e-fectivo

Un instrumento para realizar pagos electrónicos en Internet

Tesis de grado

Maestrando:

Ernesto Molinari

Tutor:

Dr. Ignacio González García

Noviembre de 2001

Indice general

1 INTRODUCCIÓN Y PLANTEO DEL PROBLEMA

1.1 Facilidades para la lectura del presente documento

Con el fín de facilitar la lectura y comprensión del trabajo de tesis que presentamos, hemos incorporado la presente guía de lectura.

Unos lineamientos generales que deseamos transmitir son los siguientes:

- El documento consta de una lista de acrónimos, con el fin de simplificar la comprensión de las abreviaturas tan frecuentemente usadas en la jerga de la informática.

- Consta además de un glosario, el cual abarca la terminología empleada en este documento. El mismo ha sido extendido con el objetivo de ser usado como referencia en lecturas conexas con esta problemática.

- Hemos incorporado una lista de direcciones WEB consultadas donde el lector podrá obtener mayor información vinculada al tema tratado.

Describimos a continuación el contenido de los capítulos considerados 'núcleo' de nuestra presentación.

Cada uno de ellos fue concebido en forma atómica, es decir puede ser leído como una unidad en sí misma.
De todas formas aquel lector que desee tener un conocimiento integral del problema debería efectuar la lectura integra y correlativa de los contenidos.

Vemos a continuación una breve descripción de los capítulos centrales.

Capítulo 2: El dinero: ayer, hoy, y mañana.

El dinero electrónico no es otra cosa que bytes que circulan a través de las redes de información como Internet. Conocemos dinero bancario que es muy parecido al dinero electrónico ya que se basa en la confianza de las personas que lo utilizan para existir.

Si no existiera esa confianza en que el dinero bancario puede funcionar sin existir físicamente, entonces el dinero electrónico tampoco podría existir. Es por ello, que, con el advenimiento de nuevas tecnologías

como Internet, con las que la gente puede establecer relaciones mucho más próximas con los nuevos desarrollos de la tecnología, pensamos que se está creando el mejor campo donde cultivar la confianza en esos mecanismos de pago nuevos y en el dinero electrónico.

Es importante, y contribuye a todo lo que decimos, que las características fundamentales del dinero, tal como lo conocemos hoy, se presenten también en sus nuevas modalidades, es decir:

- deberá ser aceptado comúnmente como medio de cambio, y no ser susceptible de venta como un bien, un producto o una mercancía.
- deberá ser dado y aceptado como pago final de una deuda: es decir, tiene que tener poder cancelatorio de las deudas.
- podrá trasladarse y transmitirse libremente mediante su entrega (Aquí los abogados tendrán trabajo extra para definir lo que debe entenderse por entrega, sobre todo si intervienen medios electrónicos de transmisión).
- deberá tener valor por sí mismo, sin necesidad de acudir a otros respaldos que lo completen o impongan de determinadas cualidades.
- deberá, como consecuencia del anterior parámetro, estar libre de cualquier reclamo posterior a su entrega (como actualmente lo es cualquier medio de pago).

Estas características necesarias deben permitir la difusión del dinero electrónico cualquiera sea la forma en la que se lo presente.

Sin estas características, el dinero electrónico no tiene posibilidades de salir adelante ya que conforman la mayoría de elementos necesarios para que el dinero electrónico tome el impulso que necesita.

Capítulo 3: Análisis del mercado

A lo largo de este capítulo se analiza el potencial mercado de usuarios, su cuantificación y caracterización sociodemográfica para aplicar el modelo de solución en la República Argentina. Se describen, asimismo, los comportamientos y actitudes de los usuarios de Internet en base a distintas estadísticas y encuestas de reciente factura. De resultas de este análisis podemos perfilar el conjunto de potenciales usuarios para el nuevo servicio.

Capítulo 4: Relevamiento y caracterización de soluciones de pagos electrónicos - Casos observados

Se decribe en éste el resultado de la observación de distintas soluciones de dinero electrónico disponibles para Internet en la actualidad, tanto en el ámbito local como internacional. Se presenta un resumen de las principales modalidades operativas y cobertura de funcionalidades para cada caso observado. Asimismo, se incluyen referencias visuales de los sitios WEB de cada uno de los servicios analizados.

Las principales marcas de soluciones analizadas son: InternetCash, e-pagofácil, Boleto Bancario, Pay Pal, C2it, Patagon.

Capítulo 5: Modelos operativos observados

Del análisis de las soluciones presentadas en el capítulo 4, surgen como factibles de ser implementados dos modelos conceptuales

- Con el instrumento de pago ya abonado (prepago), "cargado" con un monto (adquisición de efectivo virtual).
- Con pago "real" del monto de la compra posterior a la realización de ésta (postpago), disparándose la entrega del bien cuando se confirma dicho pago real.

Estos modelos son denominados conceptualmente 'prepago' y 'postpago'. Describimos la instrumentación de ambos modelos.

Capítulo 6: Conclusiones sobre los modelos observados

Como conclusión de las ventajas y desventajas analizadas, se puede considerar mayor la viabilidad del modelo operativo prepago, básicamente por las siguientes condiciones:

- Mayor versatilidad y extensibilidad de uso (C2C, recarga, pagos sobre monederos corporativos, mayor control del gasto por menores, uso como "gift certificate" – "vales de regalo")

- Mejor control y certeza de venta para los comercios (no hay uso por quien luego no pague), con relación al manejo de los pedidos no confirmados, el stock requerido, y la administración de entregas.

Capítulo 7: Descripción operativa de la solución

Describimos en este capítulo los modelos operativos para la solución propuesta, contemplando el hacerlo según la siguiente apertura:

La adquisición del efectivo virtual

- Se contemplan 2 posibles vías alternativas de adquisición:
- Desde la red de ATMs, para usuarios de tarjetas de dichas redes
- Desde una terminal POS de los servicios instalados por los emisores de TC, o a través de otras soluciones corporativas (supermercados, estaciones de servicio, etc.). Para todo usuario

Requisitos críticos del modelo

- Se describen dos aspectos que resultan críticos a los fines de concretar la especificación de este modelo de solución de pagos electrónicos para Internet:
  - **Cobertura de la seguridad**
  - **Aspectos legales**

Capítulo 8: Enfoque de Marketing

Describimos en este capítulo la visión de Marketing y su visión estratégica del posicionamiento de este instrumento de pago; de manera tal de tornar factible el modelo económico financiero.

- Ser un medio de pago en efectivo reconocido, para las operaciones comerciales realizadas a través de Internet.
- Orientado en su primera fase al consumo del público joven, y a los consumidores de Internet con renuencia al uso de la tarjeta de crédito en dicho medio.

Capítulo 9: Enfoque de Comercios

Describimos en este capítulo la visión para la selección de comercios que hagan viable el modelo económico financiero.

Capítulo 10: Análisis Económico-Financiero

Describimos en este capítulo la viabilidad de un modelo con rentabilidad sustentable.

Analizamos en este capítulo, las conclusiones propias de este análisis (**Fortalezas, Debilidades, Oportunidades, Amenazas)**

1.2 Enfoque del trabajo

Parece prudente empezar esta exposición planteándonos una serie de interrogantes, los cuales intentaremos contestar a lo largo del desarrollo de nuestro trabajo.

¿Qué es el dinero?

¿Qué son los nuevos mecanismos de pago?

¿Cuáles son los mecanismos de pago en desarrollo?

¿Qué es dinero electrónico?

¿Cuáles son los sustitutos del dinero como lo conocemos tradicionalmente?

¿Cuáles son las ventajas y desventajas de introducir un instrumento nuevo en las operaciones/transacciones comerciales?

¿Desaparecerá el dinero físico? ¿Por qué?

Si bien los interrogantes parecen ser lo suficientemente ambiciosos como para provocar dos primeras reacciones:

- desertar y/o acotar la óptica de nuestro trabajo,
- aventurarnos a encontrar respuestas que generen nuevos interrogantes y crear la espiral del conocimiento.

Escogemos el segundo camino convencidos de que daremos respuestas, y que sembraremos dudas que podrán ser la fuente de futuros trabajos, para aquellos interesados en nuestro planteo.

Hemos considerado prudente aproximarnos al punto de análisis desde dos perspectivas:

A) El marco teórico o paraguas bajo el cual analizar las implementaciones comerciales de dinero virtual

B) Un análisis del mercado, la oferta potencial, la comparación entre actores y la demanda.

A) El marco teórico o paraguas bajo el cual analizar las implementaciones comerciales de dinero virtual

Bien, empecemos con el interrogante 'más primitivo':

- *¿ Qué es el dinero ?*

Quizás la mejor definición que podemos dar del dinero es que es un medio de pago cuyo principal (si no único) fundamento es la confianza de que los demás lo aceptan como medio de pago, es decir, que mediante su entrega a terceros que tienen cosas que no son dinero, éstas pueden ser adquiridas en propiedad.

En la conciencia común se identifica dinero con una especie del mismo: el dinero legal, que, como definen Francisco Mochón y Víctor Beker , es el que es emitido por una institución que monopoliza su emisión y que adopta la forma de monedas metálicas y billetes. Este es el dinero en efectivo, los pesos, las pesetas, los dólares, los francos, las liras, las libras o los escudos.

¿ Encontramos características/atributos que hagan del dinero un 'objeto'/sujeto especial de análisis ?

Sí los posee, y veremos sólo algunos de ellos, los más relevantes para esta introducción a nuestro trabajo. Los restantes, y que afectan nuestro desarrollo serán expuestos a lo largo del trabajo de tesis que presentamos.

El dinero en efectivo, el dinero en metálico, se caracteriza, sobre todo, por no ser nominativo y por tener un valor garantizado por el emisor del dinero y no por el que lo utiliza en una transacción.

Hoy el valor del dinero físico, sin valor propio, reside en la garantía de los bancos locales, nacionales e internacionales, es decir, en realidad reside en la confianza de todos, personas, empresas y gobiernos, en un sistema financiero virtual.

Cabe preguntarnos ¿ Cuál es el fin del dinero, desde la perspectiva de este trabajo de tesis?

La respuesta es simple, aunque no son sencillos los mecanismos técnicos, sociales, políticos, necesarios para implementarla.

Para el objeto de nuestro estudio la respuesta es: el intercambio de bienes y/o servicios entre diferentes actores sociales.

El origen de esta actividad se remonta al trueque o permuta. Ahora en el umbral del siglo XXI, cuando las transacciones financieras y

comerciales de un lugar a otro del planeta se efectúan en tan sólo décimas de segundo, el trueque sigue vigente (para poner un ejemplo bastante sencillo, dos personas que utilicen medios informáticos para comunicarse, intercambian trabajos, fotos, videos, etc., sin que intervenga moneda alguna).

Mas, ¿ Cómo resolver la situación en la cual desde ambos extremos del planeta desean abonar y/o recibir dinero por el trueque realizado ?.

La respuesta que empieza a perfilarse es: nuevos mecanismos de pago.

El comercio electrónico y las nuevas tecnologías involucradas encuentran un aliado esencial en los nuevos mecanismos de pago puesto que tanto unos como otros se sirven de soporte. El desarrollo del comercio a través de Internet fomenta el uso de formas sencillas de abonar los productos o servicios que se adquieren y, a su vez, la existencia de mecanismos más útiles, rápidos o seguros favorece el desarrollo de las transacciones en línea.

Estos nuevos sistemas o mecanismos de pago encuentran uno de sus primeros problemas cuando tienen que entrar en el mercado: la baja compatibilidad entre ellos y, por lo tanto, la utilización de unos o el hecho de que los vendedores adopten un método, hace que queden excluidos total o parcialmente los demás.

Cabe plantear porqué no adquirir todos y cada uno de los sistemas que están en desarrollo en la actualidad lo que, por el momento, es antieconómico y poco práctico.

Pensemos, por un momento, en la realidad: los negocios hoy en día funcionan con métodos de pago casi unificado. Tenemos, por un lado, las tarjetas de crédito y, por otro, el dinero físico. Para que el dinero electrónico y cualquiera de los mecanismos que se están desarrollando puedan funcionar y ser competitivos, tienen que ofrecer mayores ventajas que los mecanismos convencionales que se utilizan hoy y, por lo tanto, no entrañar mayor dispersión.

Es por ello que aparece el concepto de interoperabilidad: es decir, la necesidad de que los mecanismos que se creen en el futuro puedan funcionar simultáneamente y sin requisitos particulares que no sean comunes a todos ellos. Pensamos que, en el largo plazo, está interoperabilidad existirá por sí sola, ya que de otro modo los mecanismos de pago no van a funcionar y no van a ser atractivos para los consumidores y las instituciones financieras, y menos aún para el mercado general.

Finalizada nuestra introducción delinearemos los pilares (atributos mayúsculos) sobre los cuales podemos **construir 'e-fectivo', como hemos dado en llamar a este instrumento de pago.** .

El uso de este sistema requiere un convencimiento por parte del interesado de que este dinero que utiliza, posee el mismo valor que el dinero el cual él mismo depositó, y que por tanto, cuenta con todas las características del original.

Al respecto hemos de decir que el dinero electrónico primeramente no ha cambiado ningún estándar monetario, así pues se designa al dinero electrónico como dólares y centavos dentro de los Estados Unidos, en Argentina tomamos como unidad de referencia del dinero electrónico al peso, y es altamente factible que en Europa usen la unidad 'Euro' . Por lo que hemos expuesto no se ha logrado aún la antes mencionada interoperabilidad. Podemos imaginar un futuro en el cual la unidad monetaria de referencia para el dinero electrónico sea una en común.

Se puede seguir enumerando una serie de elementos que no se cumplen, tales como la persistencia o «durabilidad». Si consideramos al dinero electrónico como tal almacenado en medios magnéticos, los mismos pueden fallar, en cuyo caso una falla física haría perder instantáneamente la calidad de durable a cierta cantidad de dinero allí almacenada.
Cabe acotar en este punto que la 'falencia' mencionada no es característica propia y excluyente del dinero electrónico. También lo es del dinero 'físico', pero que exista también en este último no excluye la validez de requerir que la característica se cumpla.

Otro ejemplo de ello, es el uso de las llamadas «Smart Cards». Estas tarjetas que crecen en popularidad, tienen la desventaja de cierta inestabilidad de persistencia. Ya que si se corrompen o no funcionan, inutilizan todas las operaciones y por tanto su calidad de «valor» en el «tiempo».

Otro punto de vital importancia es la autenticidad del dinero electrónico.

El anonimato y la privacidad de las partes son otro punto a tener en cuenta en una transacción económica electrónica. Los bancos no deberían poder saber cómo y donde un cliente gasta su dinero y a su vez, en determinadas transacciones en donde se debe llevar un control de identidad del comprador y el vendedor, los datos personales de ambas partes deberían ser seguros respecto a falsificaciones o cambios, tal como ocurre cuando se utilizan cheques.

Una transacción no debe ser repudiable.

Esta característica concierne a las reglas implícitas en un contrato comercial. Hablamos de contrato en términos de intercambio de elementos legales. Por un lado el cliente entrega una orden de solicitud de un producto determinado, por el otro el vendedor entrega al cliente una boleta que garantiza la entrega de dicho producto. En medio de estos procedimientos está el intercambio de dinero. En el caso de transacciones comerciales electrónicas, el cliente debería no poder negarse al envío de una solicitud u orden de compra (si así se estableciere), y asimismo debería poder rechazar una orden enviada en caso de ser víctima de un fraude. Similares restricciones deberían cumplirse en pos del comerciante.

Todo lo expuesto nos lleva a los primeros capítulos de nuestra tesis:

- **el marco de seguridad para el dinero electrónico y su consecuencia (el comercio electrónico);**
- **el marco legal;**
- **el marco operativo para un modelo de 'e-fectivo'.**

Como comentáramos al inicio de la presente Introducción, nuestro trabajo se basa en un marco o 'paragua' teórico (hasta aquí descripto) el cual nos dará lugar para el análisis y la comprensión de la 'realidad del mercado'.

Vemos a continuación la presentación de este segundo aspecto, la 'realidad'.

B) Un análisis del mercado, la oferta potencial, comparación entre actores y la demanda

En este contexto, el presente trabajo tiene por objetivo el presentar una alternativa de medio de pago electrónico que se caracterice por:

- Permitir operar pagos en Internet, originados por compras realizadas en el mismo entorno
- Alcanzar un espectro de aplicabilidad dentro de lo que se denomina B2C y C2C, en el ámbito del e-commerce
- Cubrir facilidades de realización de pagos para distintos segmentos de usuarios
- Conformar las seguridades requeridas para operar en una red pública (integridad transaccional, autenticidad de cliente y servidor, privacidad, no repudio transaccional)
- Permitir la utilización de montos de operación de bajo, medio y alto valor nominal
- Permitir mantener los atributos del dinero (reserva de valor, unidad de cuenta, intercambiabilidad, autenticidad)
- Conformar un equilibrio entre la necesidad de proveer al anonimato operacional del usuario final, y el mantenimiento de un soporte de información que dé trazabilidad al curso transaccional

Los números más conservadores referentes a las transacciones comerciales minoristas realizadas por medio de Internet hacen referencia a un volumen de 82 Millones $ (Fuente Boston Consulting Group, Publicado por Reuters. Nov 2000).

La necesidad de medios de pagos alternativos, frente a estos canales de compra/venta emergentes se torna imprescindible. El índice de bancarización de la población argentina es de aproximadamente 27% (Fuente: Rev. Mercado, Julio 2000), con tendencia creciente a la luz de los objetivos de la industria financiera argentina tanto como por la formalización del mercado laboral que impulsa el Estado Argentino.

Existen, además, dos factores que inciden en el uso de los medios de pago tradicionales sobre el entorno de Internet.

El primero de ellos es el temor que aún causa en los usuarios de medios de pago tradicionales el utilizarlos para abonar la adquisición de bienes y servicios a través de Internet. La introducción del número identificatorio de la tarjeta de crédito o débito, en un formulario de ingreso de datos

de un comercio de la WEB, constituye una barrera de desconfianza que no ha sido superada todavía. El alto porcentaje de fraudes detectados en el uso de tarjetas de crédito en la WEB, comparado con el que resulta de su utilización en el mundo físico (con volúmenes transaccionales enormemente superiores) es un indicador que alerta y amedrenta al usuario. Según el Gartner Group (Agosto 2000), relevadas 160 compañías de la WEB, los comercios virtuales sufren 12 veces más fraudes que los comercios reales, pagan 66 % más intereses que estos últimos, y además deben hacerse cargo de las pérdidas originadas en las disputas con el usuario, quien se presenta desconociendo la transacción (repudio).. Un más reciente estudio hecho por GartnerG2, a partir de una encuesta hecha sobre 7.000 adultos de más de 18 años, arrojó que el 60 % de ellos no comercia en la WEB por temores relativos a la seguridad transaccional y la privacidad de sus datos (Agosto 2001).

Según e-Marketer, con similar estudio (julio 2001), informa que el 50 % de los usuarios online temen por el control de su información privada. Otro informe de Ipsos-Reid indica que el 46 %, de 8500 adultos encuestados, menciona que su “mayor” preocupación es el fraude con tarjeta de crédito, siendo “moderada” la misma para el 26 % (e-Marketer – Junio 2001). El 90 % de los pagos sobre Internet son hechos con tarjeta de crédito, y los fraudes online son 12 veces más frecuentes que en el mundo real (según Gartner Group – PC Magazine – Marzo 2001).

El segundo aspecto a considerar atañe a la no disponibilidad de los medios de pago tradicionales - entiéndase tarjetas de débito y crédito - en segmentos de usuarios habituales de Internet, como lo son los jóvenes de entre 15 y 24 años. En general, este segmento no se encuentra bancarizado; sea por restricciones legales asociadas a la mayoría de edad, como por razones vinculadas a la baja inserción laboral del segmento, lo que desemboca en una improbable bancarización del mismo. Este segmento poblacional es, a su vez, el de más alta propensión a la navegación por Internet, el operativamente más hábil en la plataforma tecnológica, y el más tentado al consumo de los contenidos, bienes, y servicios que se ofrecen por Internet. Por esto, es un segmento que, normalmente, resuelve sus compras en el mundo físico y con pago en efectivo.

Por otra parte, la característica no presencial de las compras desarrolladas en Internet, y el relativamente bajo despliegue del soporte tecnológico de seguridad para este caso (en particular: autenticación del usuario y desconocimiento de la operación), ha hecho que los servicios de pago electrónico impongan altísimos contracargos a los comercios ante transacciones rechazadas o desconocidas por los usuarios. Esto empeora la aceptación del sistema de costos que ofrecen los servicios de pago electrónico en Internet, por parte de los comercios de la WEB.

Consecuentemente, existe un espacio de mercado en donde de los medios de pago conocidos no ofrecen una cobertura adecuada, y es así que el presente trabajo pretende responder a los siguientes cuestionamientos:

- Cómo 'aprovechar' esta oportunidad del mercado, si fuera tal
- Cómo capturar el segmento del mercado consumidor (personas) el cual hoy no disponen de un instrumento de pago electrónico/digital
- Cómo capturar el segmento de consumidores que temen el uso de su tarjeta de crédito en las transacciones comerciales vía Internet
- Cómo 'capturar' un porcentaje del segmento de compradores que abona en efectivo, orientándolos a nuestra propuesta de pago

Finalmente:

Nuestro trabajo consta de capítulos adicionales en los cuales analizaremos las implementaciones práctico/comerciales de medios de pago electrónico, como así también un análisis de la demanda potencial existente.

Esperamos que la lectura de los capítulos que presentamos puedan ser leídos con el agrado, preocupación e interrogantes quien recorre y observa nuestro 'futuro esperado' en la evolución de medios de pago.

2 EL DINERO: AYER, HOY Y MAÑANA

2.1 Nuevos mecanismos de pago

El comercio electrónico y las nuevas tecnologías involucradas encuentran un aliado esencial en los nuevos mecanismos de pago puesto que tanto unos como otros se sirven de soporte. El desarrollo del comercio a través de Internet fomenta el uso de formas sencillas de abonar los productos o servicios que se adquieren y, a su vez, la existencia de mecanismos más útiles, rápidos o seguros favorece el desarrollo de las transacciones en línea.
Algunas estadísticas recientes -del 31 de mayo de 1999- aportan datos de interés en este campo:

- porcentaje de crecimiento de registro de dominios comerciales de 1997 a 1999 = 118% (netcommerce magazine);
- monto gastado en publicidad en Internet durante el año 1998 = 1.900 millones de dólares (Internet Advertising Bureau);
- número estimado de internautas en 1998 = 147,8 millones;
- número de mensajes comerciales remitidos diariamente por correo electrónico en EEUU durante 1998 = 7.300 millones (eMarketer);
- número estimado de usuarios en China = 1,75 millones;
- costo de una transacción bancaria efectuada en persona en el banco = 1,07 dólares;
- costo de la misma transacción bancaria pero efectuada por Internet = 0,01 dólares (Wells Fargo Bank);
- número de páginas web en abril de 1998 = 320 millones (NYT);
- número de solicitudes de nombres de dominio en febrero de 1998 = 17,1 millones (InterNic).

Estas cifras, especialmente las que informan sobre el costo de las transacciones bancarias, pueden dar una idea bastante completa de lo que significa el potencial de este fenómeno que es la red Internet y sus desarrollos.

Según Miguel Ángel Monjas Llorente, del Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid, los potenciales consumidores se calculan en 30 millones de personas en todo el mundo (cifra en continuo aumento), con un nivel socioeconómico medio o alto.

Esta explosión del comercio electrónico debe ir acompañada de las herramientas que permitan que el comercio se desarrolle plenamente.

Queremos decir con esto que el comercio electrónico es una actividad interactiva y no se ciñe exclusivamente a la tarea de presentar los productos.

De lo que se trata es de que los consumidores puedan interactuar con las empresas que les ofrecen sus productos y servicios y que puedan pagarlos tan fácilmente como los acceden.

Los nuevos mecanismos de pago electrónico son precisamente desarrollos tecnológicos que facilitan el comercio electrónico y, más que facilitarlo, lo convierten en una realidad.

También debe quedar claro que es una forma de pago que puede servir para el comercio tal como se ha conocido durante los últimos siglos.

Efectivamente, ideas como el monedero electrónico y la tarjeta inteligente se están desarrollando tanto para el e-commerce como también para el comercio tradicional puesto que éste no muestra signos de desaparecer en plazos que imagine la razón.

¿QUE SON LOS NUEVOS MECANISMOS DE PAGO?

La respuesta es en realidad bastante sencilla pues la propia pregunta contiene la respuesta: se trata de las nuevas formas de efectuar pagos.

Lo que es algo más complicado es explicar de qué manera se instrumentan éstos, cómo pueden protegerse en una red abierta como Internet y cual es el potencial de su desarrollo en nuestras sociedades.

El comercio tradicional se desarrolla en nuestro entorno cotidiano: aparece un comprador y un vendedor, y de vez en cuando (cada día más frecuentemente) aparece un banco u otra entidad financiera, que mantiene relaciones con ambos y permite que el pago de una operación se realice sin la presencia de dinero efectivo (sería el caso de las tarjetas de crédito).

El comercio electrónico se desarrolla en un escenario que también contiene, como mínimo, un comprador y un vendedor. Generalmente, además suele llevarse a cabo una transacción económica con la intervención de un banco que se hace cargo del control efectivo del dinero. Es más, habitualmente aparecen dos bancos, el del comprador y el del vendedor, que liquidan entre ellos a través de sus redes y servicios interbancarios. Es muy similar al comercio tradicional.

En este escenario, ¿qué mecanismos de pago usamos hoy comúnmente?

Los mecanismos de pago más usados por las personas son básicamente cuatro:

1- El dinero en efectivo: el dinero en metálico se caracteriza, sobre todo, por no ser nominativo, y por tener un valor garantizado por el emisor del dinero y no por el que lo utiliza en una transacción. Hoy el valor del dinero físico, sin valor propio, reside en la garantía de los bancos locales, nacionales e internacionales, es decir, en realidad reside en la confianza de todos, personas, empresas y gobiernos, en un sistema financiero virtual. El hecho de que el uso de sistemas electrónicos de pago se haya masificado en los últimos años ha generado como resultado inmediato que nuestro contacto físico con el dinero sea cada vez más esporádico.

2- Cheque: una definición muy sencilla y simplificada de qué son los cheques sería aquellos instrumentos de pago que requieren ser validados por quien los pone en circulación.

3- Tarjeta de Crédito: Los esquemas de pago mediante tarjeta realizan su cometido aprovechando las infraestructuras ya existentes pertenecientes a las compañías de tarjetas de crédito. Generalmente el uso de este tipo de esquemas implica el envío a través de la red del número de la tarjeta, con o sin número de control.

4- El trueque o permuta: En el umbral del siglo XXI, cuando las transacciones financieras y comerciales de un lugar a otro del planeta se efectúan en tan solo décimas de segundo, el trueque sigue vigente (para poner un ejemplo bastante sencillo, dos personas que utilicen medios informáticos para comunicarse, intercambian trabajos, fotos, videos, etc., sin que intervenga moneda alguna). Los nuevos mecanismos de pago son evoluciones de estas mismas formas pero desarrolladas mediante la aplicación de nuevas tecnologías.

No vamos a hacer una exposición exhaustiva de las diferentes formas de pago que se están estudiando ya que son muy variadas y no todas tienen interés para este trabajo. Las que más sobresalen por el impacto y por las empresas u organizaciones que las secundan y desarrollan son las que siguen:

a. **Tarjetas inteligentes**
   La mayor parte de corporaciones, aún cuando se encuentran desarrollando nuevos productos financieros que implementan

diferente tecnología, por el momento utilizan las técnicas de encriptado1 de datos en sus transacciones; algunos ejemplos son: First Data/Netscape, Mondex, BarclayNet, Proton o Secure Courier.

b. **Bancos en redes globales de comunicación (Internet)**
Se trata de realizar funciones tradicionales sobre medios inseguros y sin presencia física de los interesados. Por ello, los requisitos funcionales apuntan sistemáticamente a la confidencialidad, integridad y autenticación de los objetos y las partes. Y para ello parece denominador común el uso de técnicas criptográficas. Los primeros bancos en trabajar en la red fueron los que siguen, aunque hoy todos lo hacen de forma más o menos importante:

- First Virtual: Primer banco creado en la propia Internet. El usuario solo efectúa pagos si queda satisfecho.
- First Bank of Internet (FBOI): intermediario entre vendedor y comprador.
- Wells Fargo Bank
- Bank of America
- Banesto
- La Caixa

c. **Cheques**

El proyecto más genérico es el Cheque Electronico. Este proyecto hizo su debut en los Estados Unidos cuando se emitió el primer cheque electrónico el 30 de junio de 1998 y fue enviado por el Gobierno por email. El Departamento del Tesoro desde hace algunos años ha estado estudiando la posibilidad de emitir cheques electrónicos. Está entidad ha manifestado que en los próximos años espera tener un modelo de cheque electrónico finalizado y utilizable por todo el mercado. Una de las mayores ventajas del cheque electrónico, dice el Departamento del Tesoro, es la eliminación de procesos caros para el comercio y, además, se utiliza de la misma forma que el cheque común.

El nuevos cheque electrónico está diseñado con los mejores mecanismos de seguridad de manera que los utilizadores del mismo no tendrán miedo de que se vulnere su contenido y, en consecuencia, podrá utilizarse libremente y en grandes cantidades. Esta segunda fase será la que hará que cheque pueda funcionar en todo el mercado.

Ahora vamos a ver cómo es un cheque electrónico:

Para empezar hemos decir que cheque electrónico contiene la misma información del cheque común.

1. Están basados ambos en el mismo sistema legal.

2. También ambos pueden contener todo tipo de información e intercambiarse directamente entre las partes

3. Los cheques electrónicos pueden utilizarse en cualquier transacción en la que los cheques comunes se utilizan hoy.

4. Además, permiten incluir mayor información que los cheques basados en papel.

Cómo funcionan los cheques electrónicos:

En realidad, el cheque electrónico funciona de la misma forma que cheque común. En primer lugar, el emisor escribe el cheque utilizando uno de los procesadores de texto que todos conocemos, y remite este cheque electrónico al pagador también mediante medios electrónicos. A continuación el pagador deposita el cheque electrónico en un banco y recibe crédito. El banco que recepciona el cheque electrónico lo convalida con el banco del emisor el que, además lo acredita directamente en la cuenta del emisor. Todo este proceso, naturalmente, se realiza en pocos segundos y el costo de la transacción ha sido mínimo.

Que ofrece de nuevo el cheque electrónico:

1. La posibilidad de manejarse con cheques a través de Internet, lo que hace que sus posibilidades de manejo sean infinitas, incluso emitiéndolos desde computadoras que no sean las nuestras y se encuentren en cualquier punto del globo.

2. La posibilidad de incluir información controlada dentro del cheque y sin límites.

3. La reducción de posibilidad de fraude.

4. La verificación automática de su contenido y validez.

5. La posibilidad de parar pagos inmediatamente (stop debit).

6. La posibilidad de controlar todos los cheques emitidos por el mismo emisor.

7. La posibilidad de controlar las fechas de todos los cheques.

8. Y otras muchas posibilidades que quedan por descubrir.

El cheque electrónico puede ser utilizado por todo tipo de emisores tanto grandes como pequeños. Eso, añadido a que provee una de las soluciones más rápidas y seguras en el mercado lo hace ideal para el mercado electrónico y también para el mercado tradicional.

Asimismo, hemos de destacar que el cheque electrónico puede ser emitido desde todo tipo de hardware y software. Aquí es donde interviene la firma digital y las soluciones de seguridad aplicadas a Internet.

Una pregunta que siempre surge es cuán seguro es un cheque electrónico. Lo cierto, es que el cheque electrónico está considerado como un instrumento de transacción de los más avanzados en cuanto a seguridad, utilizando técnicas de autenticación, criptografía de clave pública, firma digital, certificados por autoridad competente y encriptación. De esta forma Los cheques electrónicos se convierten en mecanismos de pago de los más seguros con los que cuentan hoy los Bancos.

Otra de las preguntas que surgen también es qué tiene el cheque electrónico que lo haga mejor que el cheque común. Según los expertos que están desarrollando el cheque electrónico varias son las ventajas para que el electrónico pase delante del común, entre ellas se pueden destacar las siguientes:

- mayor facilidad en las relaciones entre el emisor del cheque y la institución financiera;
- refuerzo de la seguridad del instrumento de pago;
- unificación de tecnologías que permiten un rápido y efectivos desarrollo del cheque electrónico;

Todo ello nos lleva a pensar que el cheque electrónico se ha convertido o se convertirá en lo inmediato en un mecanismo de pago de los más utilizados en el mercado.

d. **E-cash o dinero electrónico**

Entre todas las alternativas que hemos visto, quizás el dinero electrónico o el monedero electrónico son los más convenientes para el futuro del comercio electrónico. Se trata de, ni más ni menos, cambiar estos nuevos mecanismos por el dinero tal como lo

conocemos hoy.

Entre las distintas iniciativas destaca Mondex, surgida en Canadá, que es una especie de "tarjeta-monedero" inteligente impulsado, entre otros, por el Wells Fargo Bank y el Natwest Bank.

También en Europa, varios bancos y Cajas de Ahorro como La Caixa ofrecen desde hace varios años una tarjeta-monedero con la que los particulares pueden acudir a los comercios y gastar dinero sin tener que esperar que el comerciante tenga cambio.

Aunque el más representativo es Digicash, que provee un sistema que garantiza el anonimato del pagador, defendido como un derecho individual, sin perder seguridad. El usuario se conecta on-line a su banco y retira una cantidad de monedas electrónicas a cargo de su cuenta que guarda en su disco duro (un "monedero"). Este dinero digital puede utilizarlo a su gusto para realizar pagos a vendedores o individuos que acepten este tipo de transacción. Hoy, el Mark Twain Bank ya permite las operaciones con este método. La tecnología que se emplea en este caso es la de las tarjetas inteligentes o Smart Card, aunque, hasta la fecha, se ha venido considerando excesivamente complejo como para una implementación generalizada.

Veremos un desarrollo más completo del tema en el siguiente apartado.

e. **Handheld banking**

Es la mayor innovación en tecnología para bancos de los últimos años. Se trata simplemente de instalar las funciones de un banco en una palmtop, como si se tratase, en un principio, de un servicio tipo home banking.

En primer lugar, la transacción se genera en la palmtop y luego se envía -a través de un módem inalámbrico, una conexión tipo pager two-way o mediante un celular- hacia Internet, para luego atravesar un firewall o cortafuegos, que es la primera barrera de seguridad que protege las intranets bancarias. De ahí pasa a un handheld banking server que reenvía la transacción hacia el web server para pasar finalmente a la red corporativa.

La masificación de los dispositivos electrónicos que utilicen el handheld banking revolucionará la forma en que se realizan las transacciones comerciales. Las palmtops -como, por ejemplo, la Palm - tienen puertos infrarrojos que les permiten intercambiar información con otros dispositivos informáticos sin necesidad de cables. "Esto permite cosas inusuales, como la realización de

compras sin que aparezcan tarjetas de crédito ni dinero en efectivo".

Como podemos ver que se trata de un sistema muy similar a lo que sería el monedero electrónico pero en está de su contenedor sería una computadora de mano. Aunque ambos sistemas podrían coexistir perfectamente.

Ahora, vamos a ver de cerca algunas de las más importantes de estas nuevas formas de pago.

MECANISMOS DE PAGO EN DESARROLLO

CYBERCASH:

Cybercash establece un esquema de pago empleando sistemas propios de criptografía de clave pública (Secure Internet Payment Service). Se trata también de una empresa intermediaria entre el cliente y el banco.

Ofrece varios productos dentro del campo de los mecanismos de pago electrónicos:

- Tarjetas de crédito: desde abril de 1995 ofrece un sistema de comunicación directa para pago seguro con tarjeta de crédito a través de Internet mediante una interfase en lenguaje HTML. El sistema le conecta a la tienda virtual y al sistema de autorizaciones de compra con tarjetas en tiempo real. Después de la compra, Cybercash ofrece la posibilidad de controlar todos los pasos efectuados, capturándolos mediante una sencilla interfase de uso. Una de sus mayores ventajas es que el sistema de Cybercash se encuentra interconectado con la mayoría de los sistemas de pago electrónicos: First Data Corporation, Paymentech, Global Payment System, Vital, Checkfree, Wells, NOVA, NPC and Sligos (European).

- Monedero electrónico para micropagos: los micropagos, es decir aquellos que involucran montos de entre 25 centavos y 10 dólares (o sus equivalentes en otras monedas de curso oficial), son económicamente inviables en la mayoría de los casos y procesos de compra toda vez que el costo de la transmisión de la información es mayor que el del producto que se adquiere. Pero precisamente Cybercash ha desarrollado una herramienta capaz de manejar esas sumas menores, se trata de CyberCoin. Está pensada para que los comerciantes puedan ofrecer, especialmente, servicios on-line tales como "pagar para ver", compra de informes comerciales o de otras clases, compra de pequeños programas o utilidades de software, suscripciones mensuales o semanales, e incluso los denominados "pague y juegue" (juegos que se juegan desde Internet, como casinos virtuales). Este sistema además de ser adecuada para estas transacciones incluye herramientas especiales para remitir las compras de productos a los usuarios y para obtener recibos de las mismas.

- Pague ahora (PayNow(tm) Service): Se trata de un sistema de pago que une directamente las cuentas del comprador y el vendedor.

FIRST VIRTUAL BANK:

First Virtual está desarrollando desde hace años un sistema conocido como Green Commerce Model, actuando como una especie de agencia

bancaria que da un servicio de intermediario entre clientes y comerciantes. Se basa en el establecimiento de acuerdos entre las partes y el banco. Establecido el acuerdo, cada parte recibe un identificativo propio que queda ligado a una cuenta bancaria y a una dirección de correo electrónico.

Cuando un cliente quiere realizar una compra, le envía una orden al vendedor, el cual, a su vez la envía a First Virtual junto con el identificador del comprador en First Virtual. Éste se encarga de contactar al cliente por correo electrónico para confirmar que acepta el cargo.

La principal característica novedosa es la política de "satisfacción garantizada", que protege a los consumidores de los vendedores deshonestos permitiéndoles el derecho incondicional para rehusar el pago de artículos individuales. Un mecanismo estadístico se usa para identificar a aquellos que hacen un uso frecuente de este derecho y cancelar su cuenta.

Si se detecta un intento fraudulento de utilización (el cliente asegura no haber hecho el pedido que se le intenta cargar), la cuenta se cancela automáticamente, y se le abre una cuenta nueva.
Aceptada la transacción, su importe se le carga al cliente y se abona al vendedor, que ya puede hacer la entrega. El vendedor abona un porcentaje a First Virtual en concepto de comisión. Por otra parte, el vendedor no recibe el dinero hasta pasados 91 días, lo que da margen suficiente a detectar irregularidades.

NETBILL:

NetBill es un proyecto desarrollado en la Universidad Carnegie-Mellon. NetBill es un pequeño banco en el que tanto clientes como comerciantes mantienen cuentas privadas. Los clientes pueden poner dinero en su cuenta para ejecutar pagos, y los comercios pueden retirarlo.

Se basa en protocolos propios, con clientes y servidores específicos que pueden empotrarse en navegadores WWW u otro tipo de interfaces de usuario. Todas las transferencias por Internet van adecuadamente cifradas y firmadas por medio de claves públicas.

El sistema es muy adecuado para la venta de información a través de la red. Un cliente hace un pedido, y recibe el producto (la información) cifrado. Cuando lo recibe, ordena el pago que, una vez ejecutado, hace que el comerciante le entregue al comprador la clave necesaria para desencriptar la información. De esta forma se consigue ligar a ambas partes para evitar fraudes por desaparición súbita, o por pérdidas derivadas de fallos de la red o de los equipos terminales.

DIGICASH:

Se trata de dinero digital en metálico que usa un sofisticado sistema de utilización de claves y huellas digitales para ofrecer monederos electrónicas con dinero anónimo. El cliente recibe un programa específico que le permite comunicarse con un banco para retirar dinero, con otros individuos para intercambiarlo, y con comercios para realizar pagos.

Para retirar dinero del banco se utiliza una elaborada técnica criptográfica que se denomina "firma ciega". El cliente se inventa números de serie para las monedas que desea, los "ensobra" con una clave digital aleatoria que impide ver el número de serie, y los envía al banco para su autorización. El banco dispone de una serie de firmas, una por cada valor monetario. El banco firma la moneda ensobrada del cliente y se la devuelve a éste.
El cliente es capaz de eliminar la clave digital que ocultaba el número de serie sin alterar la firma del banco. En este momento dispone de una moneda validada por el banco cuyo número de serie sólo conoce el cliente. El banco detrae la cantidad de la cuenta; pero como ignora el número de serie de las monedas electrónicas, le será imposible asociar un pago observado a un cliente concreto.

El cliente puede enviar sus monedas a un comercio, que negociará con el banco su cobro. El banco sólo tiene que saber que la moneda es válida y que no se utiliza más de una vez. Para ello basta que lleve una base de datos de números de serie consumidos.

El cliente y el comercio reciben programas específicos que se comunican entre ellos o con un banco previamente acordado para utilizar unos protocolos de propietario. Se trata de un sistema cerrado. Lo que reciben las partes se asemeja enormemente a un monedero electrónico que debe ser cuidadosamente protegido frente a robos o intrusos telemáticos. Pero nótese que ante un robo el cliente puede informar inmediatamente al banco de los números de serie robados y anularlos. Una aplicación real es el Mark Twain Bank, que usa dólares USA.

PROTOCOLO SET DE VISA, MICROSOFT Y MASTERCARD:

Este es un sistema que autentica a todas las partes comprendidas en una determinada transacción electrónica por medio de "digital certificate" haciendo seguras las operaciones y agregando beneficios secundarios a las partes y al fisco. Consumidores y negocios tendrán que invertir tiempo y dinero en aprender lo mas rápido posible el nuevo modelo de comerciar.

VISA, en colaboración con Microsoft y MasterCard, ha desarrollado una especificación completa, la Secure Electronic Transactions (SET), basada en el uso de claves públicas, respondiendo a los siguientes requisitos comerciales:

- Respetar la confidencialidad de las transacciones, utilizando criptografía.
- Asegurar la integridad de los datos intercambiados, por medio de firmas digitales.
- Autentificar al propietario de la tarjeta, por medio de firmas digitales y certificados notariales.
- Autentificar al comercio, también por medio de firmas digitales y certificados notariales.
- Poner que la especificación en el dominio público, de forma que puedan desarrollarse productos clientes y servidores y ser todos ellos capaces de interoperar entre sí.

SET utiliza el concepto de "doble firma", que se usa para ligar los datos del pedido (que sólo interesan al comercio) con los datos financieros (que sólo interesan al banco). El cliente, que dispone de ambas informaciones, calcula sus huellas digitales, las concatena y firma digitalmente. El comercio recibe el pedido (del que él mismo puede extraer la huella) y la huella de lo que se envía al banco (difícilmente falsificable). El banco recibe, de forma similar, los datos bancarios y la huella del pedido. Así, cada receptor puede comprobar la firma del conjunto, respetándose al tiempo la confidencialidad de los datos, su integridad y la coherencia entre el pedido y el pago.

Respecto de los credenciales que autentican las claves públicas, SET propone una jerarquía de autorizaciones. En el primer nivel existe una autoridad del sector, A, debidamente acreditada. A acredita al banco del comprador, BE, y al banco del vendedor, BC. Cada banco acredita a sus respectivos clientes. Con esta delegación en cascada, cualquiera de las partes puede asegurarse la identidad de las demás. La autoridad A emite certificados al público, ligando una clave pública a un número de tarjeta y a una cuenta en un banco. Cuidadosamente se evita introducir el nombre del usuario para mantener su anonimato, quedando solamente ligada la huella digital de la cuenta de cargo.

TARJETA INTELIGENTE DE MASTERCARD:

MasterCard al margen de su participación en el proyecto con IBM y Microsoft, patrocinó protocolos de pago basados en los protocolos de IBM. Estos protocolos se plasman en una especificación conocida como Secure Electronic Payment Protocol (SEPP), y ha sido desarrollados en asociación con IBM, Netscape, CyberCash y GTE Corp. El mecanismo se basa en el uso de claves públicas.

Cabe destacar de esta propuesta el cuidadoso tratamiento de la emisión de certificados para autentificar claves públicas. La autoridad de certificación (CA) es única, y es la propia MasterCard. Esta autoridad emite certificados para los clientes, haciéndoselo saber al banco emisor. Los bancos que tratan con comercios reciben sus certificados directamente de la misma CA. Los comercios deben solicitar sus certificados al banco en el que poseen sus cuentas, el cual traslada la petición (junto con su asunción de responsabilidad) a MasterCard para que emita el certificado al comercio.

MasterCard entra en la red interbancaria, que se utilizará internamente para requerir y difundir certificados, además de su uso tradicional como vehículo de compensación.

SEPP prevé transacciones en línea con autorización inmediata del cargo, y transacciones diferidas (off-line) en las que utiliza correo electrónico. Además, el cliente puede recabar posteriormente el estado de su orden de compra.

MONDEX:

Mondex es propiamente dicho dinero electrónico, no es ni una tarjeta de crédito ni una tarjeta de débito. El corazón del sistema implementado por esta compañía es una tarjeta inteligente que se parece mucho a las tarjetas de pulsos telefónicos que incorporan un pequeño chip. En ese chip se almacenan en la memoria tanto el dinero que se desea llevar en el bolsillo como los programas de seguridad que protegen su contenido y hacen que las transacciones sean totalmente seguras.

El dinero electrónico Mondex se transfiere directamente al vendedor cuando se retira el producto adquirido, sin tener que acudir a una transacción en línea o una costosa operación de verificación y autenticación.

El origen de esta moneda electrónica se sitúa en el año 1990 cuando Tim Jones y Graham Higgins del Wesminster Bank y Groupe Natwest inventan el concepto de Mondex. Inmediatamente de presentada la idea, en tan sólo seis semanas, el Natwest asigna un presupuesto para el desarrollo de este nuevo concepto tan revolucionario.

Desde ese momento Mondex no ha parado de crecer en todos los países del mundo a pesar de otras iniciativas que representan algunas mejoras o avances respecto de la misma. En 1996 la corporación Master Card Internacional anunció la decisión de comprar el paquete mayoritario de Mondex y adaptar su tecnología como base del lanzamiento de sus aplicaciones de tarjeta inteligente para el futuro.

Sin embargo, no todo han sido resultados con esta clase de dinero electrónico. Han surgido algunos problemas en la práctica:

- Con Mondex, a pesar de regalar una pequeña cantidad de dinero para la carga inicial de la tarjeta, y tener habilitados todo tipo de comercios como taxis, parquímetros, y teléfonos, entre otros, el público en general no ha aceptado el producto.

- los consumidores ya están acostumbrados a pagar con sus tarjetas de crédito, débito y con efectivo.

- La nueva tecnología no provee ninguna ventaja adicional al consumidor, y esto ha sido mencionado por muchos de los usuarios iniciales como la principal causa para dejar de usar la tarjeta.

Una nueva prueba en Burger King en Nueva York con Mondex trata de combinar la aplicación de efectivo virtual y la de lealtad al acumular puntos para mercancía en la tarjeta. Como dicen los expertos, el "killer application" para tarjetas de efectivo virtual todavía no ha sido encontrado, y hasta que esto ocurra, los consumidores no tendrán una razón de peso para obtener una tarjeta de monedero electrónico. Mondex tiene en la actualidad algo más de un millón de tarjetas emitidas.

La tarjeta Mondex tiene serios competidores en el mundo, especialmente aquellos que cuentan con mercados regionales que se han impuesto sobre las iniciativas globales o mundiales: por ejemplo, con 21 millones de tarjetas en circulación, el producto belga Proton es el sistema con más tarjetas del mundo. Le siguen Visa Cash con 16 millones y el sistema Holandés Chipper con 2 millones de tarjetas. Además, varios bancos mexicanos, incluyendo Bancomer y Banamex, anunciaron su intención de emitir un monedero electrónico local utilizando el sistema Proton. Visa Cash está es proceso de pruebas en Colombia, Argentina y Brasil actualmente. Por su parte, Mondex ha anunciado la emisión de tarjetas en Costa Rica.

PRIMER CHEQUE ELECTRÓNICO EMITIDO

En la primera transacción dentro de un programa piloto con cheques electrónicos, el Ministerio de Hacienda de los Estados Unidos y un grupo de empresas bancarias y de tecnología informaron que un e-check por valor de u$s 32.000 fue enviado vía mail desde las arcas del ministerio a GTE como pago por un contrato de la Fuerza Aérea.

Dos bancos, BankBoston y NationsBank se ocuparon del pago, el cual será procesado a través de la Reserva Federal del Banco de Boston. Mientras un vocero de Hacienda calificó a los e-checks como "la tecnología más importante surgida en los últimos tiempos que

reemplazará el trabajo con papeles hacia el año 2002", Mark Greene, ejecutivo de IBM -empresa que provee la tecnología a los bancos-, declaró que "esta es la corriente hacia donde se dirige el comercio electrónico".

El programa piloto es auspiciado por el Consorcio Tecnológico de Servicios Financieros, un grupo integrado por instituciones, proveedores de servicios técnicos, equipos de investigación y agencias de gobierno norteamericanas, y se tardó alrededor de dos años para desarrollar este sistema que permite realizar transacciones con cheques electrónicos.

En poco tiempo, se prevé que este mismo sistema lo desarrollen en todas las redes financieras de ese país y convierta en uno de los mecanismos de pago más utilizados por su seguridad, rapidez y confiabilidad.

LA NECESIDAD DE INTEROPERABILIDAD

Todos estos nuevos sistemas o mecanismos de pago encuentran un serio problema cuando tienen que entrar en el mercado: no son compatibles entre ellos y, por lo tanto, la utilización de unos o el hecho de que los vendedores adopten un método, hace que queden excluidos todos los demás. En todo caso podría adquirir todos y cada uno de los sistemas que están en desarrollo en la actualidad lo que, por el momento, es antieconómico y poco práctico.

Pensemos, por un momento, en la realidad: los negocios hoy en día funcionan con métodos de pago casi unificado. Tenemos, por un lado, las tarjetas de crédito y, por otro, el dinero físico. Para que el dinero electrónico y cualquiera de los mecanismos que se están desarrollando puedan funcionar y ser competitivos, tienen que ofrecer mayores ventajas que los mecanismos convencionales que se utilizan hoy y, por lo tanto, no entrañar mayor dispersión.

Es por ello que aparece el concepto de INTEROPERABILIDAD: es decir, la necesidad de que los mecanismos que se creen en el futuro puedan funcionar simultáneamente y sin requisitos particulares que no sean comunes a todos ellos. Pensamos que, tarde o temprano, está interoperabilidad va a llegar por sí sola, ya que de otro modo los mecanismos de pago no van a funcionar y no van a ser atractivos para los consumidores y las instituciones financieras, y menos aún para el mercado general. El protocolo SET es uno de los esfuerzos más importantes a nivel mundial ya que combina varias de las empresas más grande del mundo en cuanto a desarrollo de productos informáticos.

En las diferentes partes del mundo existe gran diferencia en cuanto al momento en que los medios electrónicos de pago van a sustituir al

dinero en poco tiempo. En Argentina todavía no hay una conciencia clara que los bancos y las personas particulares van a sustituir los medios tradicionales de pago por estos nuevos mecanismos.

En un discurso reciente en Seattle, Bill Gates, dijo que la clave para el futuro del comercio en la Internet es saber quien se comunica con quien. Gates predijo que las tarjetas inteligentes con certificados digitales se convertirán en algo tan común como las tarjetas de cajeros hoy en día. Sugirió no esperar por tarjetas con sistemas operativos de 16 o 32 bit (que complica más la operatoria), sino establecer un estándar común de encriptación simple con llaves públicas en tarjetas de sistemas de 8 bits. Según él, estas tarjetas costarán menos de $1 en un futuro cercano. "La clave es que las tarjetas tengan aplicaciones simples y que no traten de hacer demasiado por ahora".

EL DINERO Y SUS SUSTITUTOS

En la Edad Moderna el incremento de las transacciones, da lugar a la aparición del dinero-papel, que se acepta como pago de un bien. La evolución de estos pagarés nominales a pagarés al portador, hace crecer la masa monetaria en circulación y originan el nacimiento de los billetes, sencillos trozos de papel equivalentes a certificados de depósitos de objetos, o valores a los que, cualquiera que los posea, puede acceder. Con la moneda surgieron los establecimientos que, más o menos, realizaban los mismos servicios que los bancos actuales.

Los talones o cheques, más tarde, sustituyeron a los billetes, en aquellos casos en que estaban en juego o debían trasladarse cuantías elevadas. Si damos un gran salto, podemos apreciar que la celeridad de la vida moderna, y las perfecciones tecnológicas han generalizado el uso de las transacciones electrónicas. Las transferencias y las domiciliaciones bancarias se han hecho habituales. La comodidad y la seguridad, han masificado el uso de las tarjetas de crédito. Simples plásticos, que a través de una banda magnética, registran nuestros datos y los trasladan ‘informáticamente’ a la base central donde consta si existen fondos o crédito, para que podamos pagar con ella. El restaurante, la estación de servicio, o el supermercado, el hombre de hoy, es frecuente que lo abone con tarjeta .

Incluso se da un fenómeno regional, en la Unión Europea, de realizar el objetivo de la llamada moneda única, con un previo periodo de rodaje en el que las monedas nacionales coexistirán con esa moneda única (el cronograma europeo diseñado establece que el 1 de enero del 2002, se estrenará la moneda única en su forma física y comenzarán a retirarse las monedas nacionales; en julio de ese mismo año, sólo existirá el Euro, con una política monetaria y cambiaria única).

Estos cambios que se han ido produciendo a lo largo de la historia y que hemos resumido de forma extremadamente condensada, nos hacen pensar que es probable que las monedas y los billetes, tal como los conocemos y utilizamos hoy, queden superados por instrumentos de pago basados en la tecnología. Sin embargo, pensamos que no crearán hábitos y comportamientos diferentes de los que tienen las personas en cuanto a los pagos que deben realizar.
Pero ¿qué es el dinero?

Quizás la mejor definición que podemos dar estos días al dinero es que es un medio de pago cuyo principal (si no único) fundamento es la confianza de que los demás lo aceptan como medio de pago, es decir, que mediante su entrega a terceros que tienen cosas que no son dinero, éstas pueden ser adquiridas en propiedad.

En la conciencia común se identifica dinero con una especie del mismo: el dinero legal, que, como definen Francisco Mochón y Víctor Beker , es el que es emitido por una institución que monopoliza su emisión y que adopta la forma de monedas metálicas y billetes. Este es el dinero en efectivo, los pesos, las pesetas, los dólares, los francos, las liras, las libras o los escudos.

Cuando un particular toma su dinero y lo ingresa en una institución bancaria para que lo mantenga depositado hasta tanto lo necesite el titular, el dinero pasa a estar en manos de un tercero (el banco) que lo tiene y tiene la capacidad de operar con él siempre que le garantice el retorne a su dueño. Dado que esa persona tiene la posibilidad de utilizar todo o parte de la suma depositada, el Banco debe mantener un mínimo de dinero efectivo a su disposición. Ese mínimo que todos los bancos deben respetar se denomina coeficiente de reserva (y en algunas países coeficiente de liquidez).

Supone que el resto del dinero que no está obligado a mantener como efectivo puede ser operado para emprender nuevos negocios, facilitar operaciones de compra y venta, conceder hipotecas, etc, en definitiva puede ser prestado. Aquí es donde nace el concepto de dinero bancario, en la posibilidad de que el dinero efectivo pueda generar otro tipo de dinero que, simplificando, podríamos decir que es impalpable.

El negocio de las instituciones bancarias se centra, en términos generales, en esta posibilidad que, por cierto, se encuentra restringida. Keynes al observar y analizar la práctica bancaria señaló que no todo el dinero creado por los bancos se utiliza al mismo tiempo, por lo cual no es necesario establecer una reserva en efectivo equivalente al total de depósitos, sino una proporción , "...lo que colocará un límite a las posibilidades de los bancos a crear dinero bancario" (Keynes j. 1971). También Keynes, en sus análisis en los años veinte sobre países desarrollados como Inglaterra y Estados Unidos, expresa que el dinero

bancario "...constituye quizás las nueve décimas partes del total del dinero circulante y en el sentido de que el dinero estatal ocupe una posición claramente subsidiaria" (Keynes j., 1971)., con lo cual el dinero bancario había llegado a ser dominante, lo que representa una etapa de evolución en la que se daba, mayormente, a circulación de cheques y otros títulos en lugar de efectivo.

¿ Estamos hoy a las puertas de un nuevo paso en la evolución de los sistemas monetarios ? Si el dinero bancario, como ya sucedió en los países desarrollados en determinada época, prevalece sobre el dinero efectivo o líquido (usamos estas expresiones de manera indistinta y con el mismo significado), y si la utilización de medios tecnológicos cada vez más seguros, prácticos y manejables impregna todos y cada uno de los ámbitos de nuestra vida, ¿ no sería una consecuencia bastante verosímil que los medios de pago tecnológicos se desarrollaran casi ilimitadamente en este campo en el que encuentran unas posibilidades excepcionales ?

EL DINERO ELECTRÓNICO

Como ya hemos visto en un apartado anterior, el dinero electrónico o dinero digital se puede conceptuar de dos formas: una sería el dinero electrónico que circula por la red de bancos, por ejemplo, y otra sería el dinero electrónico que podemos transportar en monederos electrónicos. Se trata, en uno y otro caso, del mismo dinero electrónico pero en contenedores diferentes.

El dinero electrónico no es otra cosa que bytes por paquetes de información que circulan a través de las redes de información como Internet. Antes hemos hablado de dinero bancario que es muy parecido al dinero electrónico ya que se basa en la confianza de las personas que lo utilizan para existir. Si no existiera esa confianza en que el dinero bancario puede funcionar sin existir físicamente, entonces el dinero electrónico tampoco podría existir. Es por ello, que, con el advenimiento de nuevas tecnologías como Internet, con las que la gente puede establecer relaciones mucho más próximas con los nuevos desarrollos de la tecnología, pensamos que se está creando el mejor campo donde cultivar la confianza de todo el mundo en esos mecanismos de pago nuevos y en el dinero electrónico.

Es importante, y contribuye a todo lo que estamos diciendo, que las características fundamentales del dinero, tal como lo conocemos hoy, se presenten también en sus nuevas modalidades, es decir:

- deberá ser aceptado comúnmente como medio de cambio, y no ser susceptible de venta como un bien, un producto o una mercancía.

- deberá ser dado y aceptado como pago final de una deuda: es decir, tiene que tener poder cancelatorio de las deudas.
- podrá trasladarse y transmitirse libremente mediante su entrega (Aquí los abogados y semiólogos tendrán trabajo extra para definir lo que debe entenderse por entrega, sobre todo si intervienen medios electrónicos de transmisión).
- deberá tener valor por sí mismo, sin necesidad de acudir a otros respaldos que lo completen o impongan de determinadas cualidades.
- deberá, como consecuencia del anterior parámetro, estar libre de cualquier reclamo posterior a su entrega (como actualmente lo es cualquier medio de pago).

Estas características necesarias deben permitir la difusión del dinero electrónico cualquiera sea la forma en la que se lo presente.

Estas características se pueden resumir en estos puntos que vamos a desarrollar a continuación. Sin ellas, el dinero electrónico no tiene posibilidades de salir adelante ya que conforman la mayoría de elementos necesarios para que el dinero electrónico tome el impulso definitivo que necesita.

Anonimato

Consiste en que no se sepa quien es el usuario o entidad que realiza la transacción. En el mundo real, el dinero en metálico (cash) es difícilmente rastreable. No tiene propietario, o más bien, no es nominativo (como antiguamente lo eran las acciones). Sin embargo, las transacciones a través de la red dejan trazas en forma de múltiples logs y registros. La falta de anonimato tiene un efecto psicológico importante sobre el comprador, que puede inhibir la realización de transacciones, sobre todo en adquisiciones relacionados con temas escabrosos o con aquellas que requieren específicamente anonimato (un ejemplo podría ser la adquisición de acciones de una compañía).

Trazabilidad

Sin embargo, el anonimato, tan deseable en muchos aspectos, choca con aquellos que desean o incluso necesitan la trazabilidad de las transacciones. Es fácil darse cuenta de que la policía y el poder judicial, así como los servicios secretos y las autoridades tributarias son los principales reclamantes de estas características de trazabilidad (pero, a veces, también los bancos o las compañías de tarjetas de crédito). Es necesario que exista la trazabilidad toda vez que, por seguridad en las transacciones, es bueno que una autoridad de control pueda efectivamente controlar, en los casos sobre los que tenga competencia, las operaciones efectuadas a través de las redes. Hoy en día eso mismo

ocurre, por ejemplo, con las llamadas telefónicas efectuadas desde teléfonos celulares Las que pueden ser rastreadas y registradas perfectamente.

Confidencialidad

Aunque en cierto modo similar, la confidencialidad no es lo mismo que el anonimato. Consiste en la protección contra la revelación, ya sea accidental o deliberada, de los datos de una transacción. Podríamos decir que se trata de una parte o elemento del anonimato.
Aunque se proporcione anonimato, la falta de confidencialidad permite la identificación de patrones de compra que podrían ser utilizados por partes a las que no se ha prohibido expresamente su utilización. En América se han dado muchos casos de personas que han exigido la confidencialidad de sus transacciones para luego no recibir publicidad vía Internet.

Autenticación

La autenticación tiene dos vertientes: la del cliente, y la del vendedor. De modo análogo al caso real, el cliente (salvo en el caso del pago en efectivo, electrónico en este caso), debe identificarse de forma que sea posible para el vendedor poder reclamar en el caso de que el pago no se realice de forma correcta o no se haga.

Del mismo modo, el comprador debe conocer la identidad del vendedor, toda vez que el producto no se entrega de modo inmediato (esto es cierto solamente en el caso de la venta de productos, y no en el de información). Sería enormemente sencillo montar comercios electrónicos falsos con la única intención de obtener, por ejemplo, los datos de las tarjetas de crédito de los posibles clientes.

En transacciones a través de Internet, lo más fácil sería que comprador y vendedor acudan a una tercera parte de confianza, conocida como autoridad de certificación (Certification Authority, CA) para garantizar la autenticación. Los sistemas de seguridad son múltiples y únicamente haremos un breve repaso de los mismos al final de este capítulo. Basta decir, por el momento, que en la Argentina ya existen autoridades de certificación, la más conocidas de las cuales es la Comisión Nacional De Valores.

Integridad de los datos

Consiste en que no sea posible la modificación, ya sea por alguna de las partes participantes, o por terceras partes, de los datos de la transacción. Se trata de prevenir el fraude por parte de cualquiera de ellas. Este fraude puede aparecer por modificación de la composición del

pedido, del monto de los pagos, del número de tarjeta de crédito o cuenta bancaria, del receptor del pedido, etc.
Como es sabido existen bancos de datos comerciales que venden sus datos a través de Internet o de correo electrónico. Imaginen por un momento que esos datos referentes a una empresa o a una persona puedan ser modificados y transferidos a su destinatario sin que éste se de cuenta. La consecuencia de este caso podría ser que se efectúe una inversión en una empresa que pudiera estar quebrada o se otorgue un préstamo a una persona con antecedentes económicamente poco viables.

No repudiación (irrenunciabilidad)

Íntimamente ligado con la característica anterior, se encuentra la cuestión de la irrenunciabilidad. Es necesario que nadie pueda desdecirse, y para ello tiene que haber una autoridad o autoridades ampliamente reconocidas que puedan probar la participación de cualquiera de las partes en la transacción. Este es un tema que los abogados tendrán que estudiar en el futuro en profundidad.

Puede ser de dos tipos:

- con prueba de origen: cuando el destinatario tiene prueba del origen de los datos.

- con prueba de entrega: cuando el origen tiene una prueba de la entrega íntegra de los datos al destinatario deseado.

Fiabilidad

Las transacciones de pago deben ser únicas, es decir, deben suceder en su totalidad o no suceder en absoluto, pero no deber quedar en un estado desconocido o inconsistente. Ningún comprador aceptaría perder dinero debido a una caída de la red o de la máquina del vendedor y precisamente los casos en que se caiga la red deben ser tenidos en cuenta por cualquier soporte sea desarrollado para estas transacciones. La recuperación de estas caídas requiere alguna clase de almacenamiento estable en todos los actores de la transacción y la existencia de protocolos de resincronización específicos.

Requerimientos no específicamente de seguridad

Además de los requerimientos enfocados a hacer seguras las transacciones, existen otros adicionales encaminados a hacer más eficaces los mecanismos:

- bajo costo.

- independencia del hardware y de sistemas operativos.

- mecanismos efectivos de ‘auditar’.

- confianza por parte del consumidor.

Todos ellos están siendo desarrollados dentro de cada uno de los programas referentes a mecanismos de pago electrónicos, sin embargo falta mucho camino por recorrer y solamente si los agentes que vayan a utilizar estos mecanismos están seguros de que se cumplen todos estos requisitos, éstos podrán funcionar correctamente con características de cotidianidad.

Es de señalar que El Banco Central Europeo publicó un informe a finales del año 1998 sobre dinero electrónico en el que analiza los riesgos asociados a un medio de pago que va a ser uno de los fundamentos del comercio electrónico dirigido al consumo y con el que se pretende solucionar, entre otros, el problema de los micropagos.

El estudio se dirige a los sistemas de dinero electrónico basados en tarjetas de prepago (es decir, aquellas que incorporan dinero electrónico en un chip inteligente) o en software específico, desarrollado para realizar pagos a través de una red de telecomunicaciones como Internet.

Entre las conclusiones del informe, destacan las siguientes:

1. La emisión de dinero electrónico tendrá una importante incidencia en la política monetaria y obligará a asegurar la estabilidad de los precios y la función del dinero como unidad de cuenta.

2. Deberá analizarse la necesidad de desarrollar nuevas normas que garanticen:

    - El funcionamiento eficaz de los sistemas de pago
    - La confidencialidad de las transacciones
    - La protección de los consumidores y de los comerciantes
    - La estabilidad de los mercados financieros
    - La protección frente a delitos

3. También deberán establecerse los requisitos que deberá cumplir la emisión de dinero electrónico y en especial:

    - Supervisión sometida a criterios de prudencia.
    - Normativa sólida y transparente
    - Seguridad técnica que impida manipulaciones y falsificaciones
    - Protección frente a delitos, especialmente el lavado de dinero

- Suministro de la información necesaria para generar estadísticas monetarias
- Garantía de conversión del dinero electrónico en moneda del banco central a requerimiento del poseedor del dinero electrónico.
- Coeficiente de caja que obligue a los emisores de dinero electrónico a mantener unas reservas apropiadas.

4. Será necesario incrementar la cooperación entre las autoridades de supervisión de los países implicados para evaluar la integridad de los sistemas de dinero electrónico, en especial, en las operaciones transfronterizas.

5. Otro objetivo importante a perseguir es la interoperabilidad de los diferentes sistemas de dinero electrónico.

6. Finalmente, el BCE recomienda, inicialmente, limitar la emisión de dinero electrónico a las entidades de crédito, tal como las define el artículo 1 de la primera Directiva sobre coordinación bancaria. Todo ello sin perjuicio de que en el futuro, dicha definición sea modificada para dar cabida a las entidades que emiten dinero electrónico y que no son entidades de crédito.

El BCE aceptaría la existencia de un periodo transitorio durante el cual las entidades que actualmente están emitiendo dinero electrónico puedan seguir haciéndolo si cumplen los requisitos propuestos, con excepción del coeficiente de caja.

Finalmente queremos hacer un breve repaso a los sistemas de seguridad que hemos mencionado anteriormente. Es importante tener en cuenta que el desarrollo de estos sistemas es lo que va a permitir que todos los temas que se encuentran entorno al comercio electrónico van a encontrar la mayoría de las respuestas a sus dolores de cabeza en los sistemas denominados criptográficos y que el objetivo de la criptografía no es otro que el de proporcionar comunicaciones seguras (y secretas) sobre canales inseguros.

Ahora bien, la criptografía no es sinónimo de seguridad. No es más que una herramienta que es utilizada de forma integrada por mecanismos de complejidad variable para proporcionar no solamente servicios de seguridad, sino también de confidencialidad.

Sucintamente, exponemos a continuación algunos de los mecanismos de seguridad que se emplean tanto para el desarrollo de sistemas de pago como en el propio comercio a través de las redes públicas como Internet:

Claves simétricas (secretas o únicas)

Se trata del mecanismo clásico. Estas técnicas usan una clave que es conocida por el remitente de los mensajes y por el receptor, y con la que cifran y descifran respectivamente el mensaje. Para mantener la seguridad del cifrado, deben mantener esta clave en secreto. Su fuerza reviste en que además de seguridad ofrecen rapidez en las transacciones.

El principal inconveniente estriba en la necesidad de que todas las partes conozcan la clave para cifrar y descifrar, lo que lleva a problemas en la distribución de las claves. Esta debilidad ha hecho que sea poco utilizada en los mecanismos desarrollados hasta el momento para permitir el pago, a no ser que vaya combinada con otro tipo de técnicas.

El sistema de cifrado más extendido es Data Encryption Standard (DES), desarrollado por IBM y adoptado por las oficinas gubernamentales estadounidenses para protección de datos desde 1977.

Claves públicas

Estas técnicas se basan en la existencia de parejas de claves, una secreta, conocida únicamente por su propietario, y una pública, libremente distribuida por su propietario o por una agencia de certificación en toda la red (Es lo que ocurre en Argentina con La Comisión Nacional De Valores).

El conocimiento de una de las claves no permite averiguar la otra. Un mensaje es cifrado con una de las claves y descifrado con la otra, y exclusivamente con la otra. Los algoritmos de cifrado que utilizan estas claves son usualmente muy lentos, por lo que no se suelen utilizar para cifrar datos.

Uno de los primeros esquemas de clave pública fue desarrollado por R. Rivest, A. Shamir y L. Adleman en el MIT. El esquema Rivest-Shamir-Adleman (RSA) ha sido desde la fecha de su publicación el único sistema ampliamente aceptado para la implementación de encriptación mediante clave pública. El principal inconveniente de este sistema es la existencia de una patente sobre este algoritmo, lo cual dificulta su uso fuera de los EE.UU. si no se ha obtenido la correspondiente licencia de exportación. Incluso, debemos señalar que la criptografía de clave pública de 128 bits, que es la que incorpora el Internet Explorer 5, no puede adquirirse fuera de EEUU o Canadá ya que se ha considerado como un arma de guerra por la potencia de su sistema de cifrado.

Códigos de integridad

A menudo es poco práctico la aplicación de técnicas de encripción a un mensaje entero. En tal caso, se utilizan funciones matemáticas que, a partir de un cierto volumen de datos, derivan una pequeña serie de datos, o huella digital.
Si se manipulan los datos, la huella cambia y el intento de modificar los datos de forma tan sabia como para obtener la misma huella es algo que en computación se considera prácticamente imposible.

Firmas digitales

Dado un mensaje, se imprime su huella digital y se cifra dicha huella con la clave privada del remitente. El receptor procede a descifrar la huella con la clave pública del remitente. De esta forma obtenemos simultáneamente la seguridad de que el contenido no se manipula (integridad), y de que el firmante es quien dice ser (autenticación).

En estos momentos varias empresas argentinas están participando en un proyecto de firma digital en el que dichas empresas remitirán a la Comisión Nacional De Valores sus estados contables firmados digitalmente. Dichos estados contables se considerarán absolutamente válidos toda vez que La Comisión Nacional De Valores dará validez a los documentos enviados con la firma digital de las empresas que previamente habrán obtenido esa firma digital en la autoridad de aplicación.

Certificados

El principal inconveniente del uso de claves pública es el modo de asociación de los pares de claves (pública-privada) con personas físicas. La solución la aportan las autoridades de certificación (notarios electrónicos) que son entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, rubricando con su firma su identidad.

Kerberos

Kerberos es un sistema de autenticación diseñado en el MIT, con dos propósitos: proveer autenticación y distribuir claves. El sistema Kerberos actúa como autoridad de certificación que garantiza una relación correcta entre claves y usuarios o entidades.

Las principales debilidades de este sistema son, la autenticación del propio servidor Kerberos y que añaden un costo adicional a cualquier transacción.

PGP (Pretty Good Privacy)

PGP es un sistema completo que proporciona integridad y autenticación para el correo electrónico y aplicaciones de almacenamiento de archivos. Fue desarrollado en 1991 por Phill Zimmermann y está compuesto por bloques que, secuencialmente, van transformando el mensaje: firma digital, encriptación del mensaje, compresión, compatibilización con correo electrónico y segmentación. En la recepción se realiza el proceso contrario.

Una vez que hemos visto tanto los requerimientos como los elementos de seguridad que forman parte del dinero electrónico, vamos a ver las ventajas y desventajas del mismo.

DESVENTAJAS Y VENTAJAS

Desventajas

a. El ordenamiento jurídico:

El alcance de las operaciones comerciales o económicas efectuadas a través de medios telemáticos va más allá de las fronteras reales y el derecho todavía está reaccionando. La creación de redes internacionales de conexión trasciende las normas internas y también las internacionales, que por el momento son extremadamente escasas en ambos niveles.

El impacto del dinero electrónico sobre los sistemas monetarios no se conoce y los problemas que se están conociendo derivados de ese cruce inmune de fronteras sin regulación no encuentran respuesta por parte de los legisladores de los distintos países.

Tímidamente, países cuya creación de tecnología les otorga ventajas competitivas en el mercado internacional (EEUU, Japón, Francia, etc) han desarrollado leyes ad hoc para proteger sus creaciones.
Sin embargo, las complicaciones a raíz de un negocio efectuado a través de Internet son múltiples para los ordenamientos jurídicos.

b. Desconocimiento:

Las diferentes operaciones que se desarrollan mediante el uso del dinero electrónico son más revolucionarias que la propia idea del dinero electrónico y sus posibilidades encuentran limitaciones prácticamente inexistentes. Las instituciones nacionales e internacionales tratan de realizar un control (aunque sea de conocimiento) para no quedar a merced de operadores o especuladores financieros.

Si se desconocen los capitales llamados golondrina harán que el uso de sistemas de dinero electrónico puede permitir mover los capitales que son totalmente especulativos puedan actuar generando efectos en países en desarrollo que podrían echar abajo toda una economía.

c. Transición:

El movimiento de transferencia de la confianza de los usuarios a los sistemas avanzados basados en tecnología puede no ser tan rápido como la evolución de las modalidades de pago y de dinero electrónico que van apareciendo, creándose, en consecuencia, un desfasaje entre la realidad cotidiana y la que se va creando conforme van evolucionando los distintos productos monetarios. Ello llevaría, quizás, a la crisis de sectores financieros que hayan efectuado cuantiosas inversiones en adelantos.

Es por ello que tiene una importancia enorme que los institutos financieros, los gobiernos y las instituciones privadas fomenten la información sobre la existencia del dinero electrónico y todos estos nuevos mecanismos que hemos visto entre el público.

d. Seguridad:

Uno de los problemas fundamentales de esta tecnología viene dado por la seguridad de las transacciones comerciales y de las transferencias electrónicas de fondos, es decir por la búsqueda de anonimato o de confidencialidad de los datos, no tanto por la seguridad de las transacciones en sí mismas.

Es un pensamiento generalizado que los sistemas de control y de seguridad tienen mucho trabajo que realizar para asegurar estar nueva forma de intercambio. Sin embargo, ello tiene poco que ver con la fortaleza y confianza en el propio dinero electrónico. También la evolución tecnológica contribuye al desarrollo de los mecanismos de seguridad y el estar implementados sobre datos y procesos digitales se adapta perfectamente a los nuevos procedimientos.

Quizás la mayor preocupación de las partes involucradas - puesta de manifiesto en las I Jornadas Internacionales de Criminalidad Informática de la Argentina (Septiembre de 1997) - es que se encuentran frente a un tipo de delitos ejecutados con medios distintos a los tradicionales (robo de dinero a través de la toma de conocimiento ilegal de cuentas y claves de seguridad transmitidas en operaciones lícitas que son "pinchadas"). Ocurre, sin embargo, que se hacen necesarios conocimientos sofisticados de la tecnología que hacen mucho más esporádicos los ataques al sistema y facilitan la identificación del origen de los mismos. Hoy en día los sistemas policiales del mundo están en contacto permanente formándose sobre las nuevas modalidades de

ataque a los sistemas e identificando una forma mucho más precisa a los criminales cibernéticos ya que éstos son personas con una educación en sistemas muy avanzada. Ello facilita enormemente su identificación y permite conocer los perfiles el criminal moderno.

e. Diferencias:

La expansión nacional y también transfronteriza del comercio y del dinero electrónico no puede ignorar algunos inconvenientes de organización, operación y control. Como menciona Iván Laguado en su artículo Comercio y Dinero Electrónico: Dos realidades en Tecnología, la eficiencia de una sociedad está ligada a la competitividad de sus estructuras; sin una adecuada velocidad de adopción de medios tecnológicos el retraso es cada vez mayor frente a quienes sí lo hacen; es como la diferencia entre una fábrica que produce un auto en un mes y la que puede hacerlo en cinco días (el retraso aumenta con cada día).

Ventajas

Si bien aparecen algunas desventajas que vienen dadas, especialmente, por el desconocimiento que se tiene del funcionamiento general y específico de los pagos e intercambios electrónicos, no se puede negar que la utilización de este tipo de tecnología aplicada sobretodo a medios de pago incorpora ventajas sobresalientes:

a. Disponibilidad:

El dinero electrónico está disponible las veinticuatro horas del día, los siete días a la semana, los trescientos sesenta y cinco días del año. Las redes informatizadas de comunicación no tienen horarios (es uno de los fenómenos más globalizadores que existen), ni días de fiesta o de descanso, ni están cerradas por horario de almuerzo, y lo más importante, llegan hasta la persona misma en cualquier lugar en el que nos encontremos con una computadora o cualquier otro método de conexión a Internet.

b. Dinamismo:

Se utiliza para todo tipo de comercio: tanto para el minorista como para el mayorista, sin importar los montos, y en cualquier sector de la actividad económica. Además el manejo de los datos que acompaña las transferencias realizadas ocurre de una forma más cercana al público, pues se realiza de forma personalizada y el dinero tiene la misma naturaleza que la información que se transmite (son impulsos electrónicos).

c. Control:

El seguimiento de las operaciones, y su verificación, son más eficientes ya que estos medios conllevan sistemas internos de comprobación de cada uno de los pasos que se dan, de las identidades de los usuarios, de los lugares de donde sale y a donde va la transferencia, etc. Y todos estos controles, y la documentación que generan y que va construyendo la historia de cada movimiento, se hacen también electrónicamente. Las facilidades para obtener copias de respaldo, desautorizar una transacción o controlar el pago efectivo del dinero electrónicamente, conllevan toda una revolución frente a los mecanismos actuales (sobre la cual los bancos y corporaciones financieras van a tener que meditar). Cada persona va a poder controlar totalmente cualquier transacción que haya efectuado y tenerla registrada en su sistema o computadora.

d. Ahorro:

Una vez que la infraestructura para efectuar las transacciones se ha puesto en marcha, no es necesario producir papel o moneda, ni custodiarlo, ni imprimir marcas de agua, etc. Si bien existen mecanismos de seguridad en el sistema, éstos se implementan a costos mucho menores que los que requiere el sistema monetario actual.

Pensemos que la realización de marcas de agua es altamente costosa para la industria del dinero. En cambio los sistemas de seguridad aplicados en dinero electrónico, además de ser más eficaces, son más baratos.

e. Eficacia:

Si nos referimos a los monederos electrónicos, la transferencia de "efectivo" desde nuestra computadora puede llegar a tardar unos cinco segundos, y el posterior pago al comerciante que sea también dura ese "tiempo" (piénsese además que no es necesario esperar el vuelto pues se paga al centavo). No hacen falta firmas, identificaciones, respaldos legales o autorizaciones: se trata de numerario, de efectivo, en definitiva, de dinero contante y sonante que se traslada de forma inmediata.

f. Privacidad:

El uso del dinero en soporte electrónico es menos evidente frente a terceros que pueden observar la operación. Ello crea un nivel de seguridad amplio, al menos con respecto al efectivo que se maneja cotidianamente.

g. Acceso total:

La globalización se encuentra en todos los rincones de la sociedad y la moneda electrónica contribuye definitivamente a ella. Permite la posibilidad de hacer compras en cualquier país del mundo, pues el dinero electrónico puede ser automáticamente convertido a otra moneda mediante una simple transferencia.

LA DESAPARICIÓN DEL DINERO FÍSICO

Los medios de pago tradicionales irán desapareciendo conforme la posibilidad de utilizar otros que no implican su transporte físico va evolucionando.

Es necesario entender que los productos desarrollados para almacenar dinero electrónico (los ya mencionados: smart-card, digicash, e-cash, etc) son diferentes del propio concepto de dinero electrónico: son medios que registran un determinado valor ingresado por el titular de ese dinero para efectuar toda clase de transacciones hasta el agotamiento del crédito incorporado a ese medio de pago.

El dinero físico, las monedas y los billetes, es emitido por una institución (generalmente denominada Banco Central) que tiene el monopolio de emisión del mismo. Sin embargo, una vez ese dinero ingresa en cualquier entidad financiera, privada o pública, se convierte en un crédito a favor del depositante, es decir, en algo que no tiene entidad física. Y ese mismo crédito (sobre una cantidad de dinero) se utiliza, como hemos reiterado a lo largo de este análisis, diariamente a través de distintos medios de pago: tarjetas de crédito, cheques, transferencias mediante sistemas de home banking , etc.

Este dinero, junto con el dinero bancario, no se materializa prácticamente nunca puesto que circula mediante transferencias y solamente adquiere materialidad cuando el titular lo tiene que retirar de donde lo depositó para efectuar operaciones en las que, en la actualidad, todavía se requiere el uso de dinero físico.

Lo que hemos tratado de poner de manifiesto en este capítulo es que esas ocasiones que requieren el uso de dinero físico son cada vez menos frecuentes. Que los medios tecnológicos que se ponen a disposición de los usuarios, en forma de medios de pago electrónicos, tienen una gran cantidad de ventajas cualitativas que van a impulsar su implementación de una manera global.

Si bien las consecuencias de grandes cambios y modificaciones en las estructuras monetarias puede acarrear alteraciones en los sistemas macroeconómicos de cada nación (por supuesto el primer afectado sería

el sistema monetario), lo cierto es que contamos con una ventaja indiscutible: la próxima entrada en vigencia de la Moneda Única europea que va a suponer un cambio importante en el medio de pago de más de 350 millones de personas y que vamos a tener la oportunidad de estudiar.

2.2 El dinero digital: Pagos sin rastro

Introducción

En los orígenes del negocio bancario está la acumulación de los recursos financieros de los ciudadanos a cambio de ciertas contrapartidas. La más tradicional de todas ellas era la seguridad que la institución bancaria aportaba y aporta frente al robo del capital, pero pronto se consolidaron otros servicios, como la posibilidad de negociar desde sus sedes con el capital sin tener que acceder físicamente al mismo. Estos servicios ofrecen al cliente la posibilidad de efectuar pagos y realizar cobros sin tener que intercambiar dinero en efectivo; para lo que tan sólo era necesario intercambiar documentos bancarios auténticos (cheques, letras, etc.) entre los agentes.

La existencia de diferentes entidades bancarias en competencia obligó a la creación de Cámaras de Compensación donde, periódicamente, los bancos realizaban los balances de sus cuentas. Esta centralización obligaba a que los bancos hubiesen de transportar capital y documentos de un modo seguro (transportes blindados, agentes, etc.) desde sus diferentes sedes hasta dichos centros de compensación o a otras sedes bancarias.

Con el ánimo de reducir costos y así aumentar el margen comercial, las entidades bancarias fueron las primeras, en la sociedad civil, en establecer redes privadas de comunicación mediante las cuales transferían capitales y documentos sin una necesidad imperiosa y frecuente de transportar moneda y documentos. Hasta este punto, las redes eran privadas, estaban constituidas por un número no excesivo de entidades, y muchos elementos de su operación se basaban en la buena fe y la confianza mutua entre los interlocutores.

En el desarrollo natural del negocio bancario pronto se propuso extender parte de estos servicios a los clientes, para lo cual hubo que establecer redes mucho más extensas en las que el cliente privado podía realizar transacciones financieras sin necesidad de dinero en metálico y sin tener que desplazarse hasta las sedes del Banco.

En este procedimiento tan sólo se sustituye el dinero metálico por documentos bancarios privados que actuaban como órdenes de pago. Sin embargo, este proceder adolece de algunos de los problemas que conlleva transferencia de fondos en efectivo; hay que transportar de un modo seguro los documentos que dan crédito de la transacción desde el punto en el que se realiza ésta y el banco emisor de las tarjetas.

Con el éxito conseguido en este proceder, tan pronto como la tecnología lo permitió a costos razonables, las transacciones con tarjeta de crédito se convirtieron en transacciones electrónicas mediante terminales especializados repartidos por los comercios adscritos a este tipo de servicios. La seguridad de estas transacciones seguía y sigue dependiendo de los documentos escritos y firmados, pero la celeridad que se obtiene con la transferencia inmediata de la información, supone una mejor calidad de servicio para los clientes y una importante ventaja operativa para los bancos.

Con la existencia de tarjetas de crédito/débito se ha reducido considerablemente la cantidad de dinero circulante en la sociedad, por lo que, actualmente, su desaparición resultaría virtualmente imposible. En España existen unos 27 millones de tarjetas de crédito/débito con un volumen de negocio anual de 2000 millones de pesetas. Por poner un ejemplo de la implantación de estos servicios, bastaría con saber que Visa Internacional tiene 360 millones de tarjetas operativas (185 solo en USA), y 11 millones de comercios de todo el mundo aceptan dicha tarjeta.

El uso electrónico de la tarjetas de crédito en una compra exige la identificación del usuario ante el comerciante mediante otro documento firmado (DNI, Pasaporte, etc.). Con los datos contenidos en ella (nombre del titular, número de la tarjeta, fecha de expedición, fecha de caducidad) y datos referentes al comerciante (identidad del establecimiento, fecha, hora, número de operación) y la cantidad debida, el comerciante envía a través de la Red Telefónica Conmutada una solicitud al Banco para la autorización de la transacción. De aceptarla el Banco, este envía un número de autorización que completa con los datos anteriores, un documento escrito que habrá de firmar el cliente para cerrar la transacción. En el caso de que surjan conflictos entre cliente y comerciante, sólo la presencia o ausencia del documento escrito determinará quien vence en la disputa.

La característica más sobresaliente de este tipo de transacciones es que siguen fundamentándose en la firma manuscrita de un documento por las partes con el arbitraje de una tercera institución; el Banco representante de la parte acreedora. En ese documento quedan claramente establecidas las identidades de los agentes y la naturaleza de la transacción, por lo que son operaciones perfectamente trazables.

Informatización de la Sociedad

Paralelamente al desarrollo del negocio bancario, también se han desarrollado otros aspectos de la vida cotidiana en cuanto al flujo de información se refiere. Las necesidades de la seguridad interior y de los servicios de toda índole que realiza el Estado a los ciudadanos, exigen la

asignación de identificadores únicos para cada uno de ellos. Así hay ciertos valores que nos identifican completamente (Nombre completo, DNI, Pasaporte, etc.) como ciudadanos y a los que están ligados todos nuestros derechos y obligaciones.

La existencia de estos parámetros permite identificar y relacionar a los individuos con muchas de sus acciones, en caso de necesidad, pero el esfuerzo puesto en juego para ello en una sociedad basada en archivos físicos,era considerable. De hecho, la confección de esos dossiers casi siempre exigía al ciudadano la presentación de credenciales autenticas (Partidas de Nacimiento, Certificados de Empadronamiento, Actas notariales, Titulaciones Académicas, etc.) en el caso de querer ejercer alguno de sus derechos, lo que supone un sobresaliente esfuerzo por parte de éste. Cuando la confección de dichos expedientes, por su naturaleza, no contaban con la colaboración del ciudadano (expedientes sancionadores, investigaciones policiales, etc.) la tarea era engorrosa y bastante cara, por lo que tan sólo se realizaban de modo esporádico y en casos de necesidad expresa.

La existencia de Identificadores Personales Universales (ej., DNI) se han extendido a todas las actividades sociales del ciudadano, por lo que son muchas las instancias, organismos, empresas, etc., que contienen en sus archivos información parcial del ciudadano, y que resulta necesaria para el correcto funcionamiento de las mismas en sus relaciones sus clientes (Bancos, Compañías de Seguros, Grandes Almacenes, Clubes Deportivos, Asociaciones de toda índole, etc.). Con la informatización de la sociedad y más aún, con su previsible crecimiento, esos archivos son cotejables electrónicamente, por lo que la dificultad de proceso que exigía la confección no autorizada de expedientes personales que defendía al ciudadano frente a los depositarios de esa información, ha desaparecido.

Dentro de las actividades cotidianas de un ciudadano, el movimiento de pequeños capitales es, probablemente, la actividad más frecuente (ingresos y gastos). Con el establecimiento de las formas de pago electrónicas, cada una de las transacciones da cuenta detallada de nuestras actividades a las bases de datos bancarios en las que estamos inscritos. La posibilidad del tratamiento automatizado de dichos datos aparentemente dispersos permite actualmente realizar informes específicos muy detallados sobre las tendencias de todo tipo, gustos y necesidades de los ciudadanos, sin contar para ello con la intervención o conocimiento de éstos. Por ello, hay algunas voces que públicamente alertan sobre la pérdida de intimidad, por parte del ciudadano, frente a la discrecionalidad de los depositarios nominales de dichos archivos y bases de datos electrónicas.

La presión del mercado y la necesidad de publicidad han hecho que se persiga individualmente al potencial cliente hasta su misma casa. Para

ello se recurre al estudio automático de diferentes bases de datos con el ánimo de descubrir de entre todos los ciudadanos, aquellos a los que pudiesen interesar (según sus criterios) los servicios ofertados. Este fenómeno de compra/venta de archivos electrónicos de datos personales, las sociedades modernas intentan, por vía legislativa, atajar esta practica, pero la eficiencia de tales normas es puesta en duda por algunas voces especializadas. El origen último de este riesgo potencial está en la existencia de parámetros universales de identificación de los ciudadanos. Mediante un número de DNI, por ejemplo, es trivial localizar todos los datos que sobre un individuo están contenidos en cada una de esas numerosas bases de datos.

Quizás sea éste relativamente fácil seguimiento de las actividades individuales una de las razones por la que no parece verosímil la completa sustitución del dinero en metálico por modos de pago automático. Mientras el papel moneda goce de su intrazabilidad esencial (no hay constancia alguna entre la identidad de los ciudadanos y los billetes con los que operan), ningún procedimiento automático podrá desbancar su importancia en la sociedad. Más aún, la proliferación de abusos contra la intimidad de los ciudadanos conduciría, sin duda, a una recesión en la popularidad de los sistemas automáticos de pago, con lo que se perderían las muchas ventajas que han hecho proliferar tanto a dichos servicios.

La propuesta técnica más seria para atajar de raíz este problema, la universalidad de los identificadores personales, consiste en el uso de *pseudónimos* hecha por David Chaum de Digi-Cash (Holanda). Según ese autor, el único modo de evitar que otros puedan reunir datos de un ciudadano que éste no les haya entregado voluntariamente, es que con cada organización interlocutora, utilice pseudónimos distintos. De ese modo, cada organización puede mantener un registro coherente de los datos personales que voluntariamente le han sido confiados, sin que esa información pueda ser útil a ninguna otra organización, puesto que los pseudónimos empleados por el cliente han sido elegidos por éste al azar, y certificados por una Autoridad Central.

Esta Autoridad Central es la única que podría relacionar los pseudónimos entre si, y éstos con un ciudadano real, por lo que la protección y control de esa información reunida en una sola organización puede ser más eficaz, y proteger así el derecho a la intimidad de los ciudadanos.

En otras palabras, la propuesta del uso de *pseudónimos* equivaldría a que, por ejemplo, el Estado, como Autoridad Central, dotase a cada ciudadano de un número suficientemente grande de Documentos Nacionales de Identidad en los que apareciesen diferentes nombres y números de identificación. De ese modo el ciudadano podría utilizar cada uno de ellos en sus relaciones con distintas organizaciones y sólo

serian conjugables aquellos registros de datos en los que se utilizase el mismo documento de identidad (el mismo pseudónimo).

Confidencialidad de las Redes Telemáticas

Las redes telemáticas actuales han sido diseñadas con objetivos puramente técnicos. Por ejemplo, los servicios de mensajería electrónica tan en boga en la sociedad occidental actual, se diseñaron para asegurar la llegada de los mensajes a su destino en el menor tiempo posible, salvaguardando a éstos de errores de transmisión o de la indisponibilidad temporal de diferentes elementos de la red. Estos objetivos están plenamente conseguidos y siguen mejorándose día a día.

Esas redes de comunicación no incluyen de forma standards nada parecido a los "sobres" del servicio postal, cuya misión en ocultar a todos, excepto al destinatario legítimo, el contenido de los mensajes. Los documentos que se transfieren a través de la mayoría de redes telemáticas en funcionamiento, no contienen ningún elemento genuino del emisor como puede ser el papel utilizado (membrete), y la firma y letra manuscrita del equivalente postal. Como consecuencia de ello, podemos ver las redes telemáticas (standards) civiles de hoy en día, como foros públicos en los que cualquier elemento de la red puede ver, registrar, modificar, y sustituir cualquier mensaje, y en las que el destinatario no puede confiar en la presunta autoría y veracidad de los mensajes que recibe.

Lo más delicado de este asunto es que la intercepción de los mensajes electrónicos puede llegar a ser prácticamente indetectable. En el equivalente postal, cualquiera puede interceptar un envío y abrirlo, pero con ello se causan modificaciones en el envoltorio del mensaje que son difícilmente ocultables. La generación de un documento físico idéntico es extremadamente difícil; se puede "fotocopiar" el contenido, pero no duplicar el documento.

Estas características hacen que la defensa legislativa de la sociedad frente a los delitos informáticos contra la intimidad sea, presumiblemente, poco eficiente. Algunas compañías incluyen en sus programas modos de cifrar ciertos detalles sensibles en los mensajes que generan, como pueden ser los números de las tarjetas de crédito, la naturaleza de la transacción, etc.

Se prevé que con la aparición de programas de cifrado suficientemente seguros, millones de usuarios crearían un comercio electrónico viable. Estas soluciones criptográficas resolverían, en un plazo breve de tiempo, el problema de la accesibilidad indiscriminada de los datos que circulan dentro de las redes telemáticas, pero no defendería en nada al usuario

respecto al uso que los destinatarios legítimos de los datos hagan de ellos.

Papel Moneda Electrónico

El dinero en metálico hace tiempo que perdió su carácter "metálico". El dinero en efectivo consiste en billetes de papel o monedas, documentos físicos, por los que el Banco emisor se compromete al reconocimiento de cierto "valor" al portador del objeto sea este quién sea. Son muchas y variadas las razones por las que dentro de cada estado hay una única entidad emisora de papel moneda, pero una de ellas es la normalización del documento, de modo que toda la sociedad sea capaz de verificar, con mayor o menor grado de precisión, la autenticidad de los billetes.

El papel moneda es una declaración firmada de un derecho del portador ante la entidad emisora, y dicha declaración sólo esta identificada por un número de serie único en cada caso, la fecha de emisión, la identidad del Banco emisor, y el valor nominal del billete. El resto de elementos que constituyen el papel moneda se repiten en todos ellos y son dificultades añadidas para su fabricación o duplicación en aras a conferirle atributos de autenticidad y unicidad. La firma de un individuo, o de una entidad a través de su representante, se considera única en cuanto a quién puede realizarla, porque se cree que el acto de firmar es un procedimiento reflejo imposible de enseñar a realizar, y difícil de imitar. Cuando se firma un documento físico, la firma se añade al documento del que pasa a formar parte. La firma válida no puede desligarse posteriormente del documento, ni puede ser alterada sin poner en evidencia dicha manipulación.

En una red telemática los mensajes consisten en secuencias de números que se transportan como señales eléctricas u ópticas a través de cables, fibras ópticas u ondas de radio. Su característica primordial es la de ser información pura y estar carente de un soporte físico específico. El equivalente electrónico de un billete bancario o de cualquier otro documento, consistiría simplemente en un vector de dígitos (bits) numéricos, lo que plantea dos grandes problemas:

- Es necesario que todo ciudadano pueda comprobar en cualquier momento que el billete es *genuino*, tanto en la información que contiene (su valor nominal), como en la identidad del emisor.

- Es necesario poder confiar en que el billete electrónico que posee es *único*.

De no poderse verificar la autenticidad de un billete electrónico, cualquiera podría emitir sin autorización billetes electrónicos en nombre de cualquier entidad (suplantación de identidad), o modificar el valor

nominal de billetes genuinos en circulación (manipulación del contenido). Si el billete auténtico no fuese único, éste se podría simplemente copiar tantas veces como fuese necesario. Los billetes electrónicos deben gozar, al menos, de las mismas características que sus análogos en papel moneda.

Dichos billetes deben contener pruebas de su autenticidad de origen, y de no haber sido manipulados con posterioridad a su emisión por parte del organismo autorizado. Dado que la información digital no está unida a ningún soporte físico concreto, la posibilidad de copiar el billete electrónico es absoluta, no habiendo diferencia alguna entre el original y sus copias.

La criptografía moderna ha desarrollado procedimientos algorítmicos que permiten, con cierto margen de seguridad, añadir valores de autenticidad a los mensajes electrónicos.Para poder comprobar que un documento digital no ha sido manipulado parcialmente en su contenido, dentro de la información que constituye el documento se incluye cierta redundancia, cierta estructura, que se vuelve inconsistente en cuanto se cambia el más mínimo elemento del mensaje. Sólo aquellos mensajes recibidos que mantengan la consistencia se aceptaran como genuinos.

La complejidad de esta estructura del mensaje marca el grado de seguridad que podemos tener sobre la autenticidad de un mensaje electrónico. La aparición de los algoritmos criptográficos de clave pública ha permitido una eficiente generación de equivalentes digitales de la firma manuscrita.

A diferencia de ésta, la identidad de una firma digital se basa en el conocimiento exclusivo por parte del firmante de cierta información secreta. Por ello, la firma digital, aún siendo mucho más difícil de falsificar que su equivalente manuscrito, si puede transferirse irreversiblemente a otros, con lo que el firmante asume la responsabilidad de mantener en secreto y protegida dicha información.

El conocimiento de la clave secreta equivale, en un algoritmo de firma digital, a la identidad en una red telemática. Combinando estos dos elementos, esto es, firmando con una información secreta propia de cada individuo un documento digital con una estructura lógica compleja y conocida, podemos estar seguros de que el documento firmado lo fue realmente por su autor y que no ha sido modificado desde entonces. Si aplicamos esta tecnología al caso del papel moneda, podríamos imaginar mensajes digitales firmados por el Banco emisor que actúen como moneda electrónica. Este billete electrónico sólo podría ser generado por una entidad, y su contenido no podría ser modificado por nadie que no fuese su autor, sin embargo, podría ser copiado por cualquier persona.

Por la inherente independencia de la información del soporte físico que la transmite o almacena, no se puede hacer un equivalente directo del papel moneda con mensajes digitales auténticos firmados. El gran reto es hacerlos únicos.

Unicidad de los Billetes Electrónicos

Una posible forma de hacer único un mensaje electrónico es vincularlo de modo indisoluble con su generación o recepción, y asegurar que esta es única.

En una primera aproximación, el Banco emisor podría generar un billete electrónico por la cantidad solicitada por uno de sus clientes, asignarle un número de serie único, la fecha de emisión, firmarlo y simultáneamente descontar su valor de la cuenta del cliente. Con este billete, el solicitante podría pagar servicios y mercancías a cambio de una factura (electrónica). La presentación del billete ante el Banco emisor acreditaría su valor nominal en la cuenta del portador y con ello se completaría la transacción. Este sistema puede hacerse suficientemente seguro como para evitar que tenga éxito cualquier duplicación de billete, puesto que dicha orden de pago está relacionada con la identidad del cliente que la solicitó y con la documentación generada en la transacción de compra/venta. Consideremos las siguientes situaciones:

- Si el cliente decidiese copiar el billete y gastarlo dos veces, el hecho se podría en evidencia en el intento de un segundo comerciante por cobrar un billete con el número de serie de un billete ya gastado previamente. Los dos comerciantes presentarían las documentaciones de dos transacciones válidas y completas, elatando así al solicitante del billete electrónico como responsable de la duplicación.

- Si fuese el comerciante quién quisiese cobrar dos veces el mismo billete, el banco detectaría que ya ha sido pagado, y al no poder el comerciante presentar la documentación de una segunda transacción válida, se autoinculparía del fraude.

Con este procedimiento, el Banco conoce el número de serie del billete que firmó, con lo que al abonarlo en la cuenta del comerciante, puede relacionarlo con la identidad del cliente que lo solicitó. Este procedimiento es seguro para las tres partes involucradas, pero no es anónimo; el Banco puede confeccionar un dossier con los datos de todas las transacciones realizadas por su cliente. Además, este billete no es transferible a una cuarta persona puesto que todas las responsabilidades caerían sobre el cliente que en origen solicitó la emisión del billete.

Este modo operativo es, a fin de cuentas, equivalente al uso de una tarjeta de crédito:

1. el número de la tarjeta autoriza al cliente para solicitar billetes electrónicos,

2. la tarjeta constituye el documento físico que relaciona esta potestad con la identidad del cliente, y

3. el código de autorización que envía la entidad bancaria, el número de la tarjeta, la identidad del cliente, y el valor de la transacción constituyen el billete electrónico.

Protocolos

Siguiendo la nomenclatura tradicional en la descripción de protocolos criptográficos, vamos a considerar los siguientes agentes: un cliente genérico llamado Alicia, el Banco emisor y un Comerciante.

Generación del Billete:

1. Alicia genera al azar el número de serie del billete. La longitud de este número será tal que, la probabilidad de que otro usuario opte al azar por el mismo número, sea suficientemente pequeña (unas 100 cifras decimales)

2. Alicia firma con un pseudónimo aceptado por el Banco dicho número/billete, y se lo entrega al banco con la recepción del correspondiente resguardo.

3. El Banco verifica que el número de cuenta declarado por el solicitante coincide con la firma del envío anterior, y la retira de dicho billete.

4. El banco firma el billete y lo hace con una clave que indica su valor nominal, descuenta esa cantidad de la cuenta de su cliente, y devuelve a éste el billete firmado.

Consumo del Billete:

1. Alicia entrega el billete al comerciante como pago de ciertas mercancías o servicios.

2. El comerciante verifica la firma del banco emisor así como el valor nominal del billete.

3. El comerciante transmite a la entidad emisora el billete recibido.

4. El Banco busca ese número de serie en su base de datos de billetes gastados y comprueba que no está.

5. El banco acredita el valor nominal del billete en la cuenta del comerciante y notifica a éste su validez.

6. El comerciante entrega a Alicia la mercancía junto con un recibo firmado de la transacción.

En este sistema las tres partes pueden estar seguras, pero no hay anonimicidad. Si el Banco tiene la capacidad de rastrear la circulación de sus billetes mediante el número de serie, entonces puede cotejar los datos de las emisiones de los billetes con los datos de los correspondientes reintegros, y así determinar exactamente, cuando y donde gastan sus clientes el dinero.

Firmas a Ciegas

Para resolver el problema anterior habría que conseguir que el Banco no pudiese relacionar los reintegros que hace, con la identidad del cliente que solicita la emisión de los billetes. Para ello se han propuesto algoritmos en los que el Banco "firma a ciegas" los billetes. El protocolo anterior quedaría modificado del siguiente modo en lo que atañe a la generación del billete:

1. Alicia genera un número de serie (billete) al azar, y lo multiplica por un coeficiente secreto (coeficiente de ocultación) también elegido en su momento al azar y suficientemente grande, generando así un billete "opaco".

2. Alicia firma con un pseudónimo aceptado por el Banco, dicho número/ billete "opaco"

3. El Banco verifica la firma de Alicia y la retira del billete opaco.

4. El Banco firma el billete opaco con una firma que le confiere su valor nominal y se lo devuelve a Alicia a la vez que retira esa cantidad de la cuenta de su cliente.

5. Alicia divide el número de serie opaco por el coeficiente secreto que utilizó y obtiene así el billete en claro.

Los números de los billetes opacos son "incondicionalmente intrazables"; es imposible relacionar el número de serie en claro del billete con el número obtenido después de la ocultación con un coeficiente secreto.

Aunque se pusieran de acuerdo el Banco y el Comerciante, de ningún modo podrían relacionar el número de serie de un billete con un cliente, ya que sólo éste conoce el coeficiente secreto de ocultación. En la generación del billete participan Alicia y el Banco, pero éste no conoce que número de serie que firmó; tan sólo sabía que se trataba de un billete de un determinado valor y que se lo solicitaba Alicia a través de uno de sus pseudónimos.

El anonimato de los billetes opacos no tiene más límite que la impredicibilidad del número elegido por Alicia como coeficiente de ocultación. Sólo Alicia puede hacer públicos dichos coeficientes y así relacionarse automática y voluntariamente con la transacción en la que lo empleó.

Para evitar que un mismo billete electrónico pueda ser gastado más de una vez, antes de aceptarlo es necesario confrontarlo instantáneamente con una lista central permanentemente actualizada de números de serie ya gastados. Esta práctica puede ser aceptable cuando la cuantía de los billetes justifique los gastos de mantenimiento y comunicación con dicha "lista central", pero sería ruinosa en el caso de billetes pequeños.

Esta necesidad de conexión on-line con el Banco emisor del billete, y la necesidad de una base de datos única de billetes electrónicos gastados, son los dos inconvenientes que limitan la eficiencia, de este protocolo.

Para evitar esta necesidad de conexión on-line, A. Fiat, M. Naor y el propio D. Chaum han propuesto una modificación de estos protocolos de firma a ciegas en los que el cliente debe responder ante el comerciante a una encuesta numérica aleatoria acerca de cada billete cuando efectúa el pago. En estos protocolos el gasto del billete implica añadirle cierta información oculta sobre la identidad del que lo gasta.

La indetectabilidad incondicional de la firma a ciegas no sufre menoscabo alguno si el billete se gasta una sola vez, pero si se gasta dos veces, los datos de la primera y segunda transacción dejarían en claro suficiente información como para localizar la cuenta e identidad del solicitante del billete. De hecho, con estos procedimientos se generaría una confesión firmada digitalmente de la autoría de fraude, sin que esta pueda ser falsificada ni por el Banco ni por el Comerciante.

Con la inclusión de información oculta del que gasta el billete se elimina la necesidad de consultar al Banco emisor sobre la validez de un número de serie, ya que, de cometerse fraude, éste sería perseguido y sancionado a posteriori.

Por último, tan sólo nos queda mencionar que la mayoría de los protocolos criptográficos propuestos para la generación de Billetes o monedas electrónicas no satisfacen una de las características

primordiales del papel moneda habitual; los billetes electrónicos no son transferibles. De ese modo, se puede mantener el anonimato en una transacción con tres agentes (Alicia, Banco, Comerciante) pero no es fácil generalizarlos para cadenas con más de tres elementos. El único protocolo que permite esta transferibilidad requiere billetes conteniendo tanta información que son, por el momento, inviables en escenarios comerciales reales y para pequeñas cuantías.

Tarjetas Inteligentes: Representantes y Observadores

Los protocolos de billetes electrónicos requieren de un soporte físico para realizarlos. Al tratarse de procedimientos algorítmicos criptográficos cada agente necesita de un ordenador que pueda realizar los cálculos implicados en las firmas digitales y en la generación y ocultación de números de serie y otras informaciones. Este ordenador actuaría como *Representante* de cada agente del mercado electrónico.

En principio, cualquier ordenador, dotado del software adecuado podría participar en ese mercado electrónico, por lo que se mantiene la independencia e inexpecificidad respecto al soporte físico que ya hemos mencionado anteriormente. Las tendencias actuales es dotar a cada usuario de Tarjetas inteligentes con una fisonomía muy similar a la de las actuales tarjetas de crédito y dentro de las cuales se incluye un chip con capacidades de procesamiento, de memoria y de comunicación.

El programa contenido y ejecutado dentro de la tarjeta inteligente sería el interlocutor del usuario dentro de los protocolos que hemos mencionado. Dichas nuevas tarjetas inteligentes podrían llegar a tener un teclado de modo que el usuario debiese identificarse mediante un número personal de identificación (PIN) ante la tarjeta, y de una pantalla en la que ésta informase al usuario de las informaciones pertinentes referentes a la transacción. La comunicación se realizaría mediante enlaces de corto alcance (señales infrarrojas) de modo que los representantes no tendrían que abandonar en ningún momento las manos de sus propietarios.

Los usuarios pueden confiar en sus representantes porque cada uno de ellos elige su propia máquina y puede reprogramarla a su voluntad. Tanto las organizaciones como los usuarios, están protegidos por la solidez de los protocolos criptográficos, y el carácter público de éstos. Los representantes al actuar en nombre de sus propietarios, ofrecerían a este resúmenes de los detalles de las transacciones así como guardarían copias de las autorizaciones del titular para entregar los fondos. En su dialogo con otros representantes, obtendría resguardos electrónicos que acreditan cada fase de las transacciones, y conservarían en secreto las claves de cada usuario. Conservando copias de seguridad de las claves, los billetes electrónicos y demás datos contenidos en los representantes,

se podrían recuperar los fondos en caso de robo o extravío del representante, minimizando así las pérdidas en el caso de situaciones adversas. Las aplicaciones que se proponen y que DigiCash tiene montadas actualmente a nivel de prueba incluyen desde el uso de fotocopiadoras, máquinas de fax, caja registradoras, máquinas de café y refrescos, etc. Hasta el cobro automático del peaje en autopistas. Todas estas precauciones amplían grandemente los márgenes de seguridad para el usuario, pero las organizaciones no suelen aceptar con agrado tener que perseguir con posterioridad los fraudes aunque tengan todos los datos para ello.

Desde el punto de vista de las organizaciones, el sistema sólo sería aceptable si en el sistema se incluyen medidas preventivas frente al fraude, por lo que se han propuesto el empleo de *Observadores*. Un observador es un pequeño circuito integrado a prueba de manipulaciones, producido por alguna entidad en la que las diferentes organizaciones puedan confiar, que se incrusta en el hardware de cada representante y que actuaría a modo de notario certificando el correcto funcionamiento de cada representante. Este modelo se basa en la hipótesis de Desconfianza Mutua Perfecta: El observador no confía en el representante que le alberga, ni el representante confía en el observador al que hospeda. Phillips, Siemens, Thompson CSF y Motorola han construido o han anunciado su propósito de construir este tipo de circuitos.

Protocolos con Observadores

En la desconfiada asociación entre observadores y representantes, estos tienen que poder controlar todos los datos que llegan o provienen del observador, y así comprobar que no se filtran informaciones inconvenientes o secretas hacia el mundo exterior. Por ejemplo, la generación de pseudónimos digitales con un protocolo con observadores sería del siguiente modo:

1. Alicia adquiere un observador, lo instala en su representante y lo lleva frente a una autoridad interventora para conferirle validez.

2. El observador genera un lote de pares de claves públicas/privadas a partir de sus propios números aleatorios y de los suministrados por el representante (consumación del matrimonio).

3. El observador no revela sus números aleatorios pero facilita suficiente información sobre ellos al representante para que éste pueda comprobar que sus números aleatorios fueron realmente empleados para producir las claves resultantes.

4. El representante genera números aleatorios secretos para ocultar cada una de las claves del observador (coeficientes de opacidad o de ocultación).

5. El observador torna opacas las claves públicas, las firma con una clave especial y se las entrega al representante.

6. El representante confirma la opacidad la opacidad de las claves, verifica la firma del observador, y se cerciora de que las claves han sido correctamente generadas.

7. El representante transfiere las claves cegadas y firmadas a la autoridad interventora.

8. El interventor reconoce la firma del observador y la retira para sustituirla por la suya propia, antes de devolverle las claves al representante.

9. El representante torna visibles las claves que, firmadas por la autoridad interventora, harán el papel de pseudónimos digitales en las futuras transacciones.

Una vez realizado este tipo de protocolos, todas las transacciones que realice el representante deberán contar, para ser válidas, con ciertos certificados emitidos por parte del observador. Al no poder el usuario alterar el comportamiento del observador se evitan los posibles comportamientos fraudulentos de éste.

La filosofía que subyace en este tipo de asociaciones es enfrentar dos unidades autónomas condenadas a colaborar entre si con el fin de verificar una serie de exigencias. El origen de este tipo de protocolos esta en algo emblemático como la verificación de tratados militares de limitación de armas entre ejércitos enemigos en tiempo de paz.

Dinero Electrónico Intrazable y Crimen Perfecto.

Los efectos que sobre la sociedad puede tener la aparición de equivalentes electrónicos del papel moneda pueden ser muchos y de índoles muy variadas. En esta tesis no pretendemos explorar ese universo de posibilidades, pero hemos querido recoger aquí un escenario aparecido en la literatura especializada sobre un “crimen perfecto” perpetrado gracias a los protocolos de firma a ciegas.

S. von Solms y D. Naccache, en su artículo “On Blind Signatures and Perfect Crimes” comentan como “ ... el creciente énfasis en la protección de la intimidad los datos personales y de sus acciones en los sistemas electrónicos, hacen de las firmas a ciegas una solución perfecta”. Sin

embargo en su artículo discuten un aspecto problemático del uso de dichos protocolos, indicando que tales técnicas, potencialmente, podrían llevar a la consecución del “crimen perfecto”. Para ello, los autores ponen el siguiente ejemplo inspirado en un caso real que no tuvo tanto éxito:

- El criminal secuestra el hijo de una familia socialmente influyente
- El criminal genera al azar suficientes números de serie y coeficientes de ocultación, y los emplea para generar billetes opacos
- Envía los billetes opacos a las autoridades junto con la amenaza de asesinar a su rehén si no se siguen las siguientes instrucciones:

  1. La casa de la moneda firmará todos y cada uno de los billetes con un valor nominal de $100.
  2. Una vez firmados, las autoridades publicaran en un periódico de distribución mundial las secuencias de números que constituyen los billetes.

     - El criminal compra un ejemplar del periódico y transcribe los números publicados a su ordenador, el cual los tornará en billetes en claro gracias a su conocimiento de los coeficientes de ocultación que empleó.
     - El criminal libera sano y salvo a su rehén
     - El criminal ahora disfruta libremente del botín conseguido sin correr el más mínimo riesgo de que le relacionen con los billetes pagados en el rescate.

En este caso de los secuestros convencionales, la transferencia del dinero del rescate a los secuestradores propicia un vinculo entre uno y otros, haciendo posible incriminar a los culpables de su delito. En el caso del dinero electrónico no se produce tal conexión puesto que cualquiera puede leer el periódico donde se publicaron los billetes, pero sólo los secuestradores pueden hacer uso de ellos. No habiendo pruebas incriminatorias, el crimen quedaría impune.

Conclusiones

Con el ejemplo anterior, sus autores quieren poner de manifiesto como esta indiscriminada protección de la intimidad del individuo puede llevar a crear situaciones en las que esos mismos individuos pueden quedar desprotegidos debido al uso de esos mecanismos. Las firmas a ciegas pueden plantear problemas potenciales en lo que se refiere al

mantenimiento del imperio de la Ley sobre ciertos tipos de acciones criminales, con lo que deben considerarse como un arma de dos filos.

No hemos querido entrar en profundidad en este tipo de disquisiciones, pero si hemos considerado conveniente exponer en este trabajo de tesis la existencia de estas posibilidades. La discusión de estos escenarios fuera del ámbito de la comunidad criptológica internacional, mejorará sin duda los desarrollos actuales y, en principio, favorecería el desarrollo de una tecnología aceptable en la que se reconociesen tanto los derechos individuales como los derechos de la comunidad, a la par que se agilizan y facilitan las relaciones comerciales y financieras.

2.3 La seguridad en las transacciones de comercio electrónico

El dinero electrónico y las transacciones comerciales

Siguiendo con el estudio, hemos de añadir un nuevo concepto. Una transacción comercial electrónica debería poseer atomicidad. Esta característica de las transacciones depende de varios factores que se describen a continuación:

Una transacción debe exhibir integridad. Esto quiere decir la transacción debe comenzar y finalizar en forma segura. Debe poderse realizar el llamado «rollback» (deshacer) en caso de desearlo por alguna de las partes, en cualquier momento de la misma. Así pues, el deshacer los pasos llevados a cabo por una transacción o el desecharla automáticamente, deben ser características básicas de la misma.

- Debe ser auténtica. Una transacción auténtica implica que ambas partes sepan fehacientemente sus respectivas identidades. Por otra parte, en caso de realizarse el pago en efectivo, puede que no sea importante la identidad del cliente pero si la legitimidad del dinero electrónico utilizado.

- Una transacción no debe ser repudiable.

- Esta característica concierne a las reglas implícitas en un contrato comercial. Hablamos de contrato en términos de intercambio de elementos legales. Por un lado el cliente entrega una orden de solicitud de un producto determinado, por el otro el vendedor entrega al cliente una boleta que garantiza la entrega de dicho producto. En medio de estos procedimientos está el intercambio de dinero. En el caso de transacciones comerciales electrónicas, el cliente debería no poder negarse al envío de una solicitud u orden de compra (si así se estableciere), y asimismo debería poder rechazar una orden enviada

en caso de ser víctima de un fraude. Similares restricciones deberían cumplirse en pos del comerciante.

Queda claro en todos los puntos mencionados que las transacciones comerciales electrónicas entran en conflicto cuando deben atenerse a reglas que de hecho se cumplen en la vida comercial actual, aún siendo absolutamente contradictorias. Así vimos que una transacción debe ser confidencial y anónima en algunos casos o todo lo contrario en otros. El dinero electrónico debería ser seguro y los sistemas que utilicen dinero electrónico deberían ser «escalables» a fin de ajustarse tanto a transacciones menores, como a algunas de mayor porte.

La seguridad en el comercio electrónico

Tal como se indicó en párrafos anteriores, el éxito en la implementación de un sistema de comercio electrónico, hace entre otras cosas en garantizar autenticidad en la información transmitida y en satisfacer requerimientos de atomicidad en la transacción. La seguridad y la atomicidad se logran actualmente mediante la práctica de diferentes procedimientos que describiremos a continuación.

Encripción

La encriptación es el proceso mediante el cual se transforma cierto texto «plano» a un mensaje codificado o cifrado («cifratexto»), el cual no por ello pierde significado. Este proceso conlleva como es de esperarse al seguimiento de una serie de pasos y técnicas a fin de obtener el resultado esperado. Así pues la criptografía clásica habla de dos métodos fundamentales: la transposición y la sustitución.

Hablamos de transposición, cuando alteramos el orden de los símbolos en un texto. De esta manera el siguiente ejemplo de texto, transpuesto quedaría como se muestra:

VENDER
[texto plano]

DNEERV
[texto transpuesto]

Por el contrario, el cifrado por sustitución reemplaza los símbolos de un mensaje por otros equivalentes.
Por ejemplo: VENDER [texto plano] quedaría 1928329 [texto sustituido]. En el ejemplo vemos claramente como cambian los símbolos y deducimos por tanto que la única forma de obtener el mensaje original es poseyendo los códigos secretos de conversión. Respecto a los métodos propuestos teóricamente, hemos de agregar que se han

implementado algunos de los que hoy en día se reconocen como los más usados. Entre ellos mencionaremos los que creemos con más difusión: DES (Estándar de Encriptación de Datos) y RSA.
Clave Privada DES -Data Encryption Standard-

Este método está basado en un algoritmo el cual fue estandarizado en 1977 por la Oficina de Estándares Nacionales de los Estados Unidos. Dicho algoritmo utiliza una clave o código secreto para ambos procesos: codificación y decodificación. Los caracteres del texto plano son divididos en bloques de 64 bits. Cada uno de estos bloques es codificado utilizando el código secreto que se escoja. El proceso de codificación sin embargo, resulta en 19 pasos intermedios de ciframiento. Cada uno de estos pasos combina procedimientos de transposición, sustitución y fragmentos XOR, resultado de cada uno de los pasos anteriores de encriptación con la clave secreta.

Clave Pública - El método RSA

El método RSA es considerado uno de los más seguros sistemas criptográficos. Este procedimiento utiliza dos claves interrelacionadas, una pública y otra privada. Asimismo una clave es complemento numérico de la otra. Una de las claves es utilizada para encriptar y la otra para decodificar. En el método RSA es imposible utilizar la misma clave para ambos procedimientos (encriptación y desencriptación).

Cuando se pretende enviar un mensaje encriptado a la otra parte, quien lo envía puede utilizar la clave pública del receptor o su propia clave privada. En el primer caso, una vez que el mensaje haya llegado a destino, sólo la clave privada del receptor será capaz de desencriptar el mismo. En el segundo caso, el receptor puede desencriptar el mensaje mediante la utilización de la clave pública del emisor. Esto asegura al receptor que el mensaje es auténtico, ya que el único que puede utilizar la clave privada es el propio emisor que posea una. Obtener esta clave privada es casi imposible aún teniendo acceso a la clave pública.

A efectos de comprender su funcionamiento, veamos un ejemplo. Existen como siempre una serie de pasos a seguir para asegurarse la autenticación del mensaje por ambas partes. De esta forma, se inicia la comunicación con la utilización de la clave pública provista y publicitada por el proveedor en su página web. El cliente utiliza dicha clave y a través del método RSA codifica su mensaje y lo envía al proveedor a fin de iniciar la comunicación. El comerciante utiliza su propia clave privada para decodificar el mensaje. En este punto ya vemos que el comerciante es el único que puede decodificar el mensaje del cliente ya que debe utilizar su clave privada para hacerlo. A partir de aquí los dos saben que están realizando una transacción segura y continúan con la misma. En el

caso que un intruso interceptara cualquiera de los mensajes, necesitaría una de las claves secretas para desencriptarlo.

Firmas digitales y abreviaciones (digests)

Utilizar claves RSA privadas como único método puede resultar riesgoso. En vez de utilizar una clave privada para codificar cada mensaje que llegue a un destino dado, sería mucho más apropiado aplicar «funciones de datos» a estos mensajes. Cuando esto sucede, el resultado es una nueva cadena resumida. Esta pequeña cadena de texto es la única que necesita ser codificada con la clave privada. La función de datos es usualmente denominada: «función de hash». La nueva cadena resultante de la aplicación de la función hashing se denomina: digest.

Los "digests" o abreviaciones se logran mediante la aplicación de funciones que son muy difíciles de revertir y a su vez muy sensibles a las alteraciones. Por ejemplo, un cambio en un sólo bit dentro de un "digest" ya generado, resultaría en otro "digest" completamente diferente. Además, es muy baja la posibilidad de que dos fragmentos de texto generen el mismo "digest". Así pues, la posibilidad de que un intruso estropee una comunicación entre dos partes que hagan uso de este sistema y que no sea detectado, se reduce a cero.

Por otra parte, la firma digital se crea cuando se codifica un "digest" bajo la clave privada de la parte emisora del mensaje original. Por tanto, la adición de este paso extra conlleva a un incremento en los niveles de seguridad utilizados en el proceso de encriptación.

Digamos pues que mientras que el "digest" asegura la integridad del mensaje, su codificación bajo la clave privada del emisor, asegura la autenticidad del mensaje.

La autenticación del usuario

El proceso de autenticación implica la verificación de la identidad de cada parte componente de una transacción. Ya que no pueden llevarse a cabo transacciones electrónicas si cada una de las partes no confía en la otra, es esencial establecer un proceso mediante el cual cada uno de los participantes pueda verificar la identidad del otro.

El primer método que surge al respecto y el más elemental es la concordancia de un nombre de usuario con una contraseña asignada.

Sin embargo, este método si bien es el más difundido no es el más seguro y existen más de un procedimiento conocido para «crackear» contraseñas encriptadas.

Afortunadamente, este no es el único método y en la actualidad se utilizan mecanismos más sofisticados tales como los que se especifican a continuación:

- Una combinación de desafío-respuesta con certificados electrónicos y
- Utilizando un servidor autentificador que actúa como tercera parte.

Combinación de desafío - respuesta con certificados electrónicos

- Este primer método de autenticación utiliza un certificado electrónico (también conocido como «pasaporte digital»). Este es un fragmento de texto cifrado generado por una «autoridad de confianza», el cual contiene información acerca de:

    1. La compañía que emite el certificado (certificador o «issuer»)
    2. La persona receptora de tal certificado (sujeto o «subject»)
    3. La clave pública del sujeto
    4. Un sello temporal

Este método hace uso de certificados firmados digitalmente por compañías autorizadas. Cualquier persona que desee realizar una transacción segura ha de constatar la certificación de dicha empresa por parte de otra empresa que se dedica a autorizar empresas proveedoras como seguras.

De esta forma cada una de las partes puede obtener certificados electrónicos de tales empresas, los cuales mantienen el siguiente formato:

> Certificate = {IssuerName, SubjectName, Subject-Public-Key, TimeStamp}

Utilización de un servidor autenticador como tercera parte.

El mejor ejemplo de este protocolo es el denominado sistema MIT-Kerberos. Este sistema funciona como un servidor basado en claves secretas que actúa como una tercera parte autenticadora. Kerberos actúa como un servidor de confianza que mantiene claves secretas de los participantes durante un largo período. Cuando un cliente desea establecer una conexión segura con un proveedor, se le requiere al cliente la presentación de un ticket válido. Dicho ticket (obtenido de Kerberos), no es más que una secuencia identificatoria de información encriptada la cual utiliza la clave secreta del proveedor. Debido a que sólo Kerberos y el proveedor conocen esta clave, un ticket válido representa la legitimidad del cliente.

Este sistema si bien es utilizado, posee dos carencias importantes. Primero que una falla del servidor que actúa como tercera parte resulta en una parálisis de las transacciones en la red y segundo, una falla de seguridad en tal servidor libera información privada de los clientes.

Intercambio seguro de claves secretas

A fin de lograr un método de encriptación más seguro y confiable es que normalmente se suelen utilizar los dos métodos a la vez: DES y RSA. El emisor utiliza primeramente una clave secreta en común para ejecutar DES y crear un texto cifrado intermedio. Este texto luego es recodificado utilizando el método de criptado RSA. La única dificultad que aparece en este planteo es la realización del procedimiento por primera vez en donde ninguna de las partes se conocen y por tanto no poseen una clave secreta en común. Sin embargo, se podría utilizar el esquema de autenticación planteado en párrafos anteriores para establecer esta primer clave secreta común.

En conclusión, las firmas digitales, la autenticación, certificación y encriptación proveen métodos seguros para la realización de transacciones comerciales. Asimismo pudimos observar que a través de estos métodos cumplimos algunos de los aspectos discutidos al principio de este artículo: integridad, autenticación y no repudio.

Así pues mediante el uso de estos procedimientos logramos que el dinero digital cumpla con las especificaciones con las que cuenta el dinero en efectivo o los cheques.

Certificados electrónicos

Hasta ahora en todas las transacciones comerciales se procura asegurar la identidad del comprador, pero no se ha hablado mucho de la identidad fehaciente del vendedor. Dado que este punto podría ser un flanco débil en materia de seguridad es que ha surgido una institución denominada: «Authentic Site Seal», quien garantiza que los que estén certificados por ellos, son quienes dicen ser. Los accesos a «Authentic Site Seal» son totalmente encriptados. Por tanto, cada vez que un usuario o cliente desea realizar una transacción económica, puede verificar ante este sitio la veracidad y el nivel de seguridad de la parte vendedora.

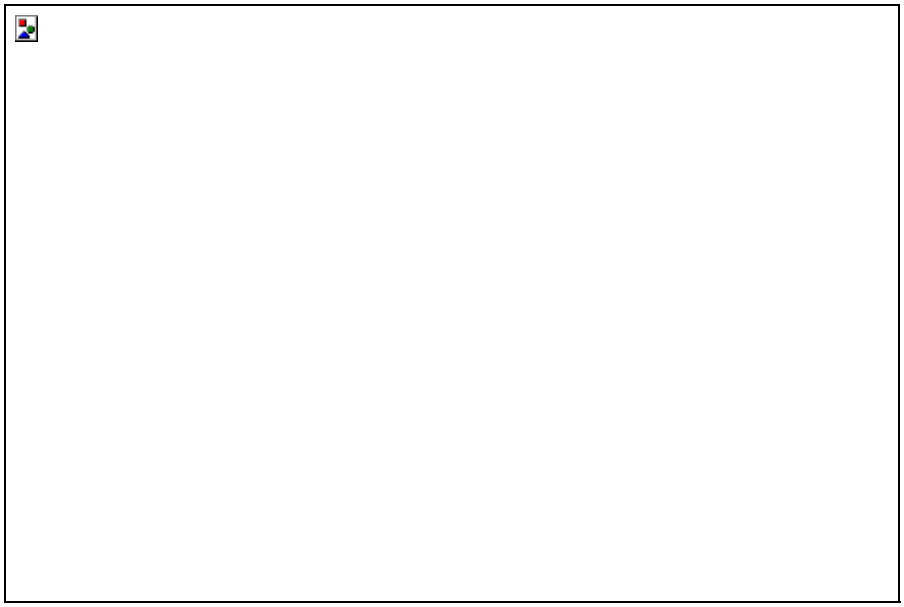
Conclusiones referentes a los aspectos de Seguridad

Queda claro que sin los controles y la seguridad adecuada, el potencial del dinero electrónico tal como lo conocemos nunca se verá realizado. Actualmente, existen una serie de protocolos que pueden asegurar la integridad, autenticidad e irrepudiabilidad en las transacciones

comerciales en el web. Es responsabilidad de los comerciantes también que inviertan en software que proteja al consumidor tal como se protege al comerciante. Por otra parte, el consumidor debe tomar una actitud defensiva ante cualquier propuesta que incluya una transacción comercial, asegurándose acerca de la fiabilidad del sitio con el que trata y siendo consciente de los riesgos asociados a tales procedimientos.

3 RELEVAMIENTO Y CARACTERIZACIÓN DE SOLUCIONES DE PAGOS ELECTRÓNICOS - CASOS OBSERVADOS

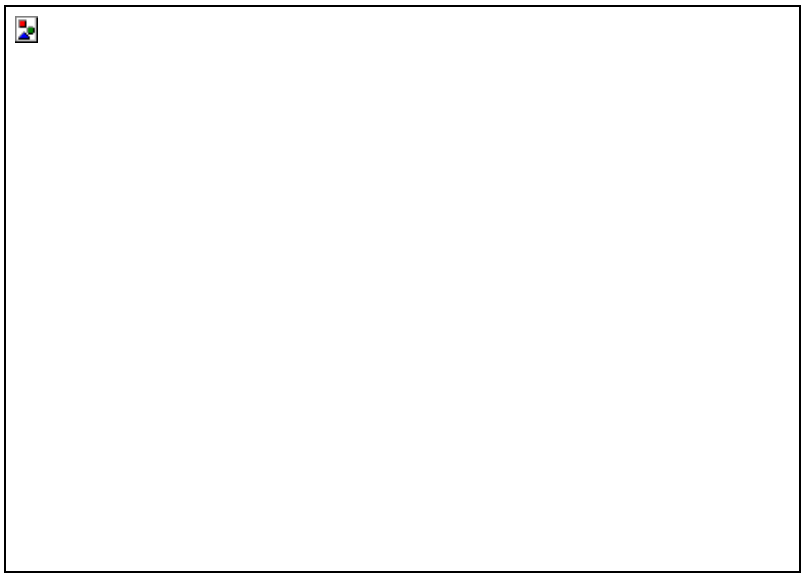
3.1 InternetCash



- Tarjetas no nominativas adquiribles en comercios físicos (valores de 10, 20, 50, y 100 $). Estiman a fin de año más de 10.000 comercios (algunos: Amerada Hess Gas Stations, Dairy Mart, Short Stop, Uneeda Check Cashing). Extensión: NY, California, Massachusetts, Ohio, Pennsylvania, Vermont). Se activan en el mismo comercio de adquisición. **Pueden adquirirse, abonando con TC,** desde el sitio de InternetCash. Recientemente, han cerrado acuerdo de distribución con la empresa IPP (In Presence Payments) habilitando 1400 bocas de distribución. Existe una reciente modalidad virtual de las tarjetas, la que puede ser comercializada como “gift certificate”.
- Accediendo al sitio de InternetCash, el usuario, le suma una clave secreta que lo habilitará a operar con seguridad. Allí pueden también consultar los saldos de los “monederos prepagos”. **El cliente es anónimo**.
- El comercio lo toma como una compra en efectivo. De hecho, es tal la consideración por la pérdida del plástico. **No hay contracargos por fraudes y las transacciones están 100 % garantizadas.**
- Es posible utilizar más de una tarjeta por compra (hasta 30), y se pueden refundir saldos de una en otra. **Esta funcionalidad también potencia la posibilidad de habilitar servicios de C2C (Remates y comercio persona a persona). Han extendido el uso hacia tarjetas corporativas.**

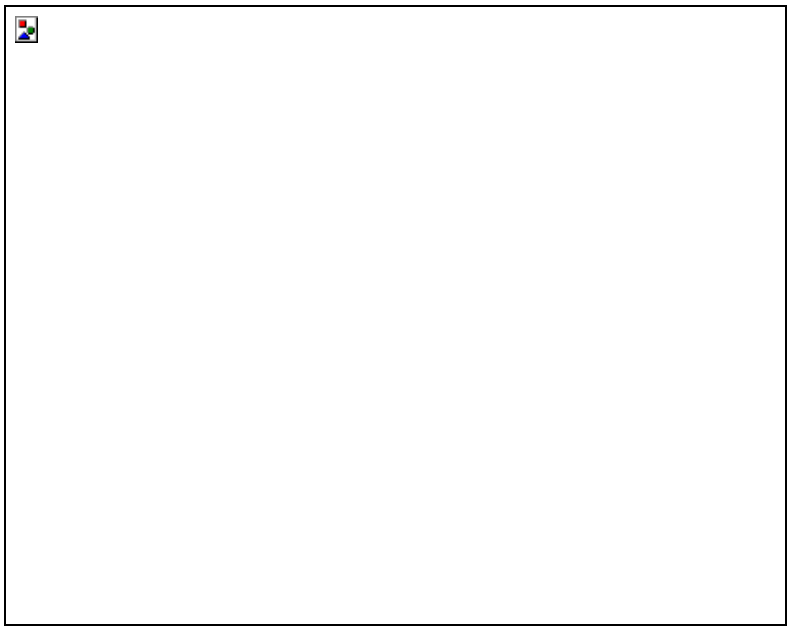
- Son inversores participantes de este servicio: los fundadores de CyberCash (líder en e-cash) y Ron Rivest (RSA) es asesor directivo.
- Tienen como foco del mercado **la inseguridad de informar números de tarjetas de crédito en comercios de la WEB**, y la **habilitación para comprar a usuarios top de la WEB, es decir: jóvenes adolescentes y niños. Asimismo apuntan al target de NO usuarios de tarjeta, que constituyen aproximadamente el 31 % del mercado en USA, y más aun en el resto del mundo.**
- **Se han expandido al mercado latino de USA, haciendo bilingüe el sitio.**
- **Sobre la base de la expansión hacia los hispano-parlantes tiene proyectos de hacerlo sobre Argentina, Brasil, y México. Anuncian la próxima incorporación de Fiera.com.**
- Aproximadamente operan con el servicio 150 retailers, entre los que están RealStores.com, TWEC.com, Overstock.com, ArtistDirect.com, totalmart.com, Allnautical.com, FindCash.com, Sun Glass, Esco.com, BAI computers, y otros).
- Es compatible con las principales soluciones de e-commerce (cart).
- Hacen uso de las seguridades clásicas de Internet (SSL, certificados digitales en comercio y sitio de pagos), sumando criptografía propia (auditada por RSA). Encripción por hardware para los números de tarjetas, y **firma digital de la transacción** por medio de un wallet local o remoto (más comúnmente) procesado desde un servidor seguro.
- Inversión a la fecha: 12 M u$s.
- Socios tecnológicos IBM, Microsoft, Allaire, Americart, HipHip Software, Plug'n Pay, Intershop, Freemerchant, y otros.
- Prevén el expendio de tarjetas por kioscos y **ATM's.**
- **Pagan comisión a los comercios distribuidores, y cobran a los e-merchant un promedio del 2,25 % del monto de la transacción.**

3.2 e-PagoFácil



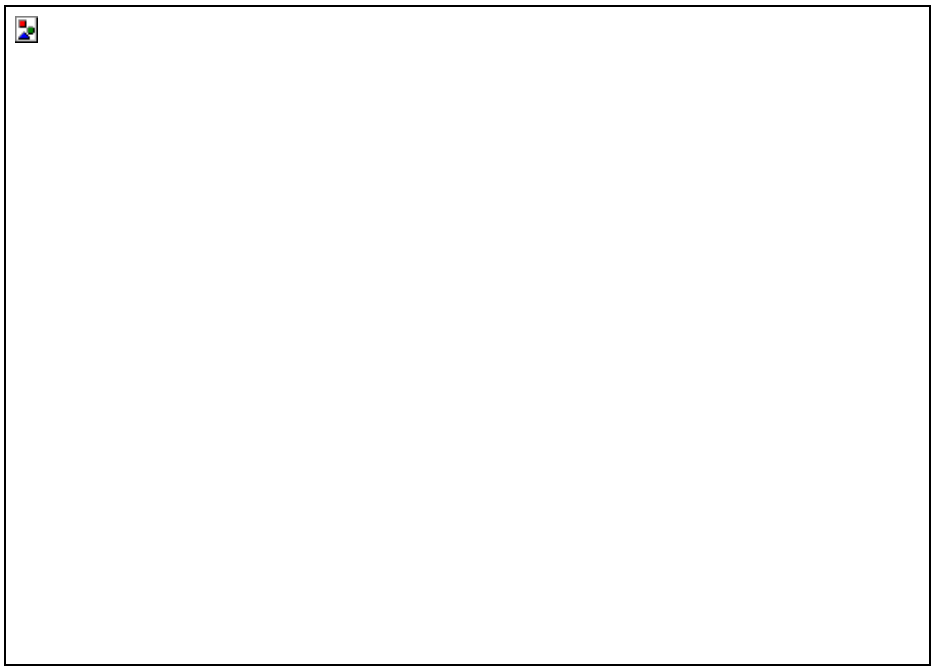
- Es un esquema de pospago (se utiliza el efectivo virtual como medio de pago antes de haberlo abonado con dinero real), en el cual el sitio emite un comprobante con código de barras, que el comprador abona luego en la red de locales físicos de pago
- Luego de recepcionado el pago por el comercio (24 hs) se dispara el envío de mercadería
- El socio financiero de SOCMA es JPMorgan, con una inversión inicial de 20 M u$s, estimando crecer a 50 M u$s más. La empresa del grupo es Mercosur Technology & Communications
- Proyectan la extensión regional (de hecho el site está en español, portugués e inglés)
- Operan con el sistema, hasta hoy: Altocity.com, lafemenina.com, segurlink.com. Hay anuncios de otros comercios electrónicos
- El site da servicios complementarios: agenda de vencimientos y consultas. Complementa con información general del servicio físico conocido.

3.3 NovaCash



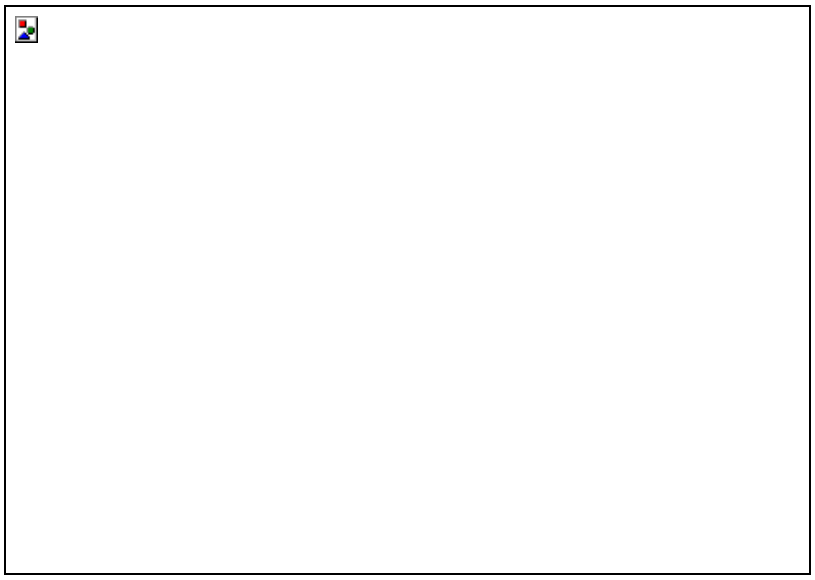
- Servicio de características similares a Internetcash (Sistema prepago contarjetas) , en el ámbito local.
- Inversión por la empresa Cardecom (administradora de tarjetas), en Latinoamérica, es de 40 millones de u$s.
- Distribuidores y expendio de tarjetas: YPF Repsol, OCA, Correo Argentino, máquinas expendedoras en shoppings y cines.
- Operador: Impsat, entidad financiera que actúa fideicomiso Sudameris.
- Emisión prevista en los 3 primeros años: 3.000.000 de tarjetas.
- El lanzamiento estaba previsto para Octubre del 2000.
- Titulares : Familia Sielecki: Laboratorios Smith Klein, Parke Davis, Osiris, Phoenix – Negocios en la Patagonia – Facturación anual del grupo: u$s 150 Millones anuales.

3.4 Boleto Bancario



- Boleto Bancario es una modalidad de pago para no bancarizados utilizada en Brasil, de características similares a la propuesta de e-pagofácil.
- Existe emisión de un ticket que se abona en sucursales bancarias, y la entrega del producto se efectúa contra confirmación del pago efectivizado.
- Bradesco tiene el servicio.

3.5 PayPal (e-mail payments)

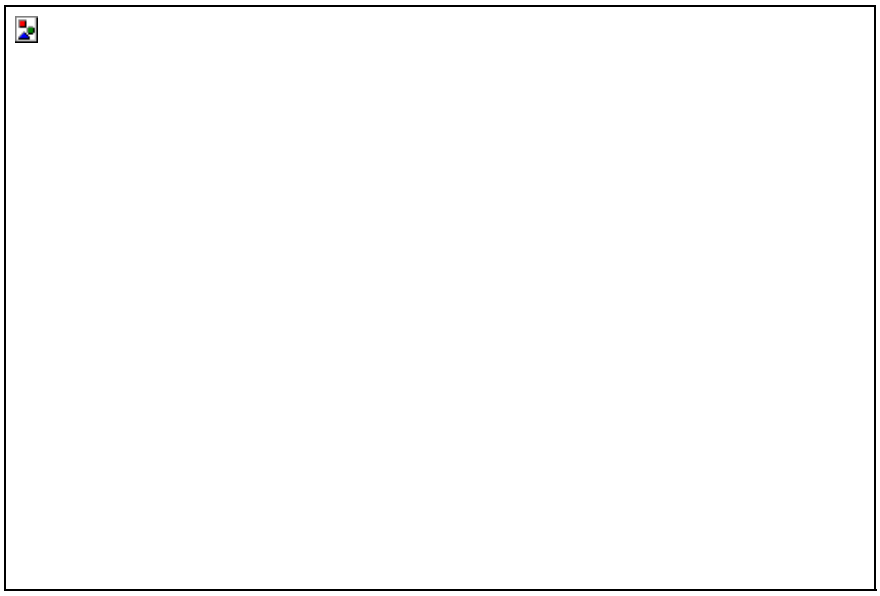


- Los pagos por e-mail cubren el segmento de servicio de pagos persona a persona (P2P)
- Su importancia radica en el volumen que el comercio persona a persona ha alcanzado (auctions)
- Implican la apertura de una cuenta no bancaria (habitualmente administrada por una compañía ajena al sector financiero, pero con fideicomiso bancario para administrar los fondos depositados)
- El usuario incorpora los fondos a la cuenta vía cheque, o habilitando que se realice una transferencia electrónica (EFT) desde una cuenta corriente bancaria
- Para el pago P2P el funcionamiento general es:
  - El pagador accede al sitio del servicio, y habilita el "envío" de un pago a una dirección de e-mail determinada
  - El destinatario del pago recibe un e-mail indicando que es receptor del mismo
  - Para efectivizar el cobro debe abrir una cuenta dentro del mismo servicio. Luego puede indicar la forma de percibir el pago (cheque, ATM, EFT a una cuenta bancaria, o dejarlo en la cuenta del servicio)
  - A los efectos del pago, los usuarios pueden cubrir el débito por depósito en la cuenta (con la instrumentación ya mencionada), o derivar el débito a una cuenta de crédito, ya que pueden relacionar una TC con la cuenta del servicio (a la que podemos llamar "e-cuenta")
- Uno de los mayores inconvenientes para los cobradores, es que la efectivización del pago suele tardar, si es que no se decide dejar el dinero en la e-cuenta, varios días en concretarse. Si no se tiene cuenta corriente, la demora es aun mayor
- El servicio es gratuito para los usuarios finales (consumidores) de USA. Existen modalidades de acuerdo con e-cuentas para empresas (uso no personal) que abonan un fee bajo. Incentivan la apertura de cuentas con bonus a los usuarios

- Existen límites de los montos a enviar y recibir, en particular cuando se opera con tarjetas de crédito. Éstas cobran un promedio de 2,5 % del importe de la operación al servicio, y éste cobra a clientes comerciales vendedores (no cuentas personales) un 1,9 % del monto transaccional
- No se permite recibir pagos sobre una cuenta de crédito
- El “spread” de pérdida con las empresas de TC intentan cubrirlo con la ganancia financiera que ofrece el dinero mantenido en las e-cuentas, el cual está depositado en un fondo. Las e-cuentas no generan intereses a los usuarios finales. Pay-Pal pierde plata con el pago derivado a una cuenta crédito, por eso incentiva el uso de vincular una cuenta corriente bancaria, a la e-cuenta
- Los principales indicadores del servicio de Pay-Pal son:
  - Creado en noviembre/99
  - Es el principal medio de pago de e-Bay, junto con el propio: Billpoint
  - Operan 4.5 millones de usuarios en USA. 120.000 transacciones por día. El volumen de usuarios crece a una tasa diaria de 20.000 (9.000/día a tres meses de su lanzamiento)
  - Goldman Sachs invirtió u$s 23 millones en segunda ronda de financiamiento, junto con un fondo vinculado a Idealab
  - Fusionada con su inicial más grande competidor, x.com, es la empresa más grande en el rubro
  - Alianza con ING en Europa
  - Posibiliadad de uso vía handheld devices y celulares (mobile)

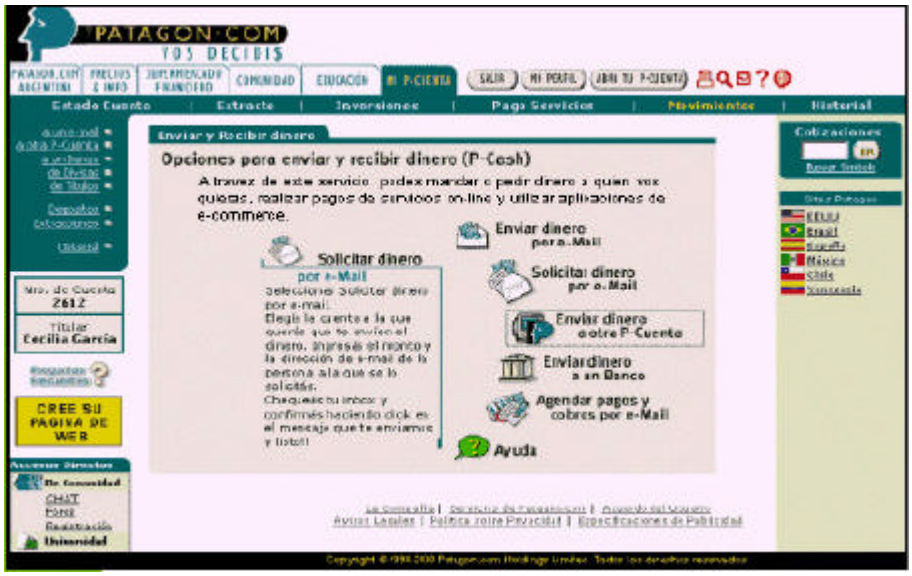
- Los competidores más fuertes son PayMe, adquirida por PayMyBills (a su vez adquirente de PayTrust), eMoneyMail, MoneyZap (Western Union), PayDirect (Yahoo, y banco de Canadá), ProPay, e-count

3.6 C2it (e-mail payments)



- C2it, es una iniciativa del Citibank en este rubro, permitiendo asociar el servicio con las cuentas corrientes del banco.
- El principal socio es AOL (AOL Quick Cash)
- Las características operativas son similares a Pay-Pal

3.7 P-cash - Patagon (e-mail payments)



- Con el respaldo del BSCH
- Esta cuenta puente no bancaria, que permite el depósito de valores varios (efectivo, cheques, inversiones), en $ y u$s, el uso en pago de servicios, permite también el ser utilizada para pago P2P instrumentado vía e-mail.
- Es gratuito, y la operatoria es análoga a la de Pay-Pal

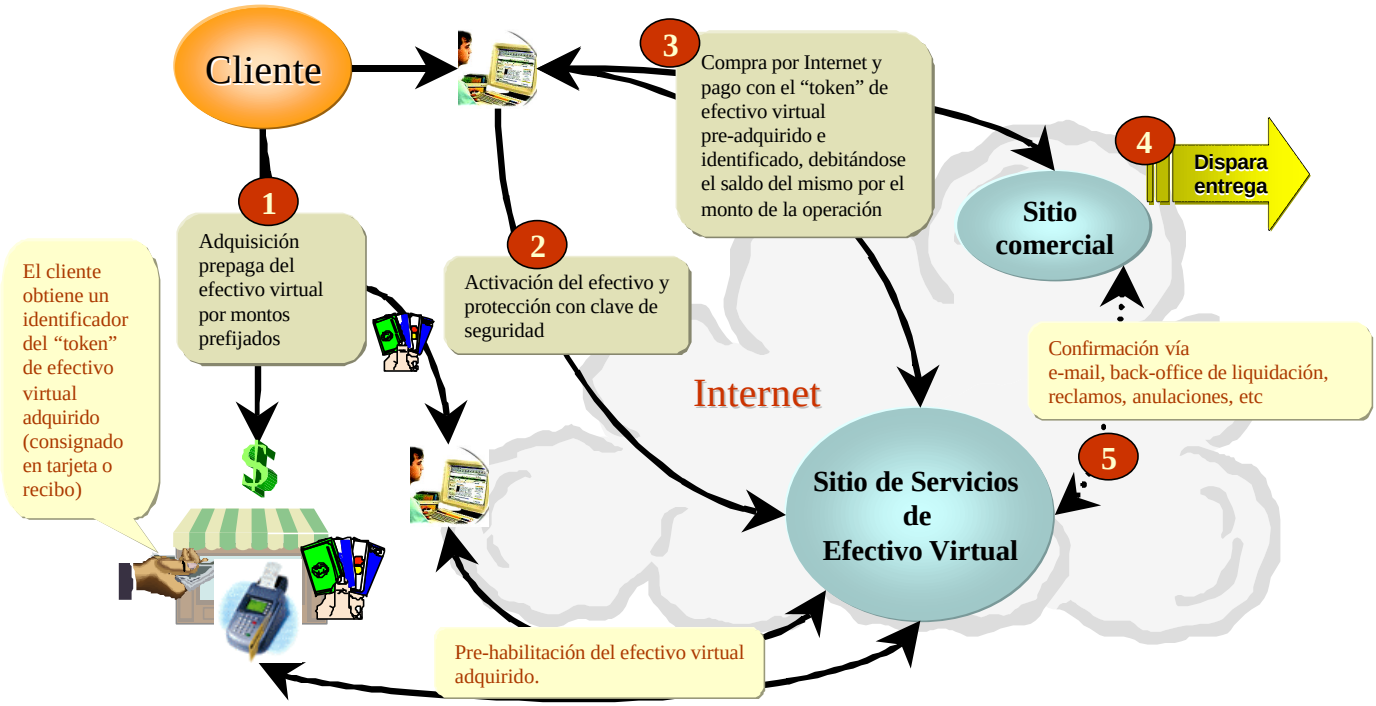
4 MODELOS OPERATIVOS OBSERVADOS

Del análisis de las soluciones presentadas en el punto precedente, surgen dos modelos conceptuales

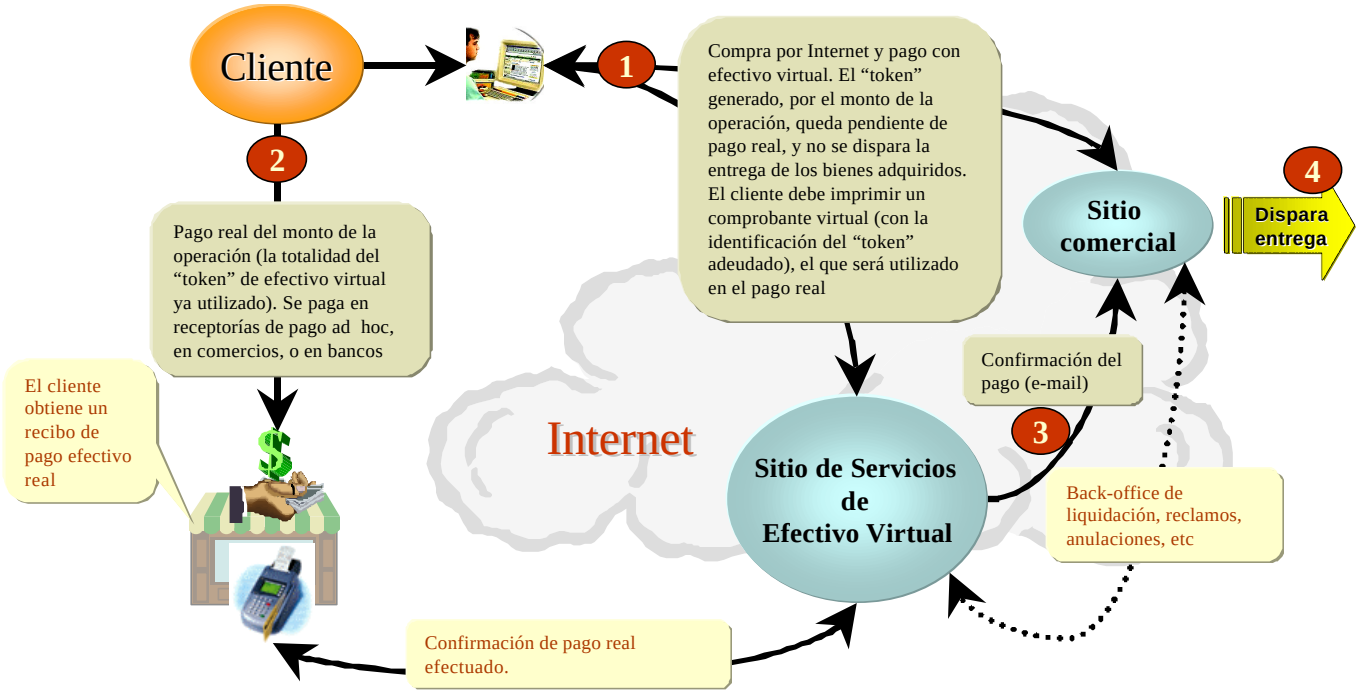
A) ***Con el prepago instrumento de pago "cargado" con un monto (adquisición de efectivo virtual).***

B) ***Con pago "real" del monto de la compra posterior a la realización de ésta (postpago), disparándose la entrega del bien cuando se confirma dicho pago real.***

4.1 Modelo de prepago (Casos: Internetcash y Novacash)



4.2 Modelo de postpago (casos: e-Pagofácil y Boleto Bancario)



4.3 Pros y Cons de los modelos

	Prepago	***Pospago***
Pros	• Permite manejar estructuras de monedero virtual, lo que lo hace reusable • La entrega del producto puede ser disparada al momento del pago por Internet • Con la operación de transferencias entre monederos, facilitaría el comercio C2C, (top del e-commerce actual – subastas) • El hecho de que sólo es aplicable a compras por Internet, orienta al público hacia dicho entorno de compras (punto de vista del e-merchant) • El pago de los bienes adquiridos es hecho de antemano	• No hay obligatoriedad de compra previa del efectivo. Un navegante podría decidir usarlo cuando accede a un sitio comercial, y no cuenta con otro medio de pago para aplicar (compra ocasional) • Puede utilizarse para el pago exacto de una compra
Cons	• Implica la adquisición previa del monedero por montos prefijados, lo que no lo hace apto para una compra compulsiva • Hay que administrar el tema de los saldos remanentes en monederos no ejecutados • El hecho de que sólo es aplicable a compras por Internet, orienta al público hacia dicho entorno de compras (punto de vista del cliente)	• Entrega disparada luego de la confirmación del pago • Debe manejarse vencimiento del pedido si no hay pago efectivo, luego de transcurrido un plazo • EL cliente debe acceder al sitio del comercio, o esperar notificación vía e-mail para saber que la entrega se disparó • No presenta posibilidad de reusabilidad ni recarga (monedero). No hay posibilidad de utilizarlos en el C2C • Puede generar numerosos pedidos de compra finalmente no abonados (trastorno administrativo alos comercios) • Mayor complejidad administrativa para los comercios • Cada vez que efectúa una compra, el cliente debe luego acceder a un local habilitado para abonar efectivamente la misma.

5 MODELO DE SOLUCIÓN PROPUESTO

5.1 Conclusiones sobre los modelos observados

Como conclusión de las ventajas y desventajas analizadas, se puede considerar mayor la viabilidad del modelo con prepago, básicamente por:

- Mayor versatilidad y extensibilidad de uso (C2C, recarga, pagos sobre monederos corporativos, mayor control del gasto por menores, uso como "gift certificate" – "vales de regalo")

- Mejor control y certeza de venta para los comercios (no hay uso por quien luego no pague), en relación al manejo de los pedidos no confirmados, el stock requerido, y la administración de entregas.

5.2 Predefiniciones de diseño

A los efectos de modelar la solución operativa del servicio estudiado, así como para definir el soporte tecnológico para la misma, se ha de tener en cuenta:

- La pre-existencia y disponibilidad de una red de servicios de cajeros automáticos, sobre la que será posible soportar parte de la funcionalidad del servicio

- La pre-existencia y disponibilidad de una red de terminales de POS (Point of Sale), utilizadas habitualmente para permitir el pago electrónico de ventas en comercios del mundo real, instrumentado con tarjetas de débito y crédito

- La existencia de un circuito preestablecido de compensación de fondos interbancarios; sobre el que sea posible soportar los débitos y créditos originados por las transacciones del servicio

- Se asume también la existencia de un público usuario de las redes de servicios precitadas. Los usuarios operan como tarjetahabientes de débito y/o crédito sobre dichas redes de servicios, interactuando transaccionalmente con las instituciones bancarias titulares de las tarjetas de débito o con las administradoras de tarjetas de crédito.

5.3 Conceptos básicos del modelo

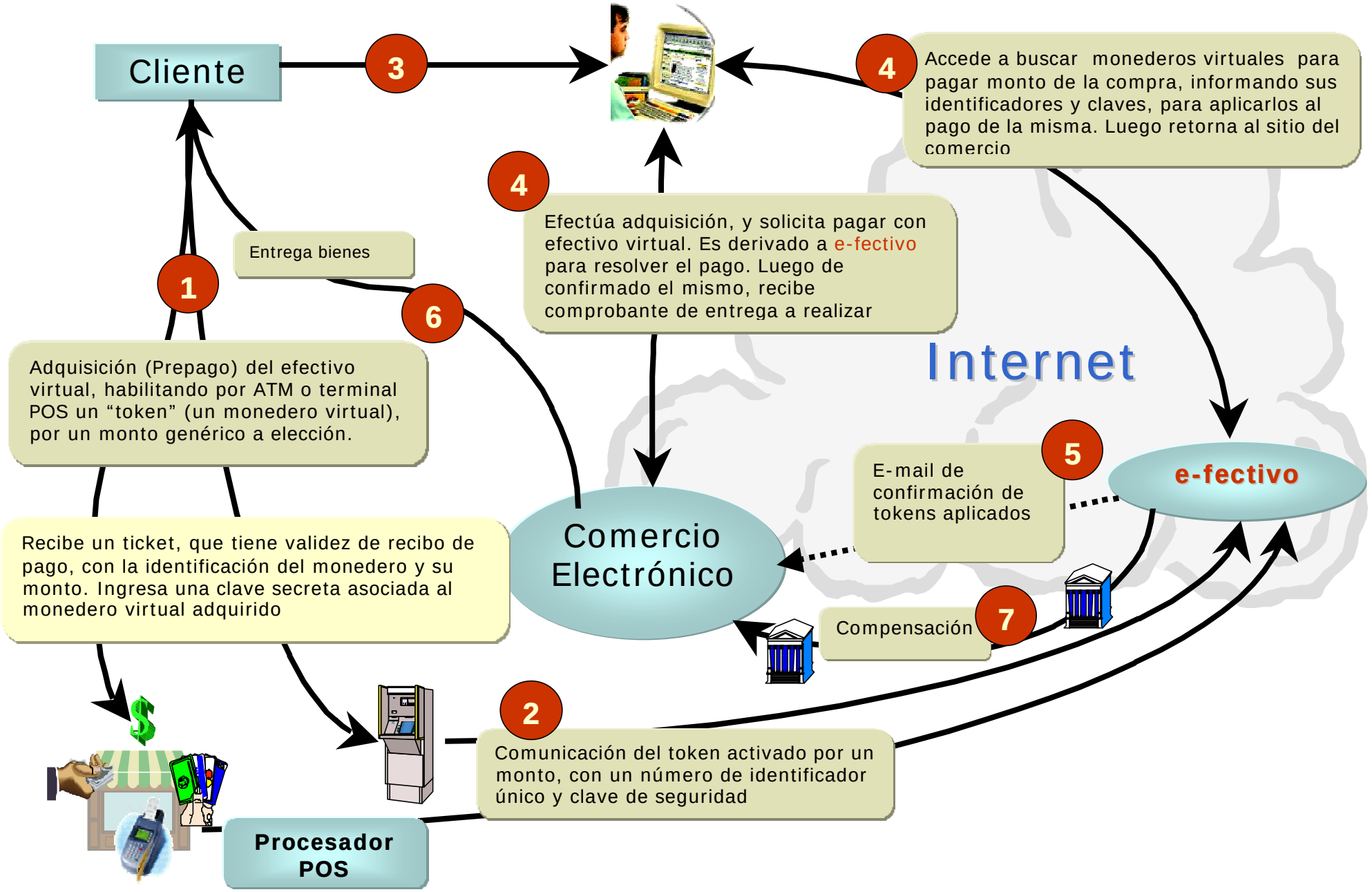
El modelo de servicio se caracteriza por conformar las siguientes características operativas:

- *Constituye un repositorio informatizado, que registra el saldo representativo de un monto de dinero.*
- *Es adquirible a través de las redes de servicios informáticos ya mencionadas (ATM y POS), contra pago en efectivo, por débito en cuenta bancaria, o por débito en cuenta de crédito; por un monto equivalente al saldo a contener registrado. Asimismo, puede ser adquirido desde algún servicio instalado en la Web, que habilite la realización de débitos en las cuentas precitadas El monto de dinero "contenido" es prepagado.*
- *Dicho saldo registrado puede ser descargado (menguar el valor registrado) cuando es utilizado en Internet, en circunstancias de la adquisición, y pago, de bienes y servicios ofrecidos por comercios electrónicos a través de dicha red pública.*
- *Puede habilitar su recarga u operar transferencias a otro repositorio similar, a los efectos de habilitar el pago persona a persona*
- **Puede visualizarse como un monedero electrónico de efectivo (e-wallet/e-purse) , prepago, para efectuar pagos en el entorno tecnológico de Internet**

A lo largo del desarrollo que se presenta en este estudio, se delinearán otras características que otorgan al modelo conformidad con aspectos de seguridad para los actores ivolucrados en el proceso transaccional (usuario final, comercio electrónico, banco, y procesador del servicio), así como con los atributos propios del dinero (reserva de valor, transferibilidad, unidad de cuenta).

En relación con el atributo "anonimato", éste sólo se cubrirá parcialmente. Consecuentemente, el servicio ofrece una base de trazabilidad transaccional del efectivo usado, lo que habilita -en parte-, la identificación de quien adquiere o utiliza el monedero virtual.

A continuación se despliega un gráfico general explicativo del modelo del servicio


Cliente
3
4
Accede a buscar monederos virtuales para pagar monto de la compra, informando sus identificadores y claves, para aplicarlos al pago de la misma. Luego retorna al sitio del comercio
4
Efectúa adquisición, y solicita pagar con efectivo virtual. Es derivado a e-fectivo para resolver el pago. Luego de confirmado el mismo, recibe comprobante de entrega a realizar
Entrega bienes
1
6
Adquisición (Prepago) del efectivo virtual, habilitando por ATM o terminal POS un “token” (un monedero virtual), por un monto genérico a elección.
Internet
5
E-mail de confirmación de tokens aplicados
e-fectivo
Comercio Electrónico
Recibe un ticket, que tiene validez de recibo de pago, con la identificación del monedero y su monto. Ingresa una clave secreta asociada al monedero virtual adquirido
Compensación
7
2
Comunicación del token activado por un monto, con un número de identificador único y clave de seguridad
Procesador POS

6 DESCRIPCIÓN OPERATIVA DE LA SOLUCIÓN

6.1 La adquisición del efectivo virtual

- Se contemplan 2 posibles vías alternativas de adquisición:
- Desde la red de ATMs, para usuarios de tarjetas de dicha red
- Desde una terminal POS de los servicios instalados por los emisores de TC, o a través de otras soluciones corporativas (supermercados, estaciones de servicio, etc.). Para todo usuario

6.2 Desde un ATM

- El tarjetahabiente accede a un ATM para adquirir un monedero virtual.
- Se identifica ante la red con el esquema estándar (tarjeta de débito de una entidad adherida y PIN).
- Selecciona la operación de compra de monedero virtual de un menú, y el monto del mismo de una grilla de valores prefijados (P ej: $ 20, $ 50, $ 100, $ 200).
- Paga la adquisición del monedero, debitando el cargo de una cuenta bancaria elegida.
- Ingresa una clave de protección (8 dígitos) para el monedero virtual, luego selecciona y confirma la cuenta a debitar por el monto de monedero seleccionado.
- Recibe un ticket de operación con los datos identificatorios del monedero (12 dígitos alfanuméricos); dicho ticket es válido como comprobante de pago.

6.3 Desde la POS de un comercio

- El cliente accede a un comercio provisto de terminal POS. Esta soporta una transacción de compra de monedero virtual. La instalación de POS debe incluir dispositivo PinPad.
- En función del medio de pago elegido, TD, TC, o efectivo real, la aplicación de la terminal permite:

Operando con tarjeta de débito

- Operando con su tarjeta de débito con la forma habitual de identificación se accede a un menú-grilla desde donde se elige un importe de monedero de un conjunto prefijado de valores posibles.
- Ingresa una clave de protección (8 dígitos) para el monedero virtual a través del dispositivo PinPad.
- Luego la terminal se conecta, para efectuar el pago, procesador adquirente de la transacción (terminal driver), y éste remite el pedido de autorización a la red autorizadora de la tarjeta.
- Se paga la adquisición del monedero, debitándose el cargo de una cuenta bancaria
- Recibe un ticket de operación con los datos identificatorios del monedero (12 dígitos alfanuméricos), que es válido como comprobante de pago.
- La transacción sólo es válida en la modalidad “on line”, lo que es exigido para las tarjetas de débito. Un número de monedero es generado por el procesador de e-fectivo, y es impreso en el ticket emitido.

Operando con tarjeta de crédito

- Operando con su tarjeta de crédito con la forma habitual de identificación se accede a un menú-grilla desde donde se elige un importe de monedero de un conjunto prejifado de valores posibles.
- Ingresa una clave de protección (8 dígitos) para el monedero virtual a través del dispositivo PinPad.
- La terminal se conecta luego al Host autorizador de la TC, transmitiendo los datos capturados.
- Se paga la adquisición del monedero, debitándose el cargo de la cuenta crédito asociada a la tarjeta.

- El Host del autorizador informa cada transacción, en forma “on line”, al procesador de e-fectivo para activar los monederos adquiridos.
- Recibe un ticket de operación con los datos identificatorios del monedero (12 dígitos alfanuméricos), que es válido como comprobante de pago.
- La transacción sólo puede ser efectuada “on line” dado que el número de monedero es generado por el procesador de e-fectivo.
- Un número de monedero es generado por el procesador de e-fectivo, y es impreso en el ticket emitido.

Abonando con efectivo real

- Los usuarios no bancarizados pueden operar sin necesidad de identificarse.
- En tal caso, se permite acceder directamente al menú-grilla desde donde se elige un importe de monedero de un conjunto prejifado de valores posibles.
- Ingresa una clave de protección (8 dígitos) para el monedero virtual a través del dispositivo PinPad.
- La terminal se conecta con el procesador de e-fectivo para enviar y registrar la adquisición del monedero.
- La transacción sólo puede ser efectuada “on line” dado que el número de monedero es generado por el procesador de e-fectivo.
- Se paga la adquisición del monedero en efectivo real.
- Recibe un ticket de operación con los datos identificatorios del monedero (12 dígitos alfanuméricos), que es válido como comprobante de pago.
- Un número de monedero es generado por el procesador de e-fectivo, y es impreso en el ticket emitido.

Otros aspectos operativos

- Los ingresos del PIN (cuando correspondieran), y de la clave de protección del monedero, son realizados por el cliente desde el PinPad, así como la selección del importe de monedero (y/o su confirmación). El resto de la operación es llevada a cabo por el operador del comercio.
- Los tickets emitidos contemplan la información que identifica al monedero adquirido, a su monto, y a la forma de pago elegida en la adquisición.

6.4 Luego de la adquisición del monedero...

- En el sitio de e-fectivo queda habilitado un monedero de efectivo virtual, por un valor (devenido en saldo del monedero) igual al elegido por el usuario. El monedero ya está disponible para su aplicación en pagos vía Internet.
- Dicho monedero tiene asociada una clave de seguridad, sólo conocida por el usuario que, vía ATM o POS, adquirió el monedero.
- El sistema mantiene asociados al monedero, datos que permitan determinar la forma de adquisición y el medio de pago utilizado. En el caso de TDs o TCs es el número de tarjeta del adquirente. Esto puede permitir el administrar reclamos en la obtención vía ATM o POS.

6.5 La realización de la compra

- Cualquiera sea la forma de adquisición con la que el cliente hubiera operado para obtener un monedero virtual, los conceptos operativos que se enumeran a continuación resultan igualmente válidos.
- Una vez que adquirió el monedero virtual, el usuario accede por Internet a un comercio virtual que permite el pago de las compras mediante e-fectivo.
- La gestión de presentación y selección de productos, corresponde a la modalidad de operación que la aplicación Web del e-merchant (comercio virtual) despliegue.
- Una vez seleccionado el producto a adquirir, y determinado el checkout por parte del cliente, éste debe seleccionar la opción de pago vía e-fectivo.
- Al seleccionar la opción de pago con e-fectivo, el usuario es redireccionado al sitio de pagos de dicho servicio. Junto con la redirección, se incluyen en el mensaje los datos de la compra, la identificación del comercio, y otros datos complementarios. Dicho paquete de información se conforma según una estructura de sobre digital, cubierto criptográficamente con el estándar PKCS #7.
- Al acceder al sitio de e-fectivo, el cliente debe seleccionar el monedero virtual a aplicar.
- Para esto, debe informar el número de monedero consignado en el ticket de adquisición obtenido vía ATM o POS, e ingresar la clave de seguridad que el mismo usuario asignó al monedero en dicha oportunidad.
- El sistema, con el monto de la compra conocido e identificado el monedero a aplicar, verifica el saldo disponible del mismo y efectúa el débito, si esto último resulta posible.
- En el caso de que el saldo no cubra el monto de la operación, el sistema solicita al usuario la utilización de otro monedero, para lo que el cliente debe cursar el mismo procedimiento de identificación (Nro de monedero y clave de seguridad).
- En el caso de que ningún monedero disponga de fondos suficientes, el sistema facilita la transferencia de saldos (total o parcial) de un monedero a otro. Esta operación se realiza con las mismas consideraciones de identificación ya expuestas.
- Otra alternativa, cuando el saldo de un monedero no cubre el monto de la operación, es habilitar el uso de varios de éstos

aplicados a un mismo pago; operando un ciclo de identificación como el ya mencionado precedentemente.

- Aplicado el pago, e-fectivo emite un comprobante virtual de pago realizado, consignando el saldo del monedero utilizado, el número de transacción de pago, el monto debitado, la identificación del comercio.
- Luego, e-fectivo devuelve al cliente al sitio de compra, junto con los datos de la transacción aprobada (análogos a los del comprobante virtual), en una estructura de sobre digital.
- El comercio, a su vez, puede emitir un comprobante virtual, para testimoniar que el circuito de compra y pago se ha cerrado satisfactoriamente, y anunciar la realización de la entrega del producto adquirido.
- El sitio de e-fectivo complementa la confirmación de la operación, tanto hacia el cliente como hacia el comercio, con el envío de e-mails.

6.6 Luego de la compra

- e-fectivo inicia el proceso de liquidación al comercio y la compensación de la operación.
- e-fectivo permite la consulta de las últimas operaciones efectuadas para cada monedero.

6.7 Aspectos operativos adicionales

- El sitio de e-fectivo no exige registración de usuarios, respetando el uso anónimo del efectivo electrónico.
- La identificación está basada en el conocimiento del número identificatorio del monedero, asignado por el servicio, y la clave de seguridad, asignada por el usuario adquirente desde un ATM o POS.
- Un monedero virtual no es nominativo, por lo que es naturalmente transferible y no se identifica con el poseedor ocasional. El solo conocimiento del número identificatorio, y especialmente de la clave de seguridad, permite a cualquier individuo el operar dicho medio de pago.
- El sitio provee la posibilidad de consultar los últimos movimientos operados sobre un monedero.
- El sitio provee la posibilidad de cambiar la clave de seguridad de un monedero.
- A los efectos de realizar transferencias entre monederos sólo es requerida la clave de seguridad del monedero debitado.
- Los monederos soportan saldos fraccionarios.
- El sistema permite a un usuario el anular o bloquear un monedero virtual, si el poseedor conoce los atributos de identificación requeridos por el sistema.

7 REQUISITOS CRÍTICOS DEL MODELO

Dos aspectos resultan críticos a los fines de concretar la especificación de este modelo de solución para los pagos electrónicos por Internet:

7.1 Cobertura de la seguridad

- Los comercios disponen de las seguridades requeridas para operar la redirección al sitio de e-fectivo, y este opera de la misma forma para devolver al cliente, con el pago aprobado, al sitio del comercio En ambos casos se utiliza criptografía de clave pública (estándar PKCS #7), para cubrir integridad y autenticación de servidores, y de clave privada, para conformar requerimientos de confidencialidad. El contenido del sobre digital incluye elementos protegidos, que dan vigencia y caducidad a una sesión de intercambio de información entre sitios.
- Las seguridades de las claves (PIN y clave de seguridad de monedero), tanto en terminales POS como en ATMs, se cubren con la infraestructura de seguridad que regularmente soportan y operan dichas plataformas. En razón de que estas plataformas constituyen redes privadas, el riesgo de exposición al fraude informático se encuentra reducido. A esto se suma que –en ambos casos- las claves se procesan en base a criptografía sustentada en hardware (cajas criptográficas), por lo que en ningún momento las claves se exponen en forma “no cifrada” sobre ningún procesador “abierto” del sistema, excepto en dicho hardware criptográfico. El almacenamiento de las claves en los procesadores centrales también verifica su no exposición en modo “no cifrado”.
- Toda conexión de usuarios (de Internet) al sitio de e-fectivo se establece contemplando que la misma sea segura. Para esto se realiza implementando el protocolo SSL (Secure Socket Layer), sobre la conexión TCP/IP, el cual garantiza el establecimiento de un canal criptográfico seguro para el intercambio de datos que ocurre entre el navegador del usuario y el servidos de e-fectivo.
  Asimismo, permite al usuario reconocer que se ha conectado con un sevidor seguro; pudiendo el mismo verificar el certificado digital del servidor, que es emitido por una entidad certificadora reconocida. El ingreso de la clave de protección del monedero, en su tránsito desde el navegador del usuario al servidos de e-fectivo, está protegida por este canal seguro.

7.2 Aspectos legales (*a desarrollar*)

8 ANÁLISIS DEL MERCADO

8.1 Navegantes por rango de edades

A lo largo de este capíulo se analizará el potencial mercado de usuarios, su cuantificación y caracterización sociodemográfica para aplicar el modelo de solución en la República Argentina.

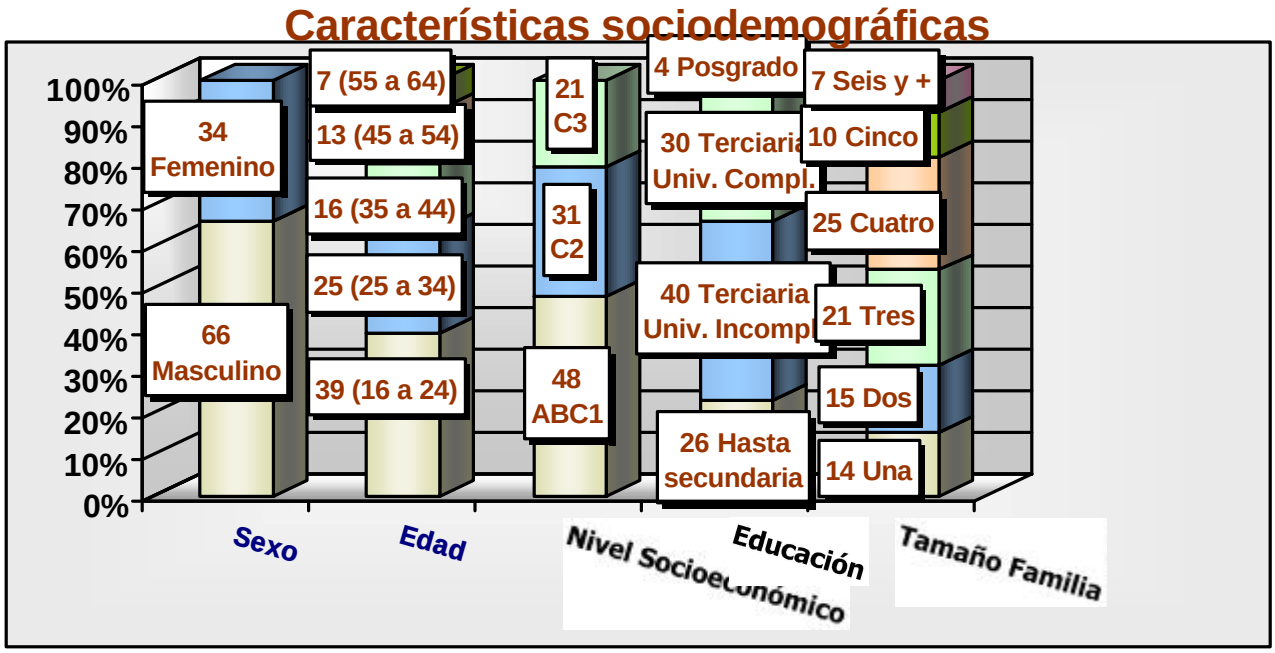
Estudios de reciente factura sobre la composición sociodemográfica de los navegantes de Internet en el mercado local, han arrojado los resultados que se exponen en el gráfico G1-“Características sociodemográficas de los navegantes de Internet en Argentina” .

Del citado gráfico surge, como consideración de interés para este trabajo, que existe un 39 % de los navegantes (indicados en la serie de edades) cuya edad oscila entre los 16 y 24 años.

Si se analiza el índice de bancarización en el país, el cual alcanza a un 27 % de la población (Revista Mercado, Juliio 2000), se observa que tiene una nula o muy baja incidencia en el rango de edades citado. Las razones se asientan en la imposibilidad legal de disponer cuentas bancarias, por parte de menores de edad, así como de la baja disponibilidad de medios de pago tradicionales (distintos del efectivo) en las franjas juveniles de reciente inserción en el mercado laboral.

Esto pone de manifiesto la existencia de un conjunto de usuarios potenciales, constituyendo casi el 50 % del conjunto poblacional menor de 45 años afecto a la navegación por Internet (que constituyen, a su vez, el 80 % de los navegantes totales), que no disponen de un instrumento de pago, ágil y seguro, para transaccionar comercialmente en la Web.

G1-"Características sociodemográficas de los navegantes de Internet en Argentina"



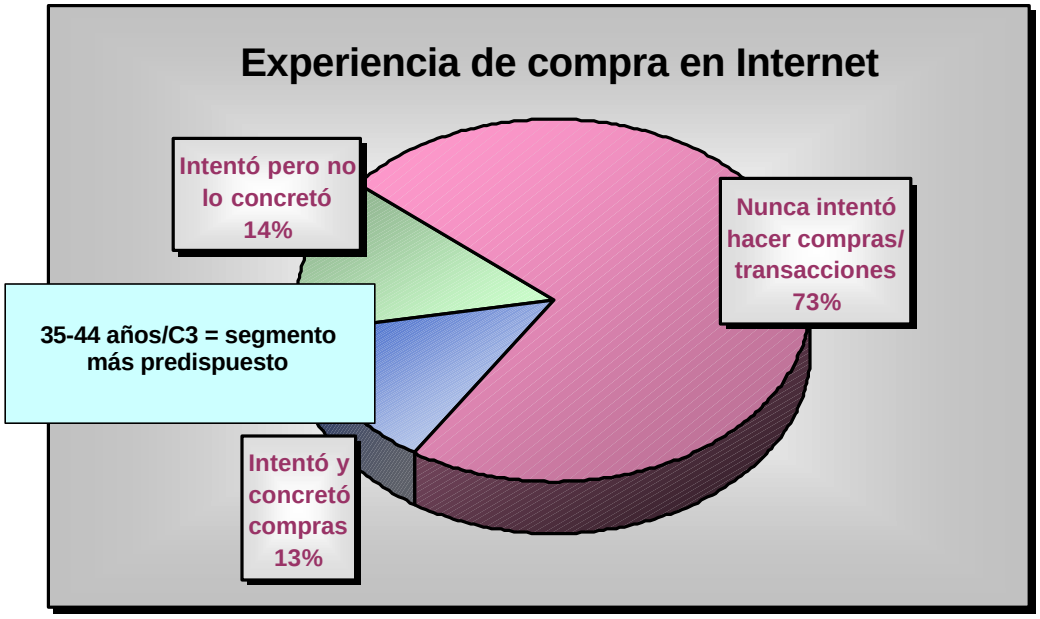
Fuente: Kleinman Research – Año 2000

8.2 El hábito de compra y pago por Internet

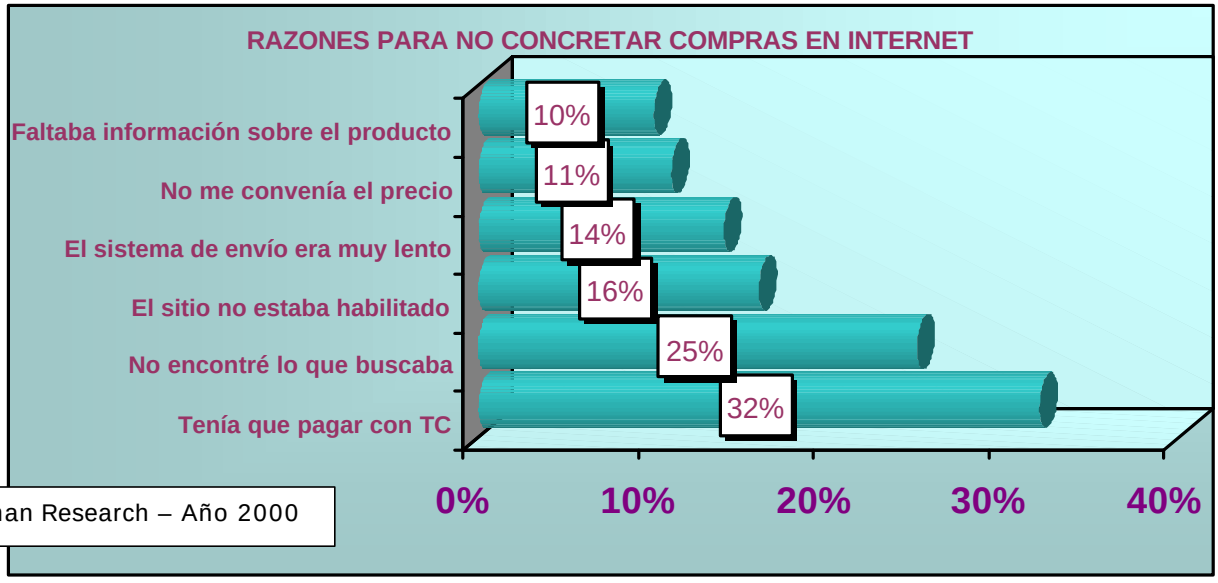
A los efectos de analizar el comportamiento de los usuarios respecto del uso de los medios de pago tradicionales, adecuados tecnológicamente para su utilización en la Web (entiéndase tarjetas de débito y crédito), se ha podido observar importantes niveles de reticencia.

Según puede verse en los gráficos, G2-"Experiencia de compras en Internet" y G3- "Razones para no concretar compras en Internet", la actitud del público ante la instancia de adquisición de bienes y servicios a través de Internet. Los datos tomados en consideración se refieren al mercado argentino.

G2-"Experiencia de compras en Internet"



G3- "Razones para no concretar compras en Internet"



Fuente: Kleinman Research – Año 2000

A partir de esta realidad, constatada por distintos estudios análogos al referenciado en este trabajo, puede concluirse que el nivel de concreción de compras y pagos sobre Internet es manifiestamente bajo (13 %) (G2).

Complementariamente pueden observarse, en el gráfico G3 referenciado, los distintos motivos genéricamente aducidos por el público para no concretar la compra o manifestarse remisos a seguir adelante en algún punto de su gestión.

A los efectos de este trabajo se rescatará únicamente el porcentual referido al causal que involucra la utilización de una tarjeta de crédito para el pago. Los restantes motivos presentados no hacen al objetivo de este estudio, dado que no inciden en la gestión del pago de los bienes y servicios adquiridos.

Se concluye de este análisis que la frecuencia de abandono en la consecución de la compra por Internet, pareciera asentarse -en un 32 % de los casos- en la renuencia de utilizar el medio de pago "tarjeta de crédito", o en la circunstancia de que el mismo constituye el único instrumento posible de utilizar.

Las condiciones operativas de las tarjetas de crédito en Internet –el nivel de recurrencia de operaciones fraudulentas en Internet y los costos para el comercio - traen a la luz el sustento de las razones expuestas.

El FBI, a través del NIPC (National Infraestructure Protection Center), denunció (Marzo 2001) que más de 1 millón de números de tarjetas habían sido "robados" en alrededor de 40 comercios de Internet durante los últimos meses del año 2000 y principios de 2001. Asimismo, Meridien Research menciona que el monto de fraudes cometidos en Internet alcanzó en dicho año los 1.600 millones de dólares.

Según se expresa en un informe de la Unión Europea: "En 2000, el fraude con tarjetas de crédito en la Unión Europea aumentó un 50%, y el volumen de operaciones ilegales alcanzó los 600 millones de euros. En buena medida a causa de las transacciones online, que si bien suponen apenas un 2% de la utilización que se realiza de las tarjetas de crédito, provocan la mitad de las quejas de los usuarios".

Según el Gartner Group, sobre datos del año 2000, el fraude con tarjetas de crédito en Internet es 12 más grande que el ocurrido en el mundo real, los comercios virtuales pagan intereses un 66 % más altos, y generalmente son castigados con altos contracargos ocasionados en las disputas y el desconocimiento de las transacciones por parte de los usuarios (cuando las compañías de tarjetas de crédito, generalmente, absorben dichas pérdidas en el mundo real).

Como resultado del análisis antes expuesto, puede concluirse en la existencia de otro segmento de usuarios potenciales afectos a utilizar un medio de pago que resuelva la problemática de inseguridad transaccional en Internet, objetiva y subjetivamente concebida.

8.3 Definición del perfil de usuario del servicio

A partir del análisis del mercado, expresado en los puntos precedentes, es posible concluir:

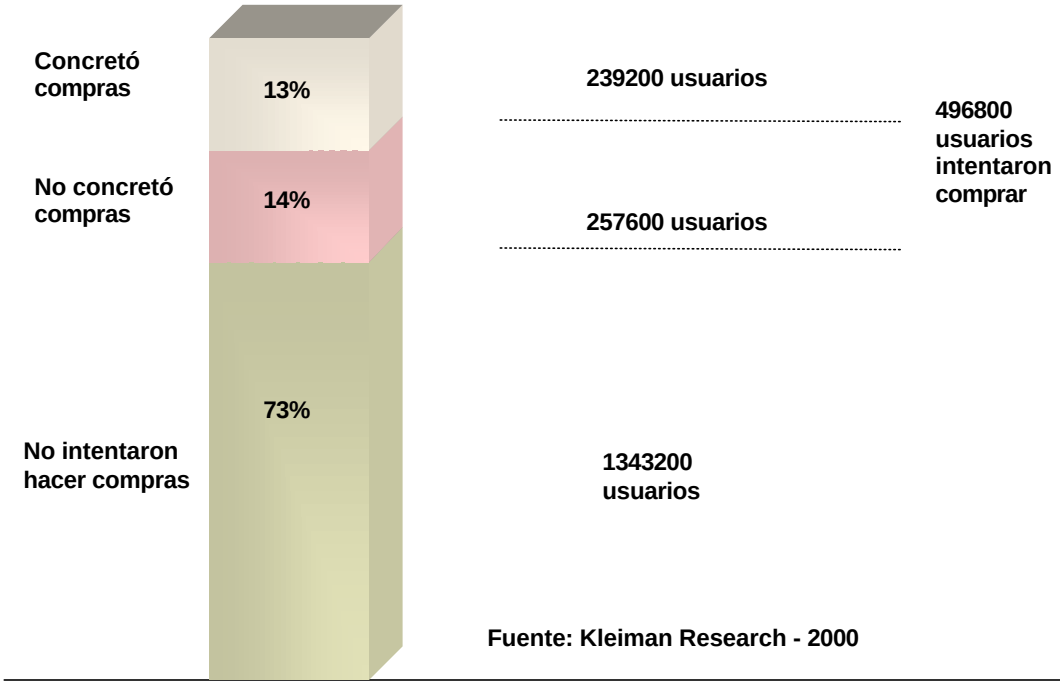
- Existe un segmento de consumidores no atendido, el cual está compuesto por:

  - *Jóvenes, que no pueden acceder a los medios de pagos tradicionales. (No bancarizados) .*
  - *Adultos renuentes a introducir la tarjeta de crédito, para pagar operaciones de adquisición de bienes y servicos, en comercios que soportan la comercialización de los mismos a través de Internet*

Tomando como base el volumen de usuarios de Internet proyectado para fin del año 2001 (Fuente: Revista Mercado) se estima un volumen de 1.840.000 navegantes, se aplicarán los porcentajes surgidos del análisis desarrollado en puntos precedentes.

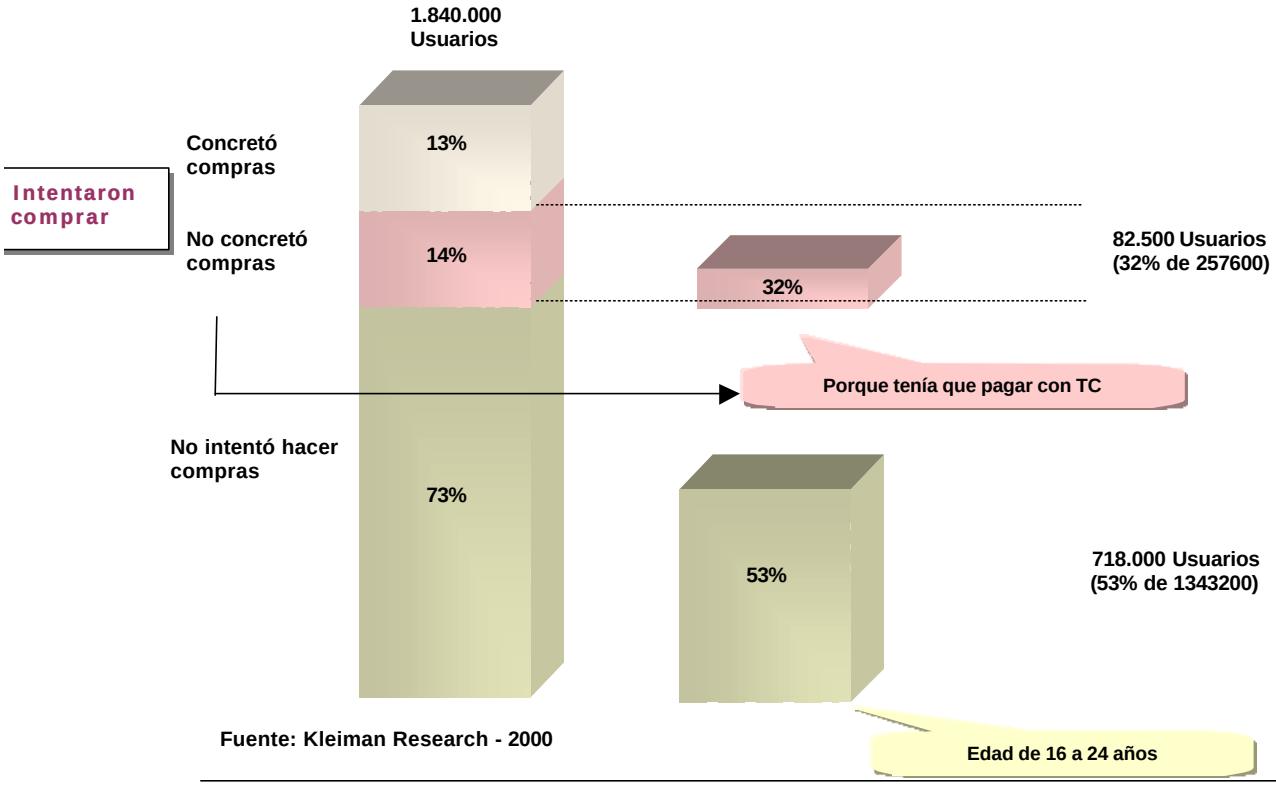
Los gráficos expuestos a continuación reflejan el cálculo considerado para estimar los volúmenes de público que accedería al servicio de pagos a diseñar. Sobre la base de los volúmenes citados se harán las proyecciones correspondientes al negocio.

8.4 Cantidad de usuarios según concreción de compras



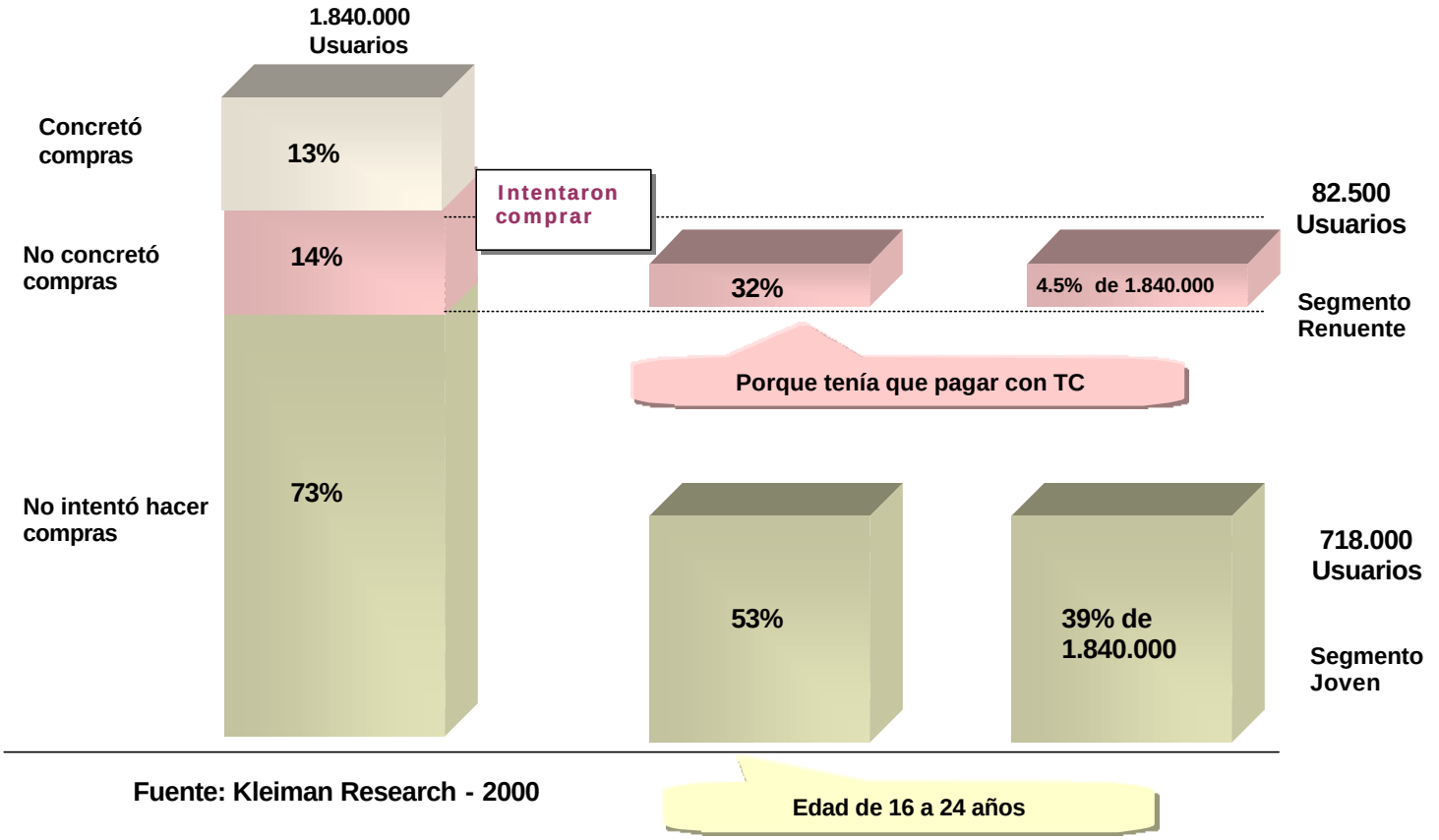
Fuente: Kleiman Research - 2000

8.5 Número de usuarios como % del segmento



Fuente: Kleiman Research - 2000

8.6 Número de usuarios como % del total



Fuente: Kleiman Research - 2000

9 ENFOQUE DE MARKETING

9.1 Misión:

- Ser un medio de pago en efectivo reconocido, para las operaciones comerciales realizadas a través de Internet.

- Orientado en su primera fase al consumo del público joven, y a los consumidores de Internet con renuencia al uso de la tarjeta de crédito en dicho medio.

9.2 Objetivos:

Cualitativos:

- Lograr una imagen reconocida como medio de pago electrónico fácil de usar, seguro, y anónimo.

Cuantitativos:

- Alcanzar xxxx transacciones (tokens vendidos) el primer año, nnnn en el 2do. Año, y zzzzz en el 3er. año.

- Incorporar 10 comercios líderes en e-commerce en una primera etapa.

9.3 Posicionamiento

E-fectivo será sinónimo de facilidad, seguridad, anonimato y privacidad para realizar una operación de pago en Internet.

9.4 Factores de éxito

- Lograr una amplia cobertura de negocios que expendan tokens.
- Hacer que el público perciba a los ATMs como expendedores de tokens eficientes, de alta disponibilidad y sencillos de ser ubicados.
- Incorporación de comercios líderes en ventas por Internet, al sistema de pago.
- Usar eficientemente los recursos asignados a publicidad para lograr los objetivos de penetración de mercado definidos.
- Adecuada publicidad para captar clientes.
- Maximizar la relación ($ invertidos en publicidad)/(% segmento capturado).

9.5 Descripción de la demanda - Segmento objetivo I

Hipótesis:

- No son compradores vía Internet debido a que no se encuentran bancarizados:
  - 39 % de la poblacion de Internautas.
  - Jovenes de entre 16 a 24 años, ambos sexos.
  - Características de su actitud de compra: adolescentes con una actitud proclive a la compra compulsiva, fuerte inclinación por la música.
  - Las compras estan basadas en la adquisición de CD´s.
  - Ticket promedio X Frecuencia de compra: ## $ x ## Compras / año.

9.6 Descripción de la demanda - Segmento objetivo II

Hipótesis:

- Personas que no compran en Internet debido a la inseguridad que representa usar tarjetas de Credito :
  - 14% de la población de Internautas, del cual un 32 % no lo hace por razones de renuencia al uso de la tarjeta (inseguridad), por lo tanto representan un 4,5% del universo muestral
  - Personas de entre 25 a 55 años, ambos sexos
  - Caracteristicas de su actitud de compra: Mantienen una actitud conservadora, debido a la cual no exponen su Tarjeta de Crédito en Internet
  - Las compras están basadas en libros, CD´s y regalos para terceros
  - Ticket promedio X Frecuencia de compra: ##$ x ## Compras / año.

9.7 Supuestos para la planificación

	Año 2001	Año 2002	Año 2003
Segmento Jóvenes	Importe promedio de compras: $ 20 Cantidad de compras por mes: 1 (desde julio/01) Penetración inicio: 0,5% Penetración Fin: 7 %	Importe promedio de compras: $ 20 Cantidad de compras por mes: 1 Penetración inicio: 7 % Penetración Fin: 15 %	Importe promedio de compras: $ 20 Cantidad de compras por mes: 1 Penetración inicio: 15 % Penetración Fin: 26 %
Segmento Renuentes	Importe promedio de compras: $ 30 Cantidad de compras por mes: 1 (desde julio/01) Penetración inicio: 3 % Penetración Fin: 12 %	Importe promedio de compras: $ 30 Cantidad de compras por mes: 1 Penetración inicio: 13 % Penetración Fin: 24 %	Importe promedio de compras: $ 30 Cantidad de compras por mes: 1 Penetración inicio: 25 % Penetración Fin: 36 %
Comisión por vta (al comercio)	4 % del importe de compra	Idem 2001	Idem 2001
Transferencias de tokens	% de tokens que transfieren: 10 % Cargo por transferencia al cliente: $ 1	% de tokens que transfieren: 10 % Cargo por transferencia al cliente: $ 1	% de tokens que transfieren: 10 % Cargo por transferencia al cliente: $ 1
Tokens $ vencidos	% de tokens que vencen: 1 % (en venta de tarjetas prepagas telefónicas es del 3 %)	Idem 2001	Idem 2001
Cargos a comercios	Fee mensual: $ 50 Cargo de U/vez (ingreso): $ 1.000	Idem 2001	Idem 2001
Vendedores de tokens	Comisión a pagar: $ 0,70/transacción	Idem 2001	Idem 2001

9.8 Cuantificación del Ingreso

	A 2001	*A 2002*	*A 2003*
Compradores jóvenes			
Total comis. anual compras	121.958	956.982	2.268.578
Total anual tokens usados	101.632	797.485	1.890.482
Compradores renuentes			
Total comis. anual compras	39.377	275.165	591.163
Total anual tokens usados	32.814	229.304	492.636
Total ingreso por comisiones	161.335	1.232.147	2.859.741
Total tokens vendidos	134.446	1.026.789	2.383.117
Total anual transferencias	13.445	102.679	238.312
Total anual tokens vencidos	40.334	308.037	714.935
Ingreso incorporación empresas			
Total anual fee a comercios	11.850	58.100	94.500

9.9 Cuantificación de Gastos e Inversiones

Concepto	Total año 1	Total año 2	Total año 3	PROYECTO
COSTOS				
Amortizaciones	50.000	50.000	50.000	150.000
Leasing	0	0	0	0
Mantenimiento	36.000	54.000	54.000	144.000
Insumos	0	0	0	0
Telecomunicaciones	0	0	0	0
TOTAL COSTOS	86.000	104.000	104.000	294.000
GASTOS				
Personal	75.000	130.000	130.000	335.000
Marketing	530.000	500.000	500.000	1.530.000
Infraestructura	8.444	14.468	28.031	50.944
Honorarios	140.000	0	0	140.000
Viajes y representación	0	0	0	0
Capacitación	0	0	0	0
Comisiones pagadas	94.112	718.753	1.668.182	2.481.047
TOTAL GASTOS	847.556	1.363.220	2.326.213	4.536.990
OVERHEAD	93.356	146.722	243.021	483.099
TOTAL COSTOS Y GASTOS	1.026.912	1.613.942	2.673.235	5.314.089

9.10 Enfoque de Marketing – Ugrades del servicio

Este servicio ofrecido primariamente en su forma básica podría crecer en varias direcciones :

- Vales de regalo (gifts certificates) : para ofrecer el efectivo virtual como un regalo para ocasiones especiales.
- Ventas de tokens por Internet :hacia otros países de latinoamérica.
- Transferencia entre particulares : permitir pagos entre individuos a través de transferencias entre monederos.
- Modalidad pos-pago : comprar y pagar posteriormente.

10 ENFOQUE DE COMERCIOS

10.1 Adhesión de comercios vendedores de tokens

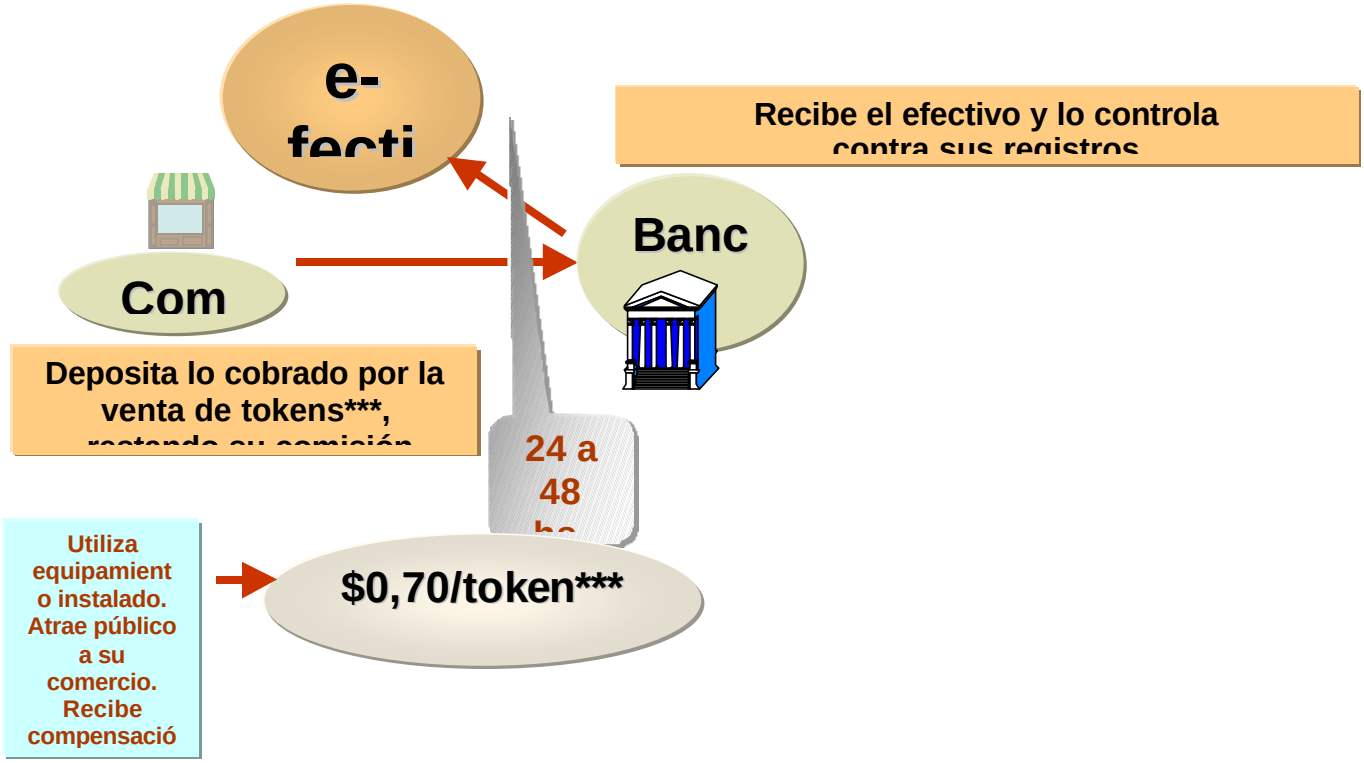
Características que deben tener :

- Asiduamente visitadas por el público objetivo.
- Distribución Geográfica acorde al target.
- Cadena de negocios con casa central y puntos de venta con información centralizada para facilitar la gestión de cobranza.
- Deben poseer sistema de POS propio.
- Deben tener un sitio de venta en la Web, para promover este medio de pago más beneficioso que las TC/TD.

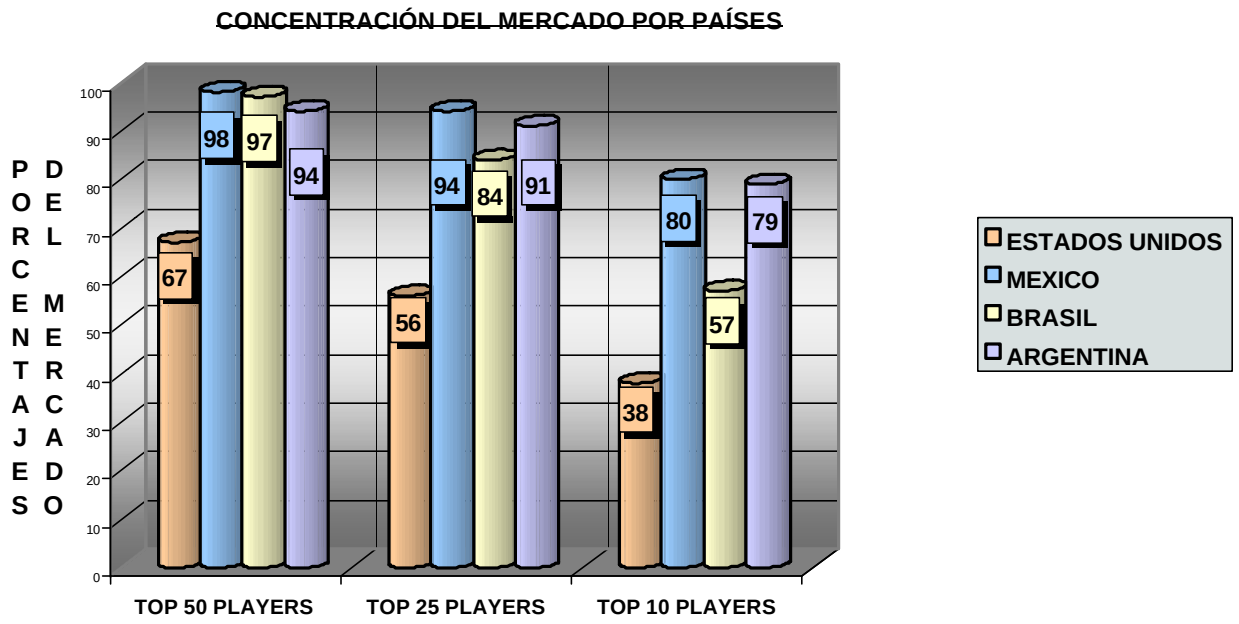
Ejemplos de comercios objetivos :

- **Musimundo.**
- **Garbarino.**
- **Compumundo.**
- **Showsport.**
- **Altocity**

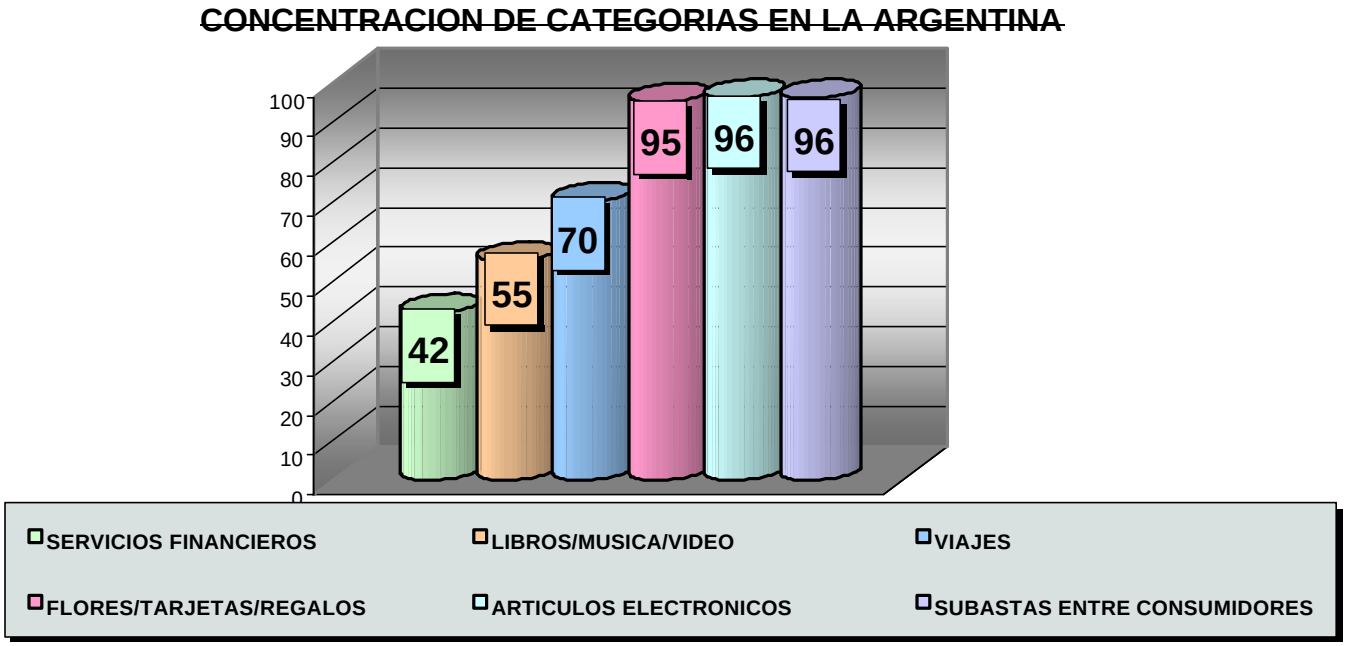
10.2 Comercios vendedores de tokens – Compensación



10.3 Selección de comercios en la Web



10.4 Selección de comercios en la Web



Fuente: The Boston Consulting Group – Rev. Mercado 11/00 -

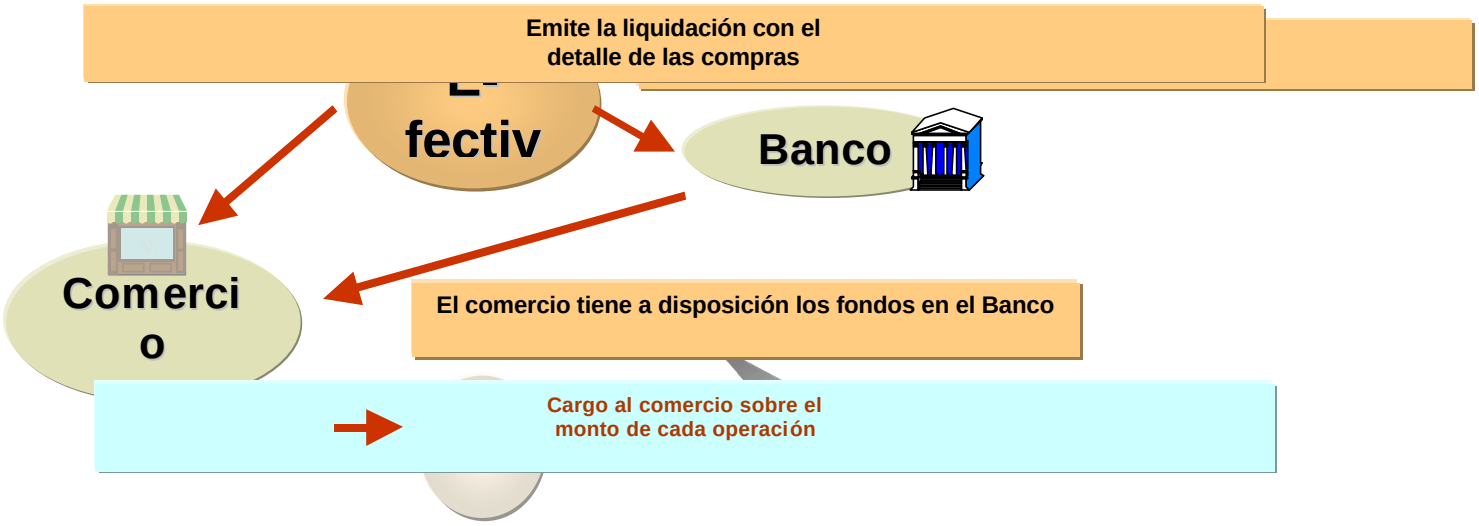
10.5 Selección de comercios en la Web

- Objetivo
- Año 1 Top 10 players.
- Año 2 25 players.
- Año 3 50 players o + .

10.6 Selección de comercios en la Web – Comisión

Condiciones actuales para comercios en la WEB con las TCs		Condiciones contempladas en el modelo para comercios en la WEB con e-fectivo	
Pago inicial	$ 5.000	Pago inicial	$ 1.000
Cuota anual	$ 1.000	Cuota anual	$ 600
Procesamiento por transacción	$ 0,10	Procesamiento por transacción	$ 0
Comisión sobre venta (promedio)	4 %	Comisión sobre venta (promedio)	4 %
Contracargos a cargo del comercio		No existen contracargos	
Pagos a 14 días		Pagos a 14 días	

10.7 Selección de comercios en la Web – Compensación



11 ANÁLISIS ECONÓMICO-FINANCIERO

11.1 Estado de resultados

Concepto	Total año 1	Total año 2	Total año 3	PROYECTO
INGRESOS				
Ingresos (hoja mercado detalle)	226.963	1.700.963	3.907.488	5.835.414
INGRESO 2	0	0	0	0
INGRESO 3	0	0	0	0
INGRESO 4	0	0	0	0
Ingresos Brutos	(6.809)	(51.029)	(117.225)	(175.062)
TOTAL INGRESOS	220.154	1.649.934	3.790.263	5.660.351
COSTOS				
Amortizaciones	50.000	50.000	50.000	150.000
Leasing	0	0	0	0
Mantenimiento	36.000	54.000	54.000	144.000
Insumos	0	0	0	0
Telecomunicaciones	0	0	0	0
TOTAL COSTOS	86.000	104.000	104.000	294.000
GASTOS				
Personal	75.000	130.000	130.000	335.000
Marketing	530.000	500.000	500.000	1.530.000
Infraestructura	8.444	14.468	28.031	50.944
Honorarios	140.000	0	0	140.000
Viajes y representación	0	0	0	0
Capacitación	0	0	0	0
Comisiones pagadas	94.112	718.753	1.668.182	2.481.047
TOTAL GASTOS	847.556	1.363.220	2.326.213	4.536.990
OVERHEAD	93.356	146.722	243.021	483.099
TOTAL COSTOS Y GASTOS	1.026.912	1.613.942	2.673.235	5.314.089
GANANCIA OPERATIVA	(806.758)	35.992	1.117.029	346.262
Resultados financieros	(65.009)	(86.892)	(22.165)	(174.066)
RES.ANTES IMPUESTOS	(871.767)	(50.901)	1.094.864	172.196
Impuesto a las ganancias	305.119	17.815	(383.202)	(60.269)
RESULTADO FINAL	(566.649)	(33.085)	711.662	111.927
% S/INGRESOS	-257,4%	-2,0%	18,8%	2,0%

11.2 Resumen

Indicadores Económicos	TOTAL	Total 2001	Total 2002	Total 2003	Total 2004	Total 2005	Total 2006
Ingresos	**5.660.351**	220.154	1.649.934	3.790.263	0	0	0
Costos y Gastos	**5.314.089**	1.026.912	1.613.942	2.673.235	0	0	0
Resultado Operativo	**346.262**	-806.758	35.992	1.117.029	0	0	0
	6,1%	-366,5%	2,2%	29,5%			
Resultado Final	**111.927**	-566.649	-33.085	711.662	0	0	0
	2,0%	-257,4%	-2,0%	18,8%			

Indicadores Financieros	TOTAL	Total 2001	Total 2002	Total 2003	Total 2004	Total 2005	Total 2006
Compras de Bienes de uso	**150.000**	150.000	0	0	0	0	0
Flujo de fondos operativo	**225.070**	-955.316	569.694	833.225	-509.934	287.402	0
Valor actual neto	**5.758**						
Tasa anual para VAN	**15,0%**						
Tasa Interna de retorno	**14,4%**						
Período de repago (meses)	**30**						

11.3 Balance

Concepto	INICIO	Total año 1	Total año 2	Total año 3
ACTIVO				
DISPONIBILIDADES				
Caja	1.000	1.000	1.000	1.000
Colocaciones financieras	0	0	0	357.589
TOTAL DISPONIBILIDADES	1.000	1.000	1.000	358.589
CLIENTES POR VENTAS				
Ingresos (hoja mercado detalle)	0	42.294	85.757	197.003
INGRESO 2	0	0	0	0
INGRESO 3	0	0	0	0
INGRESO 4	0	0	0	0
TOTAL CREDITOS	0	42.294	85.757	197.003
OTROS ACTIVOS	0	0	0	0
BIENES DE USO	0	100.000	50.000	0
TOTAL ACTIVO	1.000	143.294	136.757	555.591
PASIVO				
DEUDAS COMERCIALES				
Compra B.de Uso	0	0	0	0
Leasing	0	0	0	0
Mantenimiento	0	5.445	5.445	5.445
Insumos	0	0	0	0
Telecomunicaciones	0	0	0	0
Personal	0	0	0	0
Marketing	0	0	0	0
Infraestructura	0	0	0	0
Honorarios	0	0	0	0
Viajes y representación	0	0	0	0
Capacitación	0	0	0	0
Comisiones pagadas	0	0	0	0
OVERHEAD	0	0	0	0
TOTAL DEUDAS COMERC.	0	5.445	5.445	5.445
DEUDAS IMPOSITIVAS				
Ingresos Brutos	0	2.097	4.252	9.769
IVA	0	(13.806)	0	0
Ganancias	0	(305.119)	211.024	396.564
TOTAL DEUDAS IMPOSIT.	0	(316.827)	215.276	406.333
DEUDAS FINANCIERAS				
Total deuda financiera	0	1.020.325	514.770	30.886
TOTAL DEUDA FINANC.	0	1.020.325	514.770	30.886
TOTAL PASIVO	0	708.943	735.491	442.664
PATRIMONIO NETO				
Capital	1.000	1.000	1.000	1.000
Resultados acumulados	0	(566.649)	(566.649)	(599.734)
Resultados del ejercicio	0	0	(33.085)	711.662
TOTAL PATRIMONIO NETO	1.000	(565.649)	(598.734)	112.927
PASIVO + P.NETO	1.000	143.294	136.757	555.591
BALANCEO	0	0	(0)	0

11.4 CashFlow

Concepto	Total año 1	Total año 2	Total año 3	Total año 4	Total año 5	Total año 6	TOTAL PROYECTO
MOVIMIENTO NETO OPERAT.	(955.316)	592.447	863.637	(502.177)	287.402	0	285.994
Imp.a las Ganancias S/Financ.		(22.753)	(30.412)	(7.758)	0	0	(60.923)
FLUJO OPERATIVO NETO	(955.316)	569.694	833.225	(509.934)	287.402	0	225.070

11.5 Cashflow - Detallado

	Total año 1	Total año 2	Total año 3	Total año 4	Total año 5	Total año 6	Proyecto
CAJA INICIAL	1.000	1.000	1.000	1.000	1.000	1.000	1.000
MOVIMIENTOS DE FONDOS							
PROGRAMADOS:							
Ingreso de Fondos por:							
Reducción de caja objetivo	0	0	0	0	0	0	
Toma de Fondos	6.978.606	427.878	0	175.474	0	0	
Retiro de colocaciones	0	0	0	0	0	0	
Egreso de Fondos por:							
Incremento de caja objetivo	0	0	0	0	0	0	
Cancelación de deuda	(6.023.290)	(1.020.325)	(514.770)	(30.886)	(175.474)	0	
Colocación de fondos	0	0	(348.867)	0	(111.927)	(111.927)	
Distribución de dividendos	0	0	0	0	0	0	
NETO MOV. PROGRAMADOS	955.316	(592.447)	(863.637)	144.588	(287.402)	(111.927)	
NETO INTERESES COBR/PAG	(55.507)	(9.503)	(86.892)	(22.165)	0	0	
SUPERAVIT/DEFICIT FONDOS	(955.316)	592.447	863.637	(502.177)	287.402	0	
MOVIMIENTOS NO PROGR.							
Retiro de fondos	0	0	0	357.589	0	111.927	
Cancelación de deuda	(6.023.290)	(1.020.325)	(514.770)	(30.886)	(175.474)	0	
Colocación de fondos	0	0	(348.867)	0	(111.927)	(111.927)	
Toma de deuda	6.978.606	427.878	0	175.474	0	0	
NETO MOV.NO PROGRAM.	955.316	(592.447)	(863.637)	502.177	(287.402)	0	
COLOCACIONES							
Inicio	0	0	0	357.589	0	111.927	111.927
Colocación programada	0	0	0	0	0	0	
Retiro programado	0	0	0	0	0	0	
Colocación no programada	0	0	348.867	0	111.927	111.927	
Retiro no programado	0	0	0	(357.589)	0	(111.927)	
Intereses devengados	0	0	8.722	0	0	0	
Cierre	0	0	357.589	0	111.927	111.927	
ENDEUDAMIENTO							
Inicio	0	1.020.325	514.770	30.886	175.474	0	
Toma programada	0	0	0	0	0	0	
Cancelación programada	0	0	0	0	0	0	
Toma no programada	6.978.606	427.878	0	175.474	0	0	
Cancel. no programada	(6.023.290)	(1.020.325)	(514.770)	(30.886)	(175.474)	0	
Intereses devengados	65.009	86.892	30.886	0	0	0	
Cierre	1.020.325	514.770	30.886	175.474	0	0	

12 CONCLUSIONES

12.1 FODA del modelo

Fortalezas

- Mayor seguridad para los usuarios (montos limitados y protegido por PIN).
- Privacidad del consumidor (anonimato).
- Seguridad para el comercio on-line.
- Para el comercio ofrece un nuevo medio de pago que brinda la posibilidad de incrementar las ventas.
- Habilita el ingreso de un nuevo segmento de consumidores.
- Esquema habilitado para el uso de micropagos.
- Sinergias con capacidades instaladas.
- 'Know-how' en modelos operativos similares.

Debilidades

- Se requiere socios comerciales de envergadura para implementar el servicio de venta de tokens.

Oportunidades

- Segmento desatendido por los medios de pago actuales.
- Imagen de Inseguridad de los medios de pago para Internet.
- Esperado crecimiento de usuarios de Internet y de ofertas de compras.

Amenazas

- Falta de normas legales aplicables al modelo.

12.2 Conclusiones del trabajo

Planteamos como conclusión general de nuestro trabajo de tesis, el siguiente ejercicio para pensar. Es solo un ejercicio de imaginación o está más cerca de lo que imaginamos?

> **"El dinero virtual hace saltar la banca**
> Los bancos centrales estan desconcertados ante la posibilidad de que una moneda virtual circule por internet y acabe con los billetes"

CHARLOTTE DENNY The Guardian/ EL MUNDO

El jefe del banco central de Estados Unidos, uno de los hombres que tiene en sus manos el futuro de la economía mundial, Alan Greenspan, vive amenazado.

Las nuevas tecnologías han modificado a estas alturas el aspecto de la banca tradicional: han cerrado oficinas a medida que los clientes se han pasado a los servicios bancarios telefónicos y, ahora mismo, a Internet. La revolución que viene por Internet echará del negocio a los banqueros centrales, como Greenspan.

Olvídese del euro: las libras contantes y sonantes podrían ser reemplazadas muy pronto por monedas virtuales y sistemas digitales de pago. En cuanto el dinero se mueve por la red, escapa del control de los bancos centrales, con lo que arruina su capacidad para dirigir la economía. A Greenspan no se le permitirá ya controlar la inflación mediante la subida de los tipos de interés, porque los poseedores de dinero virtual no se verán afectados por las oscilaciones en la economía real.

El número dos del Banco de Inglaterra, Mervyn King, ha visto ya cuál es el futuro. En una reunión de los banqueros centrales más importantes del mundo hizo notar a sus colegas que, cuando perdieran el monopolio sobre el papel moneda, "los sucesores de Bill Gates habrían echado del negocio a los sucesores de Greenspan".

Revolución

La revolución ya ha comenzado en la red. Programas de fidelización cibernética como Beenz y Flooz retribuyen a los clientes que visitan determinados sitios de Internet con puntos que pueden consumirse en la red. El programa original de fidelización de compra a base de millas aéreas se ha extendido desde los cielos a otras fórmulas de remuneración. Un sitio canadiense ofrece de todo a los coleccionistas de sus puntos, desde estufas de butano hasta sartenes de cobre. El británico Charles Cohen, fundador de Beenz.com, reconoce que su invento todavía no puede considerarse dinero de verdad. No se puede

poner en circulación ni gastarse en la economía no electrónica y su poder adquisitivo se limita a la serie de sitios en los que lo aceptan. Pero él se imagina un mundo en el que el dinero electrónico privado llegue a ser de uso más corriente que el dinero oficial que emiten los bancos centrales. "Pasará menos de una década antes de que las empresas privadas emitan sus propias divisas", afirma Cohen. Las consecuencias serán enormes. "No me gustaría trabajar para Hacienda cuando eso ocurra".

La tecnología ya está haciendo inútiles los billetes y las monedas. Pagamos nuestras facturas por teléfono o mediante un cargo directo. El plástico está sustituyendo al dinero en efectivo, que es un medio de pago engorroso y caro. Pero el dinero de plástico se encuentra todavía bajo control del sistema bancario convencional: a final de mes, cuando llegan los recibos, los liquidamos con una transferencia desde una cuenta en un banco.

La auténtica revolución, según King, llegará cuando las empresas no necesiten ya más echar mano del sistema bancario para liquidarse mutuamente sus recibos. En la actualidad, cuando las empresas realizan grandes transacciones financieras, realizan la liquidación a través del sistema bancario. Cuando las empresas puedan saldar mutuamente sus cuentas por vía electrónica, sin necesidad de usar el sistema bancario, los bancos centrales ya no controlarán entonces los resortes de la economía. Los sistemas digitales de pago permitirán a las empresas la transferencia instantánea de sumas de dinero sin riesgo de impago.

Cuando no haya necesidad de utilizar el sistema bancario convencional, no habrá tampoco necesidad de utilizar las divisas nacionales.

Imagínese un mundo en el que Microsoft disponga de su propia divisa - llamada Bills, respaldada por la riqueza de la empresa. Las empresas que trabajen con Microsoft podrían optar por expedir sus facturas en Bills o en dólares. Las personas individuales podrían preferir que se les pagara en Bills si creen que la divisa de Microsoft va a correr menos riesgos inflacionistas que el dólar. Mediante el empleo de la tecnología de tarjetas inteligentes, ya disponible, los Bills podrían ser transferidos a monederos electrónicos, que harían factible su uso en la economía real en lugar de dinero en efectivo o cheques.

Garantías

Internet ofrece a los individuos la oportunidad de escapar del monopolio de los gobiernos. Los promotores de dinero electrónico tienen la posibilidad de hacerlo llegar fácilmente a un gran número de personas, la tecnología criptográfica avanza en el camino de garantizar la intimidad y la seguridad y, a medida que se desarrolle el comercio electrónico, habrá que dar por hecha la generalización de las monedas

digitales. Internet es una red internacional, por lo que tiene sentido que alguien desarrolle para su uso en la red una divisa mundial que protegería de las oscilaciones de las divisas nacionales a los consumidores que compran a través de las fronteras nacionales.

Ha llegado la época del dinero electrónico, dice Jon W. Mantonis, autor de Dinero digital y libertad monetaria. "Ni el dólar ni ninguna otra divisa gubernamental han logrado establecerse en esta nueva economía. El paisaje monetario está maduro y completamente abierto, y las divisas privadas deberían infiltrarse ya en él".

De momento, la mayoría de los sitios que anuncian dinero electrónico o digital son programas de diversas clases, para cifrar las tarjetas de crédito, con lo que se ofrece a los consumidores una posibilidad de pago seguro mediante las divisas nacionales ya existentes. Beenz y Flooz son, más propiamente, divisas electrónicas pero de circulación muy restringida como para competir con el dinero.

Establecer divisas

La auténtica revolución llegará cuando una gran empresa, con reconocimiento mundial de su marca, decida establecer una divisa. Una empresa como American Express, que ya maneja un sustituto del dinero cheques de viaje, sería el sitio natural desde el que empezar, según Mantonis.

Si empleara su propia moneda el Amex, podría cargar comisiones menores a los comerciantes que aceptan sus tarjetas. "American Express se beneficiaría de las connotaciones del nombre y de la identificación de marca que acompaña a todo sistema de precios", escribe Mantonis.

Los Amexes podrían llegar a reemplazar a las actuales divisas de países proclives a la hiperinflación. Varios países latinoamericanos sopesan el abandono de sus propias divisas, en favor de la estabilidad del dólar norteamericano. Esos complejos desaparecerían si se adoptara una moneda privada con credibilidad.

Pero todavía hay que superar enormes obstáculos antes de que el dinero electrónico se convierta en realidad. ¿A qué recurrirán las empresas para respaldar sus divisas y quién determinará la tasa de cambio entre las nuevas divisas y las ya existentes? ¿Serán realmente las ventajas de las nuevas divisas superiores a las complejidades de tener más tipos de dinero en circulación? ¿Opondrán a la inflación mayor resistencia que las divisas gubernamentales o sucumbirán las empresas a la tentación de endurecerse con sus clientes a base de aumentar su volumen de dinero y reducir su valor?

12.3 Riesgos Involucrados

Riesgos involucrados	Forma de acotamiento
Lanzar tardíamente	Tener una acción proactiva en el desarrollo del producto, y en la comunicación a los futuros usuarios
Reacción de los organismos de control (BCRA, AFIP, etc)	Consultas no vinculantes a los organismos pertinentes

13 GLOSARIO

Acceso legal:
Acceso por parte de terceras personas o entidades, incluyendo gobiernos, al texto en claro, o claves criptográficas, o datos cifrados, de acuerdo a ley.

Autenticación:
Proceso por el cual se garantiza que el usuario que accede a un sistema de ordenador es quién dice ser. Por lo general, los sistemas de autenticación están basados en el cifrado mediante una clave o contraseña privada y secreta que sólo conoce el auténtico emisor.

Autoridad certificadora:
Entidad que da testimonio de la pertenencia o atribución de una determinada firma digital a un usuario o a otro certificador de nivel jerárquico inferior.

Adjunto:
Se llama así a un archivo de datos (por ejemplo una plantilla de cálculo o una carta de procesador de textos) enviado junto a un mensaje de correo electrónico. Para que el documento pueda viajar, debe ser codificado de alguna manera, ya que el e-mail solo puede transportar el más estándar de los códigos: el ASCII. Entre los formatos de codificación más populares están el UUENCODE, el MIME y el BinHex. En la actualidad, el proceso de codificación para el envío por e-mail es generalmente realizado sin que el usuario o perciba.

Agente (agent):
Pequeño programa “inteligente” creado para efectuar ciertas tareas, facilitando la operatoria del usuario. Un ejemplo muy conocido de agente son los Asistentes (wizards) que existen en la mayoría de los softwares modernos.

Ancho de banda (bandwidth):
Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso y mayor tráfico o cantidad de personas que pueden utilizar el mismo medio simultáneamente. Se mide en hertz o bps (bits por segundo), por ejemplo 32 Kbps, 64 Kbps, 1 Mbps, etc.

ANSI (American National Standards Institute, Instituto Americano de Normas):
Organización que desarrolla y aprueba normas de los Estados Unidos. Participó en la creación de gran parte de las normas en uso actualmente en Internet. http://www.ansi.org

Applet (programa):
Pequeño programa hecho en lenguaje Java.

Archie:
Herramienta que permite localizar archivos en la red Internet creada en Montreal por la Universidad de McGill. Un server de Archie (hay varios distribuidos por toda Internet) mantiene una base de datos que registra la ubicación de varios miles de archivos en la Red. Actualmente el sistema sigue la pista a alrededor de 1.500.000 archivos en 900 lugares de almacenamiento. Cayó en desuso a partir de la aparición de la World Wide Web.

***ARP (Address Resolution Protocol, Protocolo de Resolución* de Direcciones):**
Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

ARPANET (Advanced Research Projects Agency NETwork, Red de la Agencia de Proyectos de Investigación Avanzados):
Una red pionera de computadoras, fundada por DARPA, una agencia de investigación del gobierno norteamericano. Fue la base fundamental en los años sesenta para el desarrollo de lo que luego se convertiría en la red Internet.

ASCII (American Standard Code for Information Interchange, Código americano Normado para el Intercambio de Información):
Conjunto de caracteres, letras y símbolos utilizados en todos los sistemas de computadoras de cualquier país e idioma. Permite una base común de comunicación. Incluye las letras normales de alfabeto español, con excepción de la ñ y toda letra acentuada. Cada símbolo posee un número asignado entre el 0 y el 127 y que es común en todos los países. Del número 128 al 255 cada idioma puede agregar otros símbolos necesarios para su propio lenguaje.

Attachment (adjunto):
Ver Adjunto.

Autoridad Certificante (Certificanting Authority):
Empresa en Internet que realiza las funciones de una especie de "escribano virtual". Se encarga de garantizar la identidad de las personas físicas y las empresas que participan en la Red, a través de la emisión de los llamados Certificados. La más conocida mundialmente es la firma VERISIGN.

Authoring (autoría):
Actividad de crear contenido para la Web en Páginas en formato HTML.

El administrador de un sitio Web o Webmaster es, en general, el responsable de la autoría de su contenido.

Avatar (figura humana de un dios en la mitología hindú):
A Identidad ficticia, una representación física (cara y cuerpo) de una persona conectada en el mundo virtual de Internet. Muchas personas construyen su personalidad digital que utilizan luego en servers determinados (por ejemplo Chats) para jugar o charlar con otros.

Backbone (columna vertebral):
conexión de alta velocidad que conecta a computadoras encargadas de circular grandes volúmenes de información. Los backbones conectan ciudades o países, y constituyen la estructura fundamental de las redes de comunicación. Las Redes WAN y los ISPs utilizan backbones para interconectarse.

Backdoor (o trapdoor, puerta trasera o puerta trampa):
sección oculta de un programa de computadora, que sólo se pone en funcionamiento si se dan condiciones o circunstancias muy particulares (por ejemplo, si se ingresa una clave particular, o se presionan juntas varias teclas determinadas del teclado). Son creadas por los programadores para situaciones especiales; por ejemplo para tener accesos especiales a la información, diferentes a los de un usuario común.

Bandwidth:
ver Ancho de banda.

Banner:
aviso publicitario que ocupa parte de una página de la Web, en general ubicado en la parte superior al centro. Haciendo un click sobre él, el navegante puede llegar hasta el sitio del anunciante. En general, los banners se cobran en base a los click-throughs que se obtienen, o a las veces que son vistos por los visitantes a la Página Web.

BBS (Bulletin Board System, Sistema de mensajería también llamado erróneamente Base de Datos):
es un sistema computarizado de intercambio de datos entre un grupo de personas que comparten una misma zona geográfica donde archivos, mensajes y otra información útil pueden ser intercambiados entre los distintos usuarios. Normalmente se trata de sistemas amateur, y son los antecesores aislados de la Red Internet. La red mundial que comunica a los BBSs se llama Fidonet.

Binhex:

un estándar para la codificación de datos bajo plataforma MACINTOSH, utilizada para enviar archivos adjuntos. Similar en concepto al MIME y al Uuencode.

Bookmark (señalador o favoritos):
la sección de menú de un navegador donde se pueden almacenar los sitios preferidos para luego volver a ellos simplemente eligiéndolos con un simple click desde un menú.

Boolean (booleana):
lógica simbólica que se utiliza para expresar la relación entre términos matemáticos. Su base lógica puede ser extendida para analizar la relación entre palabras y frases. Los dos símbolos más usuales son AND (y) y OR (o). Se utilizan para acotar las búsquedas de temas en los Buscadores de la Web.

Bottleneck (cuello de botella):
"embotellamiento" de paquetes de datos (información) que circulan por una conexión causando demoras en la comunicación.

Bots:
abreviatura de robots. No son otra cosa que programas muy particulares, inteligentes y autónomos, que navegan por el ciberespacio intentando causar caos en los Chats y esquivando las maniobras que intentan detenerlos. Los bots son sumamente ingeniosos y capaces de reaccionar según situaciones. No necesariamente son benignos: sólo obedecen las órdenes de sus creadores

Browser / Web browser (navegador o visualizador):
programa que permite leer documentos en la Web y seguir enlaces (links) de documento en documento de Hipertexto. Los navegadores "piden" archivos (páginas y otros) a los servers de Web según la elección del usuario, y luego muestran en el monitor el resultado en forma Multimedial. Entre los más populares se encuentran el Netscape Navigator, Microsoft Explorer y Mosaic. El primer navegador se llamó Line Mode Browser, pero el primero en alcanzar popularidad fue el Mosaic, nacido en 1993. Usualmente, a los navegadores se les agrega Plug-ins para aumentar sus capacidades.

Buscador (Search Engine, motor de búsqueda):
herramienta que permite ubicar contenidos en la Red, buscando en forma booleana a través de palabras clave. Se organizan en buscadores por palabra o índices (como Lycos o Infoseek) y buscadores temáticos o Directories (como YAHOO!). Dentro de estas dos categorías básicas existen cientos de buscadores diferentes, cada uno con distintas habilidades o entornos de búsqueda (por ejemplo sólo para médicos, para fanáticos de las mascotas o para libros y revistas).

***Certificado**:*
Documento digital que identifica a la autoridad certificadora que lo ha emitido, identifica al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido.

***Cifrado**:*
Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.

***Clave criptográfica**:*
Parámetro que se utiliza junto con un algoritmo criptográfico para transformar, validar, autenticar, cifrar o descifrar datos.

Confidencialidad:
Característica o atributo de la información por el que la misma sólo puede ser revelada a los usuarios autorizados en tiempo y forma determinados.

Criptografía:
Ciencia que mediante el tratamiento de la información, protege a la misma de modificaciones y utilización no autorizada. Utiliza algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro extremo.

Cablemódem:
Dispositivo que permite conectar una computadora a Internet a través de la conexión del cable coaxil que utiliza la televisión de señal por cable. No es realmente un módem ya que no debe modular/demodular debido a que se trata de un sistema de transporte puramente digital. Se perfila como una de las posibilidades de conexión que resolverían la problemática del limitado ancho de banda que es posible obtener a través de una conexión telefónica. Vea DirecPC.

Caché:
Almacenamiento intermedio o temporario de información. Por ejemplo, un navegador posee un caché donde almacena las últimas páginas visitadas por el usuario, y si alguna se solicita nuevamente en un corto plazo, el navegador mostrará la que tiene en su memoria, en lugar de volver a buscarla en la Red. El término se utiliza para denominar todo depósito intermedio de datos solicitados con frecuencia. Vea Proxy.

CERN (Conseil Européen pour la Recherche Nucléaire, Consejo Europeo de Investigación Nuclear):
Organización que fue la cuna de la World Wide Web. Está ubicado en la ciudad de Ginebra, en el límite entre Francia y Suiza. Tim Berners-Lee,

considerado uno de los padres de la Web, trabajaba en el este instituto cuando tuvo la original idea de la Web. http://www.cern.ch

Certificado (certificate):
Mecanismo de validación y garantía de identidad de una entidad o persona en Internet. Son necesarios para dar fe, por ejemplo, de que una empresa es quien dice ser al realizar una compra electrónica. Su fin es reducir el riesgo en las operaciones comerciales virtuales. De escaso uso por ahora, son la base fundamental para el correcto funcionamiento de la firma electrónica. Los Certificados son emitidos por las Autoridades Certificantes. Probablemente en los próximos años todo usuario de Internet tendrá su propio certificado.

CGI (Common Gateway Interface, Interfaz Común de Intercomunicación):
En programación, conjunto de medios y formatos creados para permitir y unificar la comunicación entre la Web y otros sistemas externos y programas, como las bases de datos. Similar en funcionalidad al Activex.

Chat:
Sistemas de conversación en línea que permiten que varias personas de todo el mundo conversen en tiempo real a través de sus teclados sobre los temas más variados. Existen varios sistemas de chat, uno de los mas populares es el IRC.

Click-throughs:
Sistema de medición que almacena la cantidad de veces que un potencial cliente hace click en un banner de publicidad y de visitas realizadas al sitio del anunciante. Utilizado como métrica para la venta de espacios de publicidad en los sitios Web.

Client side CGI script:
Script CGI que se ejecuta/corre en la computadora del cliente.
Ver también Server side CGI script.

Cliente (Client):
Computadora o programa que se conecta a servidores para obtener información. Un cliente sólo obtiene datos, no puede ofrecerlos a otros clientes sin depositarlos en un servidor. La mayoría de las computadoras que las personas utilizan para conectarse y navegar por Internet son solamente “clientes”de la Red. Vea Cliente/Servidor.

Cliente/Servidor (Client/Server):
Sistema de organización de interconexión de computadoras que sirve para el funcionamiento de Internet, así como de otros tantos sistemas de redes. Se basa en la separación de las computadoras miembros en dos categorías: los que actúan como servidores (oferentes

de información), y los que lo hacen como clientes (receptores de información).

Comercio Electrónico (E-commerce):
Es la utilización de redes de datos (entre ellas principalmente Internet) para la realización de actividades comerciales entre empresas, consumidores finales y entidades de gobierno. Recién está naciendo, pero se trata de un área de negocios que se espera tendrá mucho desarrollo.

Cookies (galletitas):
Son pequeños archivos con datos que algunos sitios Web depositan en forma automática en las computadoras de los visitantes. Lo hacen con el objetivo de almacenar allí información sobre las personas y sus preferencias. Por ejemplo, la primera vez que un navegante visita un site y completa algún formulario con sus datos y perfil, el sistema podrá enviarle una cookie al asignarle una identificación. La siguiente vez que retorne allí, el sitio Web pedirá automáticamente a la computadora cliente la cookie, y a través de ella lo reconocerá.

Cracker (pirata informático):
Persona que se especializa en atravesar medidas de seguridad de una computadora o red de computadoras, venciendo claves de acceso y defensas, para obtener información que cree valiosa. Un cracker, en general, es considerado un personaje ruin y sin honor, diferente de un hacker. Vea Firewall.

Cross-platform (multi-plataforma):
Se refiere a un programa o dispositivo que puede ser utilizado sin inconvenientes en distintas plataformas (sistemas) de hardware y sistemas operativos. Un programa en lenguaje Java posee esta característica. CSLIP (Compressed Serial Line Internet Protocol, Protocolo Internet Comprimido para Líneas Seriales): una variante comprimida del protocolo SLIP, que permite una conexión vía módem más rápida.

Cybermoney (ciberdinero):
Formas de pago virtuales alternativas que se están desarrollando en Internet, especialmente apuntadas al Comercio Electrónico. En este momento, la falta de mecanismos de pago sencillos que garanticen el intercambio de dinero es una de las principales barreras para el desarrollo de los negocios por Internet. Actualmente, existen distintas alternativas en experimentación como CyberCash, Cybercoin, y los mecanismos para el pago de sumas muy pequeñas, llamados micropagos.

Cyberspace (ciberespacio):
Es la denominación del espacio virtual (no-físico) donde las personas se reúnen en Internet. También denomina a la cultura, usos y costumbres de la comunidad electrónica. Término inventado por el escritor de Ciencia Ficción William Gibson, en su obra Neuromancer. Vea Netiquette.

DARPA (Defense Advanced Research Project Agency, Agencia de Proyectos de Investigación Avanzados):
Una agencia del Departamento de Defensa de los Estados Unidos. Creadores de la red ARPANet que años más tarde se convertiría en Internet.

Data Mining:
Conjunto de técnicas de Bases de Datos para el análisis avanzado de la información almacenada, y la extracción de conclusiones a partir de ello.

Datagram (datagrama):
Conjunto de datos de características específicas. Paquete de datos que viaja por una red.

Datos personales:
Cualquier información referente a una persona identificada.

Default (acción por omisión):
Opción que un programa asume si no se especifica lo contrario. También designa los llamados “valores predeterminados”.

Depositario de la clave*:*
Persona o entidad que está en posesión o tiene el control de las claves criptográficas. El depositario de la clave no es necesariamente el usuario de la misma.

Descifrado*:*
Función inversa al cifrado.

Dinero Electronico:
Unidades o símbolos de valor monetario que toman forma digital y se trasmiten a través de redes electrónicas. Las Unidades de Valor Digital son las unidades básicas de denominación del dinero electrónico; pueden corresponder o no a las unidades de la moneda nacional.

Disponibilidad:
El hecho de ser accesibles y utilizables los datos, informaciones o sistemas de información en el tiempo deseado y del modo requerido.

Dial-in:
Conexión a Internet que se establece a través de un módem y una línea telefónica. A cada usuario le es asignado un número IP dinámico, es decir, que es otorgado sólo durante la comunicación. Para establecer la conexión, se utiliza algún estándar adecuado, como por ejemplo el PPP, SLIP o CSLIP.

Dial-up:
Término actualmente utilizado como sinónimo de dial-in. Anteriormente definía una conexión a Internet ligeramente diferente a la dial-in. Digital signature: Ver Firma Digital.

Dirección electrónica (electronic address):
Serie de caracteres que identifican unívocamente a un servidor (por ejemplo iworld.com.ar), una persona (por ejemplo rox@iworld.com.ar) o un recurso (por ejemplo un sitio Web como http://www.iworld.com.ar) en Internet. Se componen de varias partes de extensión variable. Las direcciones son convertidas por los DNS en los números IP correspondientes, para que puedan viajar por Internet.

Directory:
Tipo de buscador organizado por temas o categorías.

DirectPC:
Nueva forma de conexión a Internet, basada en el uso de una antena satelital conectada a la computadora durante las 24 horas. Se perfila como una de las posibilidades de comunicación que resolverían la problemática del limitado ancho de banda que se puede obtener en una conexión telefónica. Vea Cablemodem.

DNS (Domain Name System/Server, servidor de nombres de dominios):
Sistema de computadoras y bases de datos que se encarga de convertir (resolver) las direcciones electrónicas de Internet (como www.iworld.com.ar) en la dirección IP correspondiente, y viceversa. Componen la base del funcionamiento de las direcciones electrónicas en Internet y están organizados jerárquicamente. Ver Internic, ARP. DoD (Department of Defense, Departamento de Defensa de los Estados Unidos): una de sus agencias -DARPA- fue la responsable de la invención de la Internet.

Dirección electrónica (electronic address):
Serie de caracteres que identifican unívocamente a un servidor (por ejemplo iworld.com.ar), una persona (por ejemplo rox@iworld.com.ar) o un recurso (por ejemplo un sitio Web como http://www.iworld.com.ar) en Internet. Se componen de varias partes de extensión variable. Las

direcciones son convertidas por los DNS en los números IP correspondientes, para que puedan viajar por Internet.

Download:
Es el proceso de bajar (traer) un archivo desde algún lugar en la Red a la computadora de un usuario. Vea Upload, el proceso inverso. Dynamic IP (IP dinámico): se designa así cuando el número IP de una computadora conectada a un proveedor de servicio vía dial-in, es otorgado en el momento de la conexión, en lugar de ser un número IP fijo.

EDI *(Electronic Data Interchange):*
Protocolo creado a principios de los años 70 para permitir que las grandes compañías pudieran transmitir información a través de sus redes privadas, y está siendo adaptado en la actualidad a los Webs corporativos.

EFF (Electronic Frontier Foundation):
Un organismo civil de Internet y sin fines de lucro, cuyo objetivo es “civilizar la frontera electrónica, hacerla útil no sólo para la elite técnica, sino también para el resto de la humanidad, y lograr esto conservando las mejores tradiciones de nuestra sociedad: el flujo libre y abierto de información y comunicación" (EFF Mission Statement, Abril, 1990). Más datos en http://www.eff.org.

E-mail (Electronic mail o Correo electrónico):
Servicio de Internet que permite el envío de mensajes privados (semejantes al correo común) entre usuarios. Basado en el SMTP. Más rápido, económico y versátil que ningún otro medio de comunicación actual. También utilizado como medio de debate grupal en las mailing lists.

Emoticons (o Smilies):
Conjunto de caracteres gráficos que sirven para demostrar estados de ánimo en un medio escrito como el e-mail. Por ejemplo, los símbolos :-), vistos de costado apoyando la mejilla izquierda sobre el hombro, muestran una cara sonriente y puede significar un chiste o buenos deseos.

Enlace (link):
Conexiones que un documento de la Web (escrito en HTML) posee. Un enlace puede apuntar a referencias en el mismo documento, en otro documento en el mismo site; también a otro site, a un gráfico, video o sonido. Ver Hipertexto.

Estándar:
Ver Norma.

Extranet:
Utilización de la tecnología de Internet para conectar la red local (LAN) de una organización con otras redes (por ejemplo de proveedores y clientes). Ver Intranet.

E-ZINE (Electronic Magazine):
Revista electrónica, en general amateur, sobre cualquier tema. Han proliferado debido a que Internet es, posiblemente, el medio más barato del que se dispone en la actualidad para acceder a la mayor cantidad de lectores. Una variada lista de e-zines es la de John Labovits, disponible en http://www.meer.net/johnl/e-zine-list/index.html

Ecommerce:
Vea Comercio electrónico.

Encriptación:
Método para convertir los caracteres de un texto u archivo de modo que no sea posible comprenderlosi antes no se lo lee (des-encripta) con la clave correspondiente. Utilizado para proteger la integridad de información secreta en el caso en que sea interceptada. Uno de los métodos más populares y seguros de encriptación es el PGP.

Encryption:
Ver Encriptación.

Estándar:
Ver Norma.

Extranet:
Utilización de la tecnología de Internet para conectar la red local (LAN) de una organización con otras redes (por ejemplo de proveedores y clientes). Ver Intranet.

Firma digital:
Información añadida o transformación cifrada de los datos que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Consiste en una transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posea el mensaje inicial y la clave pública del firmante, pueda determinar de forma fiable si dicha transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante, y si el mensaje ha sido alterado desde el momento en que se hizo la transformación.(Utah) Es un sello integrado en datos digitales, creado con una clave privada, que permite identificar al propietario de la firma y comprobar que los datos

no han sido falsificados (Alemania).

FAQ (Frequently Asked Questions, Preguntas Frecuentes):
Conjunto de preguntas y respuestas habituales sobre un determinado tema. Utilizados para despejar las dudas de los neófitos. Farming, farm server: servidor externo que se alquila para alojar información y ponerla a disposición de los navegantes de la Red. Sinónimo de Hosting.

Fibra óptica (Fiber Optics):
Material con el que se construyen las conexiones de datos de más alta velocidad conocida.

Fidonet:
La red que intercomunica a la mayor cantidad de BBSs amateurs del mundo, nacida en 1982. Reúne a unas 30 mil personas. Actualmente está desapareciendo ante el crecimiento de Internet.

Finger:
Comando que permite obtener información de una persona en la Red (por ejemplo dirección de e-mail, dirección postal, hobbies), buscando ciertos datos que la persona puede dejar en un formulario de consulta. En la actualidad está en desuso.

Firewall (pared a prueba de fuego):
Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada (por ejemplo, una Intranet). Es utilizado para proteger los recursos de una organización ante el ingreso de consultas externas no autorizadas.

Flame (llamarada):
Ataque personal insultante. Mensaje de correo electrónico ofensivo.

Frame (cuadro, marco):
Instrucciones en el lenguaje HTML (utilizado para diseñar las páginas Web); una forma de dividir la pantalla del navegante en varias zonas, cada una con autonomía de movimiento. Por ejemplo, se puede dividir una pantalla de modo que haya un frame vertical que ocupe el lado izquierdo de la pantalla durante toda la navegación, que contenga el menú de un sitio Web. Los frames son un agregado al HTML estándar inventado por la empresa NETSCAPE y luego adoptados como norma.

Frame-relay:
Tecnología de transporte de datos por paquetes utilizada muy comúnmente en las conexiones por líneas dedicadas.

Freeware:
Política de distribución gratuita de programas. Empleada para gran parte del software de Internet. En general, estos programas son creados por un estudiante o alguna organización (usualmente una Universidad) con el único objetivo de que mucha gente en el mundo pueda disfrutarlos. No necesariamente son sencillos: muchos de ellos son muy complejos y han llevado cientos de horas de desarrollo. Ejemplos son el sistema operativo Linux (un Unix) o el PGP (Pretty Good Privacy, un software de encriptación), que se distribuyen de este modo.

FTP (File Transfer Protocol, protocolo de transferencia de archivos):
Servicio de Internet que permite transferir archivos (upload y download) entre computadoras conectadas a la Internet. Este es el método por el cual la mayoría del software de Internet es distribuido.

Full-Duplex:
Característica de un medio de comunicación por la cual se pueden enviar y recibir datos simultáneamente por el mismo canal. Vea half-duplex.

FYI (For your information, para su información):
Documentos de distribución destinados a hacer públicas ciertas decisiones, cambios o novedades de Internet. Son más informativos que los RFCs. Utilizados por las entidades que regulan y organizan Internet.

Gateway:
Dispositivo de comunicación entre dos o más redes locales (LANs) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación. Como término genérico, es utilizado para denominar a todo instrumento capaz de convertir o transformar datos que circulan entre dos medios o tecnologías.

Gopher (topo):
Herramienta de Internet que organiza la información y permite acceder a ella en forma sencilla. Es precursora de la Web y actualmente está cayendo en desuso. Creada en la Universidad de Minessotta, su nombre hace referencia a la mascota del lugar, que es un topo. Otros, sin embargo, sugieren que es una deformación de la frase goes-for (busca). El Gopher resolvió el problema de cómo ubicar recursos en Internet, reduciendo todas las búsquedas a menús y submenús. Con el tiempo, el Gopher fue perdiendo popularidad frente a la World Wide Web, gracias a la ventaja de tener contenido multimedial de imágenes y sonido.

Groupware:
Conjunto de programas preparados especialmente para que un grupo de personas trabaje en grupo. Contiene entre otros, programas para chats, teleconferencias, correo electrónico grupal, whiteboards (pizarras de trabajo), etc. Permite que se formen grupos de trabajo entre personas que están a miles de km. de distancia, y la adopción masiva de estas herramientas probablemente revolucione la forma de trabajar que hoy se conoce.

Gurú:
Dícese, por extensión, de una persona con muchos conocimientos sobre un tema, en general técnico.

Hacker:
Experto técnico en algún tema relacionado con comunicaciones o seguridad; de alguna manera, es también un gurú. Los hackers suelen dedicarse a vencer claves de acceso por pura diversión, o para demostrar fallos en los sistemas de protección de una red de computadoras, casi como un deporte. A diferencia de los crackers, los hackers son muy respetados por la comunidad técnica de Internet.

Half-Dúplex:
Característica de un medio de comunicación por la cual no se pueden enviar y recibir datos simultáneamente. A diferencia del full-dúplex, se debe esperar que una parte termine de transmitir para poder enviar información por el mismo medio. En cierta forma, hablar por teléfono es un proceso de comunicación half-dúplex, donde por momentos se habla y por momentos se escucha, pero donde se hace difícil establecer una comunicación si los dos participantes hablan a la vez.

Hardware:
Componente físico de la computadora. Por ejemplo: el monitor, la impresora o el disco rígido. El hardware por sí mismo, no hace que una máquina funcione. Es necesario, además, instalar un Software adecuado.

Hipermedia:
Combinación de hipertexto y multimedia. Uno de los grandes atractivos de la Web.

Hipertexto:
Concepto y término inventado por Ted Nelson en 1969. Nelson era un famoso visionario de la informática que investigaba, desde hacía 25 años, las posibilidades de interacción entre las computadoras y la literatura. Uno de los conceptos base para el desarrollo de la WWW. El hipertexto es una forma diferente de organizar información. En lugar de leer un texto en forma continua, ciertos términos están unidos a otros

mediante relaciones (enlaces o links) que tienen entre sí. El hipertexto permite saltar de un punto a otro en un texto, y a través de los enlaces (con un simple click con el mouse sobre las palabras subrayadas y en negrita) permite que los navegantes busquen información de su interés en la Red, guiándose por un camino distinto de razonamiento. Algunos programas muy difundidos, como la Ayuda de Windows o las enciclopedias en CD-ROM, están organizadas como hipertextos.

Hit (acceso o pedido):
Unidad de medición de accesos a un determinado recurso. Forma de registrar cada pedido de información que un usuario efectúa a un server. Por ejemplo, en el caso de un sitio Web, la solicitud de cada imagen, página y frame genera un hit. Por lo tanto, para conocer en realidad cuántos accesos hubo, debe dividirse la cantidad de hits por la cantidad de objetos independientes (texto, frames e imágenes) que una página contiene, o usar un contador de accesos.

Home page (página principal o de entrada):
Página de información de la Web, escrita en HTML. En general, el término hace referencia a la página principal o de acceso inicial de un site.

Host:
Sinónimo de servidor.

Hosting:
Ver Farming.

Hostname (nombre de un host):
Denominación otorgada por el administrador a una computadora. El hostname es parte de la dirección electrónica de esa computadora, y debe ser único para cada máquina conectada a Internet.

HTML (HyperText Markup Language, Lenguaje de Marcado de Hipertextos):
Lenguaje que define textos, subgrupo del SGML, destinado a simplificar la escritura de documentos estándar. Es la base estructural en la que están diseñadas las páginas de la World Wide Web. Su definición está a cargo del Web Consortium.

HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto):
Es el mecanismo de intercambio de información que constituye la base funcional de la World Wide Web.

Hyperdocuments (Hiperdocumentos):
Documento que tiene estructura de hipertexto, pero contiene

además referencias a objetos multimediales (como sonidos, imágenes, videos).

Hyperlink:
Enlace entre dos nodos de un hipertexto.

Hypermedia:
Ver Hipermedia.

Hypertext:
Ver Hipertexto.

IAB (Internet Activities Board, Panel de Actividades de Internet):
Comité coordinativo creado para el diseño, ingeniería y administración de Internet. Supervisa al IETF.

IANA (Internet Assigned Numbers Authority, Autoridad de Asignación de Números de Internet):
Organismo que asigna los números IP a las instituciones que desean participar de Internet. Actualmente funciona junto a Internic.

ICANN (Internet Centre for Assigned Names and Numbers, Centro de Internet para la asignación de nombres y números):
Organismo de Internet muy importante, que se ocupa de otorgar grupos de números IP y direcciones electrónicas a cada organización que desee conectarse a Internet, garantizando que sean únicas. Representado en la Argentina por la Cancillería (www.nic.ar). Más datos en http://www.icann.net.

Integridad*:*
Garantía de la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

IETF (Internet Engineering Taskforce, Fuerza de trabajo de Ingeniería de Internet):
Gran comunidad abierta de ingenieros, operadores, vendedores e investigadores cuyo propósito es coordinar la operación, administración y evolución de Internet. Más datos en http://www.ietf.org

IMO (In My Opinión, En Mi Opinión):
Una de las siglas utilizadas en los mensajes de Internet. También IMHO (In My Humble Opinion, En Mi Humilde Opinión).

Impressions (visualizaciones):
Unidad de medida que verifica cuántas veces un navegante ve un determinado banner de publicidad. Alternativa de click-through.

Inteligencia Artificial (Artificial Intelligence o AI):
Rama de la computación que analiza a la computadora y sus posibilidades de poseer inteligencia. La IA estudia las habilidades inteligentes de razonamiento, capacidad de extracción de conclusiones y reacciones ante nuevas situaciones de las computadoras y sus programas. El razonamiento es parecido al del cerebro humano (no es lineal, se aprende de cada situación). Existen dos ramas de la IA: la fuerte (strong), sostiene que llegará el día en que puedan construirse programas que sean realmente inteligentes y computadoras pensantes. La débil (weak) cree que las computadoras sólo pueden ser diseñadas para convertirse en importantes herramientas para modelar y simular el pensamiento humano.

Interface (interfaz):
Cara visible de los programas. Interactúa con los usuarios. La interface abarca las pantallas y su diseño, el lenguaje utilizado, los botones y los mensajes de error, entre otros aspectos de la comunicación computadora/persona.

Internet address:
Sinónimo de número IP. Número asignado que identifica a un server en Internet. Está compuesto por dos o tres partes: número de red, número opcional de sub-red y número de host. Ver direcciones electrónicas, DNS.

Internet Worm:
Programa similar a un virus de computadora creado por Robert Morris, un estudiante de Cornell University, que fue muy famoso en 1988. El Worm se aprovechó de una fallo de seguridad de un programa de e-mail muy utilizado, y causó desastres al reproducirse sin límite, infectando y luego dejando catatónicas a la mayor parte de las computadoras conectadas a Internet. El pánico causado por el virus fue tan grande que generó el nacimiento de varios organismos dedicados a investigar los fallos de seguridad de los programas.

Internet (con mayúscula):
La red de computadoras más extendida del planeta, que conecta y comunica a más de 50 millones de personas. Nació a fines de los años sesenta como ARPANet, y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre si en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar de qué tipo de computadoras se trate, para intercomunicarse utilizan el protocolo TCP/IP. Las computadoras que utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en

general a través en un tipo de conexión llamado dial-in, utilizando un módem y una línea telefónica.

internet (con minúscula):
Denomina a un grupo interconectado de redes locales, que utilizan un mismo protocolo de comunicación.

InterNIC (Internet Network Information Centre, Centro de Información de Red de Internet):
antiguo nombre de ICANN.

Intranet:
Utilización de la tecnología de Internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una organización. Permite crear un sitio público donde se centraliza el acceso a la información de la compañía. Bien utilizada, la Intranet permite optimizar el acceso a los recursos de una organización, organizar los datos existentes en las PCs de cada individuo, y extender la tarea de colaboración entre los miembros de equipos de trabajo. Cuando la Intranet extiende sus fronteras más allá de los límites de la organización para permitir la intercomunicación con los sistemas de otras compañías, se convierte en una Extranet.

IP (Internet Protocol):
Protocolo de Internet definido en el RFC 791. Confirma la base del estándar de comunicaciones de Internet. El IP provee un método para fragmentar (deshacer en pequeños paquetes) y rutear (llevar desde el origen al destino) la información. Es inseguro, ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.

IP Número o dirección (IP address):
Dirección numérica asignada a un dispositivo de hardware (computadora, router, etc.) conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números, y cada uno de ellos puede ser de 0 a 255, por ejemplo 200.78.67.192. Esto permite contar con hasta 256 elevado a la 4 números para asignar a las computadoras: cerca de 4 mil millones. Las direcciones IP se agrupan en clases. Para convertir una dirección IP en una dirección electrónica humana (por ejemplo, www.iworld.com) se utilizan los DNS.

IPv6 (IP versión 6):
Propuesta para aumentar los números IP disponibles, utilizando seis grupos de números en lugar de cuatro. Más información sobre este nuevo estándar en http://www.cis.ohio-state.edu/htbin/rfc/rfc1885.html

IRC (Internet Relay Chat):
Uno de los sistemas más populares de charlas interactivas (chats) de múltiples usuarios vía Internet. Permite que miles de personas se reúnan a "conversar" en forma escrita con personas de todo el mundo simultáneamente.

IRTF (Internet Research Taskforce, Equipo de investigación de Internet):
Comunidad de investigadores de redes, generalmente enfocados en la Internet. Dedicados al avance tecnológico de la Red y asociados a la ISOC.

ISDN (Integrated Sevices Data Network, Red Digital de Servicios Integrados):
Tecnología rápida de conexión para líneas dedicadas y transmisión de datos. Se utiliza para acceder a Internet o a una videoconferencia. Si bien esta tecnología existe desde hace varios años, aún se encuentra poco difundida.

ISOC (Internet Society, Sociedad Internet):
Asociación civil sin fines de lucro integrada por profesionales, técnicos, investigadores y gente interesada en colaborar en la difusión, desarrollo y organización de la comunidad Internet. Esta constituida por capítulos (chapters), es decir, asociaciones regionales. Para más información http://www.isoc.org.arISP

(Internet Service Provider, Proveedor de servicios de Internet):
Ver Provider.

ISP (Internet Service Provider, Proveedor de servicios de Internet):
Ver Provider.

IAB (Internet Activities Board, Panel de Actividades de Internet):
Comité coordinativo creado para el diseño, ingeniería y administración de Internet. Supervisa al IETF.

IANA (Internet Assigned Numbers Authority, Autoridad de Asignación de Números de Internet):
Organismo que asigna los números IP a las instituciones que desean participar de Internet. Actualmente funciona junto a Internic.

ICANN (Internet Centre for Assigned Names and Numbers, Centro de Internet para la asignación de nombres y números):
Organismo de Internet muy importante, que se ocupa de otorgar grupos

de números IP y direcciones electrónicas a cada organización que desee conectarse a Internet, garantizando que sean únicas. Representado en la Argentina por la Cancillería (www.nic.ar). Más datos en http://www.icann.net.

IETF (Internet Engineering Taskforce, Fuerza de trabajo de Ingeniería de Internet):
Gran comunidad abierta de ingenieros, operadores, vendedores e investigadores cuyo propósito es coordinar la operación, administración y evolución de Internet. Más datos en http://www.ietf.org

IMO (In My Opinión, En Mi Opinión):
Una de las siglas utilizadas en los mensajes de Internet. También IMHO (In My Humble Opinion, En Mi Humilde Opinión).

Impressions (visualizaciones):
Unidad de medida que verifica cuántas veces un navegante ve un determinado banner de publicidad. Alternativa de click-through.

Inteligencia Artificial (Artificial Intelligence o AI):
Rama de la computación que analiza a la computadora y sus posibilidades de poseer inteligencia. La IA estudia las habilidades inteligentes de razonamiento, capacidad de extracción de conclusiones y reacciones ante nuevas situaciones de las computadoras y sus programas. El razonamiento es parecido al del cerebro humano (no es lineal, se aprende de cada situación). Existen dos ramas de la IA: la fuerte (strong), sostiene que llegará el día en que puedan construirse programas que sean realmente inteligentes y computadoras pensantes. La débil (weak) cree que las computadoras sólo pueden ser diseñadas para convertirse en importantes herramientas para modelar y simular el pensamiento humano.

Interface (interfaz):
Cara visible de los programas. Interactúa con los usuarios. La interface abarca las pantallas y su diseño, el lenguaje utilizado, los botones y los mensajes de error, entre otros aspectos de la comunicación computadora/persona.

Internet address:
Sinónimo de número IP. Número asignado que identifica a un server en Internet. Está compuesto por dos o tres partes: número de red, número opcional de sub-red y número de host. Ver direcciones electrónicas, DNS.

Internet Worm:
Programa similar a un virus de computadora creado por Robert Morris, un estudiante de Cornell University, que fue muy famoso en 1988. El Worm se aprovechó de una fallo de seguridad de un programa

de e-mail muy utilizado, y causó desastres al reproducirse sin límite, infectando y luego dejando catatónicas a la mayor parte de las computadoras conectadas a Internet. El pánico causado por el virus fue tan grande que generó el nacimiento de varios organismos dedicados a investigar los fallos de seguridad de los programas.

IP (Internet Protocol):
Protocolo de Internet definido en el RFC 791. Confirma la base del estándar de comunicaciones de Internet. El IP provee un método para fragmentar (deshacer en pequeños paquetes) y rutear (llevar desde el origen al destino) la información. Es inseguro, ya que no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.

IRC (Internet Relay Chat):
Uno de los sistemas más populares de charlas interactivas (chats) de múltiples usuarios vía Internet. Permite que miles de personas se reúnan a "conversar" en forma escrita con personas de todo el mundo simultáneamente.

IRTF (Internet Research Taskforce, Equipo de investigación de Internet):
Comunidad de investigadores de redes, generalmente enfocados en la Internet. Dedicados al avance tecnológico de la Red y asociados a la ISOC.

ISDN (Integrated Sevices Data Network, Red Digital de Servicios Integrados):
Tecnología rápida de conexión para líneas dedicadas y transmisión de datos. Se utiliza para acceder a Internet o a una videoconferencia. Si bien esta tecnología existe desde hace varios años, aún se encuentra poco difundida.

ISOC (Internet Society, Sociedad Internet):
Asociación civil sin fines de lucro integrada por profesionales, técnicos, investigadores y gente interesada en colaborar en la difusión, desarrollo y organización de la comunidad Internet. Esta constituida por capítulos (chapters), es decir, asociaciones regionales. Para más información http://www.isoc.org.arISP

JAVA:
Lenguaje de programación creado por Sun Microsystems. Desde su aparición, Java se perfila como un probable revolucionario de la Red. Como lenguaje es simple, orientado a objetos, distribuido, interpretado, robusto, seguro, neutral con respecto a la arquitectura, portable, de alta performance y dinámico. Java es un lenguaje de programación, un subset seguro de C++. Subset, porque algunas instrucciones (como las relacionadas con la administración de memoria)

no se pueden usar. Seguro, porque agrega características de seguridad a los programas. Un applet de Java se baja automáticamente con la página Web, y es compilado y ejecutado en la máquina local. Permite, entre otras cosas, agregar animación e interactividad a una página Web, pero su característica más importante es que un programa escrito en Java puede correr en una computadora de cualquier tipo. Para más datos http://java.sun.com

Javascript:
Lenguaje de scripts para utilizar en páginas Web, desarrollado por la empresa Netscape. Permite aumentar la interactividad y la personalización de un sitio.

LAN (Local Area Network, Red de Area Local):
Red de computadoras interconectadas, distribuida en la superficie de una sola oficina o edificio. Llamadas también redes privadas de datos. Su principal característica es la velocidad de conexión. Ver también WAN y MAN.

Línea dedicada (leased line):
Forma de conexión (con acceso las 24 horas) a través de un cable hasta un proveedor de Internet. Esta conexión puede ser utilizada por varias personas en forma simultánea.

Link:
Ver enlace.

Listas de interés:
Ver mailing list.

Listserv:
Software robot usado para la administración de un servidor de mailing list. Ampliamente utilizado.

Log:
En un servidor, archivo que registra movimientos y actividades de un determinado programa (log file). Utilizado como mecanismo de control y estadística. Por ejemplo, el log de un Web server permite conocer el perfil de los visitantes a un sitio Web.

Login:
Proceso de seguridad que exige que un usuario se identifique con un nombre (user-ID) y una clave, para poder acceder a una computadora o a un recurso. Ver Telnet.

Lynx:
Navegador de la Web en modo texto, que no permite ver imágenes. Es utilizado aún por quienes navegan desde estaciones UNIX.

Mail Robot (autoresponder):
Programa que responde e-mails en forma automática, enviando al instante información, catálogos, etc. Simplifica la tarea de administrar un correo. Los programas utilizados para administrar mailing lists son un tipo de mail robots.

Mailing List (listas de interés):
Modo de distribución grupal de e-mails. Mecanismos de debate entre distintas personas interesadas en un mismo tema. Similares en concepto a los newgroups, pero a diferencia de ellos, no es necesario utilizar un servidor especial ya que los mensajes son recibidos por el usuario como correo electrónico.

Majordomo:
Uno de los softwares de tipo mail robot usado para la administración de un mailing list.

MAN (Metropolitan Area Network, Red de Área Metropolitana):
Red que resulta de la interconexión de varias redes locales (LANs) a través de un enlace de mayor velocidad o backbone (por ejemplo de fibra óptica) distribuidas en varias zonas. Es el tipo de estructura de red que se utiliza, por ejemplo, en un campus Universitario, donde se conectan los diversos edificios, casa de estudiantes, bibliotecas y centros de investigación. Una MAN ocupa un área geográfica más extensa que una LAN, pero más limitada que una WAN.

MIME (Multipurpose Internet Mail Extensions, Extensiones Multipropósito para e-mail):
Formato especifico de codificación para la transferencia de correo electrónico y attachments entre dos computadoras, conteniendo cualquier tipo de datos. Más moderno que el UUEncoding; aunque menos difundido.

Mirror Site (Sitio espejado o duplicado):
Site que hace una copia, en forma regular o sistemática, de toda la información de otro site. Se utiliza para disminuir y repartir la cantidad de accesos a un sitio Web muy visitado o solicitado.

Módem (Modulador/Demodulador):
Dispositivo que se utiliza para transferir datos entre computadoras a través de una línea telefónica. Unifica la información para que pueda ser transmitida entre dos medios distintos, como un teléfono y una computadora. La velocidad del módem se mide en una unidad llamada baudios (bits por segundo), por ejemplo 28.800 baudios. Cuanto más rápido es el módem, más datos pueden viajar a través de él en menos tiempo.

MOOs (Multiuser Object Oriented MUDDs):
Similares a los MUDDs. Mosaic: primer browser de gran difusión, utilizado para navegar la Web. Desarrollado en febrero de 1993 por Marc Andreseen, fundador luego de la empresa Netscape.

Motor de búsqueda:
Ver Buscador.

Mudd (Multi User Dungeons & Dragons, castillos multi-usuarios):
Conjunto de juegos virtuales de texto para jugar a través de Internet con personas de todo el mundo. Originados en las universidades y basados en los llamados juegos de rol (role-playing games), consisten en «universos» virtuales con cientos de partes, definidos por programadores, donde los participantes deben resolver acertijos y enigmas requiriendo muchas veces, de la ayuda de otros jugadores. Son, junto con los chats, una de las actividades más adictivas de Internet.

Multimedia:
Combinación de varias tecnologías de presentación de información (imágenes, sonido, animación, video, texto) con la intención de captar tantos sentidos humanos como sea posible. Previamente a la existencia de la multimedia, el intercambio de información con las computadoras estaba limitado al texto. Luego, con el nacimiento de las interfaces de usuario gráficas, y los desarrollos en video y sonido, la multimedia permitió convertir el modo de comunicación entre personas y dispositivos, aumentando la variedad de información disponible. El uso de la multimedia fue la razón principal por la que la World Wide Web facilitó la difusión masiva de Internet.

No repudio*:*
Propiedad que se consigue por medios criptográficos, que impide a una persona o entidad negar haber realizado una acción en particular relativa a datos (como los mecanismos de no rechazo de autoría (origen); como demostración de obligación, intención o compromiso; o como demostración de propiedad).

Notario electrónico *(TTP, Trusted Third Parties):*
Entidad pública o privada encargada de la emisión de certificados digitales que atestigüen la autenticidad de los propietarios de los mismos.

NAP (Network Access Point, Centro de Acceso a la Red):
Punto de interconexión para intercambio de datos de dos o más conexiones pertenecientes a distintas organizaciones o ISPs.

Navegador:
Ver browser.

Navegar:
Recorrer la Web sin destino fijo, siguiendo distintos enlaces o direcciones.

Netiquette:
Reglas de etiqueta, usos y buenas costumbres de Internet. Surgieron como una serie de políticas informales de «buen comportamiento», y se difunden de usuario en usuario para mantener vivo el espíritu de respeto propio de la Red. Un ejemplo de estas reglas es no escribir mensajes completos de correo electrónico en letras MAYUSCULAS, ya que significa GRITAR!

Network:
Ver Red.

Newsgroup (grupos de debate o discusión):
Mecanismos de debate grupales entre personas de todo el mundo interesadas en un mismo tema. Los Newsgroups permiten crear mensajes públicos, que los usuarios pueden crear, leer y contestar. Son distribuidos diariamente por todo Internet. También se define de esta manera al área en la cual se agrupan los mensajes públicos según su temática.Similares en concepto a las mailing lists.

Nickname (Nick, del inglés: sobrenombre o alias):
Nombre de fantasía que un usuario de Internet utiliza, por ejemplo para participar de un Chat.

NNTP (Network News Transfer Protocol):
Protocolo estándar de Internet utilizado para el intercambio y transferencia de Newsgroups entre servidores.

Norma (o estándar):
Conjunto de reglas sobre algún producto o servicio que garantiza uniformidad en todo el mundo y en cualquier sistema en el que se implemente. Existen dos tipos de normas: la estándar (o normada), generada por comités especiales, y la de facto (o impuesta) que se acepta cuando la difusión de su uso la convierte en universal. Los tres organismos más activos en el desarrollo normas son: la ISO (International Standards Organization), la IEEE (American Institution of Electrical and Electronic Engineers) y la CCITT (International Telegraph and Telephone Consultative Comitee). Las normas son la base de los Sistemas Abiertos.

NSF (National Science Foundation):
Organismo norteamericano que administra los recursos que el gobierno otorga a las áreas científicas. De gran incidencia en los primeros tiempos de Internet.

NSLookup (antiguamente conocido como Yellow Pages):
Programa que consulta al DNS para resolver direcciones IP en las direcciones de dominio correspondientes.

Número IP:
Ver IP, número

Off-line (del inglés, fuera de línea):
Estado de comunicación diferida, opuesta a la de tiempo real.

On-line (del inglés, en línea):
Estado de comunicación activa, también llamado de tiempo real.

Overhead:
Desperdicio de ancho de banda causado por la información adicional (de control, de secuencia, etc.) que debe viajar, además de los datos en los paquetes de un medio de comunicación. El overhead afecta al Throughput de una conexión .

Página (page o Webpage):
Unidad que muestra información en la Web. Una página puede tener cualquier longitud, si bien equivale por lo general a la cantidad de texto que ocupan dos pantallas y media. Las páginas se diseñan en un lenguaje llamado HTML, y contienen enlaces a otros documentos. Un conjunto de páginas relacionadas componen un site.

Password (del inglés, clave o contraseña):
Palabra utilizada para validar el acceso de un usuario a una computadora servidor.

PDN (Public Data Network, Red pública de Datos):
Red establecida y operada por una autoridad de transmisión de datos con el objetivo de establecer comunicaciones.
PGP (Pretty Good Privacy): Programa de libre distribución, escrito por Phil Zimermann, que impide, mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser interpretados por personas no autorizadas. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autenticación del autor.

PGP (Pretty Good Privacy, Muy Buena Privacidad):
Software de encriptación freeware muy utilizado, desarrollado por Paul Zimmerman. Se basa en el uso de un método de clave pública y clave

privada, y es extremadamente seguro. Su eficacia es tal, que los servicios de inteligencia de varios países ya han prohibido su uso. Más datos en http://www.pgpi.com

Ping (Unix):
Herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP entre dos computadoras de cualquier parte de Internet.

Pipe:
Conexión, cable, línea, enlace. Ver Línea dedicada. Plug & Play: tecnología que permite agregar dispositivos a una computadora (por ejemplo, CD-ROMs o placas de sonido) que se conectan y configuran automáticamente.

Plug-in (agregado):
Programa agregado que extiende las habilidades de un navegador, permitiéndole mayor funcionalidad. Por ejemplo, se puede agregar un plug-in al navegador que permita ver videos, participar de un juego grupal o realizar una videoconferencia.

Port (puerto):
Conexión lógica y/o física de una computadora, que permite comunicarse con otros dispositivos externos (por ejemplo, una impresora) o con otras computadoras. Los servicios de Internet (como el e-mail o la Web) utilizan ports lógicos para establecer comunicaciones entre una computadora cliente y un servidor.

Postmaster:
Administrador humano de un servidor Internet. Cuando se desea efectuar una consulta sobre algún usuario de ese server, se envía un e-mail al postmaster quién responderá la consulta. Ver Sysop y Webmaster.

PPP (Point to Point Protocol):
Protocolo serial para el acceso telefónico a Internet (dial-in). Más moderno que el SLIP. Estándar normado (RFC 1134), multiprotocolo y que admite algoritmos de compresión y autenticación de los datos que viajan. Aún no es soportado por algunos softwares de conexión.

Programa:
Sinónimo de software. Conjunto de instrucciones que se ejecutan en la memoria de una computadora para lograr algún objetivo. Creados por equipos de personas (llamados programadores) en lenguajes especiales de programación. Se les diseña una interface de usuario para que puedan interactuar con las personas que los utilicen.

Protocolo:
Conjunto de reglas formuladas para controlar el intercambio de datos entre dos entidades comunicadas. Pueden ser normados (definidos por un organismo capacitado, como ser la CCITT o la ISO) o de facto (creados por una compañía y adoptados por el resto del mercado).

Provider (Proveedor, ISP o Intermediario):
Empresa que actúa de mediador entre un usuario de Internet y la Internet en sí misma. Ofrece el servicio de conexión dial-in o dedicado, y brinda servicios adicionales como el Web farming.

Proxy Server (intermediario, mediador):
Utilizado en relación a Internet, hace referencia a un servidor que media entre el usuario (su computadora) y otro servidor de la Red. El Proxy Server puede hacer, por ejemplo, un pedido de información para un cliente en lugar de que el cliente lo haga directamente (método usado para salir de un firewall). También pueden actuar como traductores de formato de archivos (por ejemplo, convertir toda imagen GIF que pase por ellos en un BMP, o traducir del inglés al castellano, o convertir los attachments), o como cachés (almacenando en un directorio los archivos de mayor uso reciente, para entregarlos ante una nueva solicitud sin necesidad de que el usuario los busque por toda Internet), verificar la seguridad (virus, accesos permitidos, etc.), entre otras muchas tareas.

Página (page o Webpage):
Unidad que muestra información en la Web. Una página puede tener cualquier longitud, si bien equivale por lo general a la cantidad de texto que ocupan dos pantallas y media. Las páginas se diseñan en un lenguaje llamado HTML, y contienen enlaces a otros documentos. Un conjunto de páginas relacionadas componen un site.

Password (del inglés, clave o contraseña):
Palabra utilizada para validar el acceso de un usuario a una computadora servidor.

PDN (Public Data Network, Red pública de Datos):
Red establecida y operada por una autoridad de transmisión de datos con el objetivo de establecer comunicaciones.

Pesos vencidos:
Los **tokens** tienen una fecha de vencimiento. En el momento de llegar a la mencionada fecha es factible que el total de dinero disponible en el **token**, no haya sido consumido. Este residual se denomina **'pesos vencidos'**.

PGP (Pretty Good Privacy, Muy Buena Privacidad):
Software de encriptación freeware muy utilizado, desarrollado por Paul Zimmerman. Se basa en el uso de un método de clave pública y clave privada, y es extremadamente seguro. Su eficacia es tal, que los servicios de inteligencia de varios países ya han prohibido su uso. Más datos en http://www.pgpi.com

Query (del inglés, consulta):
Formulación de consulta en una base de datos, en general organizada en un formato básico definido por un lenguaje estructurado.

Red (network):
Dos o más computadoras conectadas para cumplir alguna función, como compartir periféricos (impresoras), información (datos, sistema de ventas) o comunicarse, (correo electrónico). Existen varios tipos de redes. Según su estructura jerárquica se catalogan en redes client/server -con computadoras que ofrecen información, y otras que sólo la consultan-, y las peer-to-peer, donde todas las computadoras ofrecen y consultan información simultáneamente. A su vez, según el área geográfica que cubran, las redes se organizan en LANs (locales), MANs (metropolitanas) o WANs (área amplia).

Red Local :
Ver LAN.

Request (pedido):
Solicitud de información o datos que una computadora cliente efectúa a un servidor. RFC (Request For Comment, pedido de comentario). Documentos a través de los cuáles se proponen y efectúan cambios en Internet, en general con orientación técnica. Los RFCs son formularios con una estructura determinada, que pueden ser generados y distribuidos por cualquier persona que tenga una buena idea para cambiar, o mejorar, algún aspecto de Internet. Las propuestas que contienen estos documentos se analizan, modifican y se someten a votación. Si resultan útiles, son puestas en práctica, convirtiéndose así en normas de Internet. La mayoría de los aspectos técnicos de la Red de redes nacieron primero como RFCs creados por distintas personas, por eso hoy en día hay cientos de ellos. Se puede consultar una base de datos hipertextual de los RFC en http://www.auc.dk/RFC . RFD (Request For Discussion, pedido de debate). Similar a los RFCs, pero se emiten para llamar a debate sobre determinado tema. RFV (Request For Vote, pedido de votación). Similar a los RFCs, pero se emiten para llamar a "Votación" antes de aprobar alguna norma, cambio, o decisión, que pueda afectar a toda la comunidad Internet.

R-login (Remote Login):
Acceso a un server desde un sistema remoto. Ver Telnet.

Router (ruteador):
Dispositivo de conexión y distribución de datos en una red. Es el encargado de guiar los paquetes de información que viajan por Internet hacia su destino. Ver TCP/IP, LAN.

ROT13:
Método de pseudo-encriptación de datos en un mensaje público, utilizado para disimular el envío de un texto que pueda molestar a algunas de las personas que lo lean. Para leerlo, hay que reemplazar cada letra por la correspondiente a la que la precede 13 lugares en el alfabeto, ej. la "N" por la "A", etc. Por ejemplo, la frase "Esto está codificado con ROT13" se leería "Rfgb rfgn pbqvsvpnqb pba EBG13". Muchos programas de newsgroups pueden realizar este proceso de conversión, en forma automática.

Servidor Web:
Es el programa que, utilizando el protocolo de comunicaciones HTTP, es capaz de recibir peticiones de información de un programa cliente (navegador), recuperar la información solicitada y enviarla al programa cliente para su visualización por el usuario.

Servidor Web seguro:
Servidor Web que utiliza protocolos de seguridad (SSL, SHTTP o PCT) el ejecutar transacciones en él. Un protocolo de seguridad utiliza técnicas de cifrado y autenticación como medios para incrementar la confidencialidad y la fiabilidad de las transacciones.

SET *(Secure Electronic Transactions):*
Protocolo creado para proporcionar mayor seguridad a los pagos on-line con tarjetas de crédito verificando la identidad de los titulares de las tarjetas con "certificados digitales" y encriptando los números de las tarjetas durante todo el trayecto, desde el navegante, el vendedor y el centro de proceso de datos. Este estándar ha sido creado por VISA y Master Card y tiene un amplio apoyo de la comunidad bancaria mundial.

Sistema de gestión de claves:
Sistema para la generación, almacenamiento, distribución, revocación, eliminación, archivo, certificación o aplicación de claves criptográficas.

Sistemas de información*:*
Ordenadores, instalaciones de comunicación y redes de ordenadores y de comunicación, así como los datos e informaciones que permiten conservar, tratar, extraer o transmitir, incluidos los programas, especificaciones y procedimientos destinados a su funcionamiento, utilización y mantenimiento.

SSL *(Secure Sockets Layer):*

Protocolo, creado por Netscape, para crear conexiones seguras al servidor, de tal modo que la información viaja encriptada a través de Internet.

Script:
Programa no compilado realizado en un lenguaje de programación sencillo. Vea JavaScript.

Search Engine:
Vea Buscador

Server side CGI script:
Script CGI que se ejecuta/corre en el servidor. Ver también Client side CGI script.

Server (servidor de información):
Computadora que pone sus recursos (datos, impresoras, accesos) al servicio de otras a través de una red. Ver Host, Client/Server.

Service Provider:
Ver Provider.

Servidor:
Ver Server.

SGML (Standard Generalized Markup Language, Lenguaje de Marcado Generalizado Normado):
superconjunto de HTMLs. Lenguaje que define a otros lenguajes con tags, base del HTML utilizado en la Web.

Shareware:
Política de distribución de programas donde se tiene derecho a probar un software por un determinado período, antes de decidir su compra. El importe a abonar por el programa es en general bajo, prácticamente nominal. Ver Freeware.

Sistema Operativo:
Conjunto de programas que se encarga de coordinar el funcionamiento de una computadora, cumpliendo la función de interfaz entre los programas de aplicación, circuitos y dispositivos de una computadora. Algunos de los más conocidos son el DOS, el Windows y el UNIX.

Sistemas Abiertos:
Conjunto de computadoras de distintas marcas que se interconectan utilizando el mismo protocolo normado de comunicación. El protocolo estándar más difundido es el TCP/IP.

Site (sitio):
En general, se lo utiliza para definir un conjunto coherente y unificado de páginas y objetos intercomunicados, almacenados en un servidor. Formalmente la definición sería: un servicio ofrecido por un server en un determinado port. Esta definición no siempre establece una correspondencia entre un solo site y un server. Varios servers pueden responder a un mismo site (por ejemplo los ocho que componen el buscador Yahoo) o también es posible que un solo server atienda simultáneamente a varios sites, como los de los proveedores de Web Farming

SLIP (Serial Line Internet Protocol, Protocolo Internet para Líneas Seriales):
Norma de facto para comunicaciones dial-in en Internet, creada en los años '80. Ampliamente utilizada, no admite sin embargo algoritmos de compresión ni de autenticación de los datos que viajan. Está siendo reemplazado por el PPP. Ver CSLIP.

Smilies:
Ver Emoticons.

SMTP (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo):
Protocolo estándar de Internet para intercambiar mensajes de correo electrónico.

Snail mail (correo caracol):
Modo en que se conoce el correo postal común en Internet. Juego de palabras que alude a su lentitud cuando se lo compara con la inmediatez del e-mail.

SNMP (Simple Network Management Protocol, Protocolo Simple para el Manejo de Redes)
Protocolo del TCP/IP usado para controlar remotamente el estado de los dispositivos de una red.

Software:
Componentes intangibles (programas) de las computadoras. Complemento del hardware. El software más importante de una computadora es el Sistema Operativo.

Spam:
Mensaje electrónico no solicitado y enviado a muchas personas. Considerado una mala práctica del marketing directo por quienes desconocen las reglas de Netiquette.

Spiders (arañas):
Complejos programas que recorren la Web siguiendo enlace tras

enlace cada página; almacena estas últimas para que más tarde sean catalogadas en las enormes bases de datos de los índices de búsqueda.

Standard:
Ver Norma.

Streaming (Transferencia Continua):
Sistema de envío continuo de información que permite, por ejemplo, ver un video a medida que se lo está bajando de la Red.

Stylesheets (hojas de estilo):
Novedosa facilidad de HTML, similar a la que poseen los procesadores de texto, que permite definir un parámetro de diseño y que se repite en todas las páginas de un sitio.

Sysop (System Operator, Operador del Sistema):
Persona encargada de la administración y el mantenimiento de un host. Ver Postmaster y Webmaster.

Tarjetas Inteligentes:
Tarjetas plásticas, similares a una tarjeta de crédito, que contienen una microficha que puede usarse para recuperar, almacenar, procesar y transmitir datos digitales tales como dinero electrónico o información médica.

Tag (etiqueta):
Código marcador de estructura de lenguaje HTML utilizado para estructurar las páginas de la Web.

TCP (Transmission Control Protocol, Protocolo de Control de Transmisión):
Conjunto de protocolos de comunicaciones que se encargan de la seguridad y la integridad en la transmisión de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP.

TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo Internet):
Conjunto de casi 100 programas de comunicación de datos, usados para organizar redes de computadoras. Norma de comunicación en Internet, compuesto por dos partes: el TCP/IP. El IP desarma los envíos en paquetes y los rutea, mientras que el TCP se encarga de la seguridad de la conexión, comprueba que lleguen los datos en forma completa, y que compongan finalmente el envío original.

Teleconferencia:
Sistema que permite conversar con una o varias personas simultáneamente, recibiendo sus imágenes en movimiento (video) además de sus voces.

Telnet (Unix):
Programa que permite el acceso remoto a un host. Utilizado para conectarse y controlar computadoras ubicadas en cualquier parte del Planeta.

Thread, threaded messages (hilación, mensajes hilados):
Mensajes de correo electrónico, (de un newsgroup o una lista de interés), relacionados al mismo tema, o que son respuestas a un mismo asunto.

Throughput:
Rendimiento final de una conexión. Volumen de datos que una conexión brinda como resultante de la suma de su capacidad, y la resta de los overheads que reducen su rendimiento. Ver Red.

Token:
Este concepto define a un comprobante virtual (un número y una clave) la cual está asociada a la una cantidad de dinero. El mismo puede usarse para realizar pagos en negocios que lo acepten como medio de pago.

Unix:
Sistema operativo diseñado por los Laboratorios Bell y refinado en la universidad de Berkley (California), entre otros lugares, que soporta operaciones multiusuario, multitasking y estándares abiertos. Ampliamente difundido en la Internet, es utilizado para ejecutar en los servidores.

Upgrade:
Actualización o mejora de un programa.

Upload (subir):
Proceso de enviar un archivo desde una computadora, a otro sistema dentro de la red. Ver. Download, FTP.

URL (Uniform Resource Locator, Localizador Uniforme de Recursos):
Dirección electrónica (ejemplo: iworld.com.ar). Puntero dentro de páginas HTML que especifican el protocolo de transmisión y la dirección de un recurso, para poder accederlo en un server de Web remoto.

User Account:
Cuenta de usuario. Similar a user ID.

User ID:
Identificación del usuario en una computadora. Relacionado con una clave de acceso o password.

UUCP (Unix to Unix CoPy):
Antiguo protocolo de comunicaciones para intercambio de mensajes y archivos, mayormente utilizado por computadoras que utilizan el Sistema Operativo UNIX.

UUEncoding:
Mecanismo de conversión que permite adjuntar (attachment) cualquier tipo de archivo a un mensaje, codificando el archivo en caracteres ASCII para que los sistemas en Internet lo puedan entender y transmitir. Similar al MIME, aunque menos moderno y más difundido.

Verisign:
La más conocida de las Autoridades Certificantes.

Virus:
Pequeños programas de computadora que tienen la capacidad de autoduplicarse y parasitar en otros programas. Una vez que se difunden, los virus se activan bajo determinadas circunstancias y, en general, provocan algún daño o molestia. Ver Worm.

Verónica (Very Easy Rodent-Oriented Netwide Index to Computarized Archives):
Una herramienta de búsqueda, que explora bases de datos de Gophers. Ver Gopher.

W3C (World Wide Web Consortium):
Organización que desarrolla estándares para guiar el desarrollo y expansión de la Web. Organizado por el CERN y el MIT (Massuchusetts Institute of Technology) y apadrinado por varias empresas. Su Website es http://www.w3.org. Ver Sistemas Abiertos.

WAIS (Wide Area Information Services, Servicio de Información de Grandes Areas):
Herramienta que permite la búsqueda de información en grandes bases de datos remotas. Cayó en desuso desde el nacimiento de la World Wide Web.

WAN (Wide Area Network, Red de Area Amplia):
Resultante de la interconexión de varias redes locales situadas en diferentes sitios (distintas ciudades, distintos países), comunicadas a través de conexiones públicas (líneas dedicadas). La conexión puede ser física directa (un cable), o a través de un satélite, por ejemplo. La conexión es más lenta que una LAN. Ver MAN, RED.

Wanderer (vagabundo):
Ver Spider.

Webmaster:
Administrador y/o autor de un sitio Web. Vea Postmaster.

WebTV:
Dispositivo que cruza una PC simple con un televisor. Tiene como fin abaratar los costos de acceso a la red y simplificar su uso. Si bien fue lanzado en diciembre de 1996, hasta ahora ha tenido poca difusión. Más datos en http://www.webtv.com

White Pages (páginas blancas):
Listado de direcciones electrónicas de usuarios de Internet.

Whiteboard (pizarrón blanco):
Programa especial para trabajo en grupo que permite que varias personas participen de un proyecto a la vez. Por ejemplo, una presentación o un presupuesto. Aunque las personas no estén físicamente en un mismo lugar, pueden trabajar desde cualquier punto del planeta a través de Internet. Ver Groupware.

Workstation (estación de trabajo):
Puesto de trabajo o computadora de un usuario. Similar al concepto de Cliente. También reciben ese nombre pequeños servidores con gran capacidad gráfica, como los de Silicon Graphics.

World Wide Web, o W3, o WWW:
Conjunto de servidores que proveen información organizada en sitios, cada uno con cierta cantidad de páginas relacionadas. La Web es una forma novedosa de organizar toda la información existente en Internet a través de un mecanismo de acceso común de fácil uso, con la ayuda del hipertexto y la multimedia. El hipertexto permite una gran flexibilidad en la organización de la información, al vincular textos disponibles en todo el mundo. La multimedia aporta color, sonido y movimiento a esta experiencia, haciendo versátil y rico el contenido. El contenido de la Web se escribe en lenguaje HTML y puede utilizarse intuitivamente mediante un programa llamado navegador. Se convirtió en el servicio más popular de la Red y se emplea cotidianamente para los usos más diversos: desde leer un diario de otro continente, hasta participar de un juego grupal.

Worm (gusano):
Tipo de programa similar al virus que se distribuye en una red. Generalmente, su objetivo es afectar o dañar el funcionamiento de las computadoras.

X25:
Uno de los tantos protocolos estandarizados bajo normas internacionales, de comunicación packet-switching. Utilizado ampliamente en redes públicas de comunicaciones.

Yellow Pages (páginas amarillas):
Listado de direcciones electrónicas de comercios en Internet. Ver White Pages.

14 ACRÓNIMOS

AOL	America On Line
APD	Agencia de Protección de Datos
ATM	Automatic Teller Machine
BCE	Banco Central Europeo
C2C	Consumer to Consumer
CA	Autoridad Certificante
DES	Data Encryption Standard
FBOI	First Bank of Internet
HTML	Hyper Text Markup Language
ID	Identificación
MIT	Instituto de Tecnología de Massachusetts
NYT	New York Times
P2P	Person to Person
PGP	Pretty Good Privacy
PIN	Personnel Identification Number
PKCS	Public Key Cryptographic System
POS	Pont of Sale
RSA	Rivest-Shamir-Adleman
SEPP	Secure Electronic Payment Protocol
SET	Secure Electronic Transaction
SSL	Secure Socket Layer
TC	Tarjeta de Crédito
TCP/IP	Protocolo de Transmisión de Datos
TD	Tarjeta de Débito
TSR	Terminate and Stay Resident
WWW	World Wide Web
XOR	Operación de Boole – OR exclusivo

15 REFERENCIAS BIBLIOGRÁFICAS Y FUENTES DE INFORMACIÓN CONSULTADAS

Dávila Jorge, El dinero electrónico (I) , Enero 2000

Törnroth Jonas, A server based wireless wallet enabling secure payment transactions, Master Thesis, Marzo 2000

Recent Fraud Statistics, www.cybersource.com/fraud_resource_center/

Overview of secure electronic payment systems, www2000.ogsm.Vanderbilt.edu/

El uso del dinero electrónico en transacciones de comercio electrónico, www.isaca.org/

El dinero físico y su desaparición, publicaciones.derecho.org/redi/

El derecho en la era digital. Aspectos jurídicos de las nuevas tecnologías de la información y de las comunicaciones, publicaciones.derecho.org/redi/

Ragoni Rodolfo, E-money, Editorial Prentice Hall, Marzo 2001