoja de inscripción a ATI

NV 135

Deseo sólo información sobre ATI ☐

Tipo de socio: De Número ☐ Estudiante ☐ Adherido ☐

Apellidos .....
Nombre .....
Domicilio .....Nº.....Piso.....
Localidad .....Tel.....
Provincia .....C.P.....
Fecha de nacimiento ...../...../.....

Empresa/Entidad.....
.....Ramo.....
Puesto actual en ella .....
Dirección .....Nº.....
Localidad.....Tel.....
Provincia .....C.P.....
E- Mail .....Fax.....

Firma ...../...../19.....

Banco/Caja .....

CODIGO CUENTA CLIENTE			
Entidad	Oficina	D.C.	Núm. de Cuenta

Dirección .....Nº.....
Localidad .....
Provincia .....C.P.....

Autorización de cobro

Le rogamos repita los datos bancarios otra vez. ATI se encarga de su envío al Banco / Caja.

Banco/Caja .....

CODIGO CUENTA CLIENTE			
Entidad	Oficina	D.C.	Núm. de Cuenta

Dirección .....Nº.....
Localidad .....
Provincia .....C.P.....

Ruego a Uds. se sirvan tomar nota de que, hasta nueva orden mía en contra, deberán adeudar en mi cuenta arriba indicada los recibos que a nombre de D.....
.....
les sean presentados por la ASOCIACIÓN DE TÉCNICOS DE INFORMÁTICA (ATI)

Firma ...../...../19.....

Datos complementarios

Títulos Superiores o Medios que posee y centros otorgantes:

.....
.....
.....

Resumen experiencias .....
.....
.....
.....

Número de años experiencia informàtica .....

Presentado por los socios

Apellidos y Nombre .....
Número de socio ..... Fecha.../.../.....

Firma

Apellidos y Nombre .....
Número de socio ..... Fecha.../.../.....

Firma

ATI envía a sus socios información procedente de otras entidades, fundamentalmente sobre productos y servicios relacionados con la informática. Si no desea recibir dicha información, indíquelo a continuación. En cualquier caso ATI cumple escrupulosamente la Ley de Datos Personales.

- Anuncios de ATI solamente: ☐
- Anuncios de ATI y otras entidades: ☐

http://www.ati.es

Asociación de Técnicos de Informática

Vía Laietana, 41, 1º. 1ª
08003 BARCELONA
VOZ: (93) 412 52 35
FAX: (93) 412 77 13
E-mail: *secregen@ati.es*

c/. Padilla, 66 3º dcha.
28006 MADRID
Voz: (91) 402 93 91
Fax: (91) 309 36 85
E-mail: *secremdr@ati.es*

Av. Republica Argentina, 25, 4.º
41011 SEVILLA
Voz: (95) 427 30 57
Fax: (95) 427 30 57
E-mail: *secreand@ati.es*

c/. Palomino, 14, 2º
46003 VALENCIA
Voz/Fax: (96) 391 85 31
E-mail: *secreval@ati.es*

c/. San Miguel. 2. 9º B
50001 ZARAGOZA
Voz: (976) 23 51 81
E-mail: *secreara@ati.es*

Asociación de Técnicos de Informática

Una Asociación abierta a todos los informáticos

Una Asociación útil a sus socios, útil a la Sociedad

¿Qué es ATI?

- ✓ ATI es una asociación *abierta a todos los técnicos y profesionales informáticos y que está implantada en todo el país a través de los Capítulos Territoriales existentes en diversas Comunidades Autónomas*. Creada en 1967, es en la actualidad la asociación más dinámica y más numerosa (más de 5.000 socios a principios de 1998) de las existentes en el Sector Informático español, con sedes en Barcelona (sede general), Madrid, Sevilla, Silleda (Pontevedra), Valencia y Zaragoza.

- ✓ ATI es miembro de *CEPIS (Council for European Professional Informatic Societies)* y tiene un acuerdo de colaboración con *ACM (Association for Computing Machinery)*. En el plano interno tiene establecidos acuerdos de colaboración o vinculación con Ada Spain, AII y ASTIC.

¿Cuales son los objetivos de ATI?

Se resumen en uno esencialmente:

SER UTIL A SUS SOCIOS Y A LA SOCIEDAD

Más concretamente, ATI se propone:

- ✓ Defender, promover y mejorar el desarrollo de la actividad de quienes ejercen como profesionales y técnicos en el campo de las Tecnologías de la Información.
- ✓ Facilitar a sus socios el intercambio de experiencias, la formación y la información sobre dichas tecnologías.
- ✓ Contribuir a la promoción y desarrollo de las Tecnologías de la Información.
- ✓ Mantener relaciones con el entorno social y económico en que la Asociación se mueve.
- ✓ Fomentar la difusión de las Tecnologías de la Información y estudiar su impacto sobre la sociedad y sobre los ciudadanos.
- ✓ Colaborar con otras entidades profesionales informáticas implantadas tanto en nuestro país como fuera de él, especialmente en Europa y en la América Latina.

¿Cómo está organizada ATI?

- ✓ La *Asamblea General* de socios y la *Junta Directiva General* son los órganos máximos para el conjunto de la asociación.
- ✓ Los *Capítulos Territoriales*, con sus *Asambleas Territoriales* y sus *Juntas Directivas Territoriales*, estructuran la asociación en las Comunidades Autónomas mediante una organización de orientación federal.
- ✓ Las *Secciones Técnicas* y los *Grupos de Trabajo* sobre diversos temas facilitan la participación de los socios en las actividades de la Asociación.

¿Qué ofrece ATI?

Mediante el pago de una cuota anual, los socios de ATI pueden disfrutar de la siguiente gama de servicios:

- ✓ *Formación Permanente*
  - Cursos, Jornadas Técnicas, Mesas Redondas, Seminarios, Conferencias, Congresos
  - Secciones Técnicas y Grupos de Trabajo sobre diversos temas
  - Intercambios con Asociaciones Profesionales de todo el mundo
- ✓ *Servicios Profesionales*
  - Asesoramiento profesional y legal
  - Modelo europeo (EISS) de referencia de carreras profesionales
  - Peritajes, diagnósticos y certificaciones
  - Bolsa de Trabajo
  - Plan REMAKE de actualización profesional
- ✓ *Servicios de Información*
  - Revista Novática (bimestral)
  - Boletín Informativo (mensual)
  - Servidor Web
  - Servicio ATInet (acceso básico gratuito a Internet, correo electrónico, listas de distribución generales y especializadas, Intranet asociativa)
  - Biblioteca
- ✓ *Actividades Sociales*
  - Promociones y ofertas comerciales
  - Intercambios internacionales

Juntas Directivas

Junta Directiva General

Presidente: Alberto Llobet Batllori
Vicepresidente Primero: Fernando Piera Gómez;
Vicepresidente Segundo: Celestino Martín Alonso; Secretario: Miquel Sàrries Griñó; Interventor-Tesorero: Sebastián Aguado Alonso
Vocales: Fernando Sanjuán de la Rocha, Asunción Yturbe Herranz, José Onofre Montesa Andrés, Antoni Carbonell Nogueras, Pedro Gómez Grau, Xavier Iribarne Navarro

Capítulos Territoriales (Presidentes)

Andalucía (Juan Carlos Granja Alvarez); Aragón (Javier Bruna Sánchez); Catalunya (Pere Lluis Barbarà Butifull); Madrid (Angel Alvarez Rodríguez); Valencia (José López Soriano)

¿Dónde está ATI?

Servidor Web: *http://www.ati.es*

Sede General y Capítulo de Catalunya
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.(93)4125235; fax 4127713 / *secregen@ati.es*
Capítulo de Andalucía
Isaac Newton, s/n, Ed. Sadiel (Isla Cartuja), 41092 Sevilla
Tlf./fax (95)4460779 / *secreand@ati.es*
Capítulo de Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax (976)235181 / *secreara@ati.es*
Capítulo de Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.(91)4029391; fax.3093685 / *secremdr@ati.es*
Capítulo de Valencia
Palomino 14, 2ª, 46003 Valencia
Tlf./fax (96)3918531 / *secreval@ati.es*
Grupo Promotor de Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.(986)581413; fax 580162 / *gpgal@ati.es*
Revista Novática
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.(91)4029391; fax.3093685 / *novatica@ati.es*