Parte de la información obtenida en Internet es una fuente de preocupación par los usuarios, para los gobiernos y para las propias empresas del sector

Comercio electrónico, Internet y su seguridad

Los usuarios preocupados por la información accesible por Internet, afecte a sus hijos, los gobiernos tropiezan con inquietantes obstáculos en la lucha contra las informaciones ilícitas y nocivas, y las empresas que ofrecen sus servicios en la red comparten estas preocupaciones. La seguridad en Internet es vital para el desarrollo del mismo y del comercio electrónico según Forrester Research.

Desde el punto de vista de la gestión, habría que analizar las siguientes áreas relacionadas con la seguridad:

- Acceso del usuario (identidad y autorización de acceso de usuario). ∑ Seguridad de las bases de datos, de las aplicaciones informáticas y de la información (es decir: aplicaciones informáticas para la seguridad). • Seguridad en el comercio electrónico (en el pago y en las transacciones). • Seguridad en la red. • Seguridad y control en la detención de los contenido ilícitos y nocivos en Internet. • Mantenimiento y gestión de la seguridad (p.e. sistemas de control y seguimiento de la piratería informática).

INQUIETUDES DE LA INTERNET

Estas inquietudes tienen su origen en los contenidos que circulan en Internet como consecuencia de un uso ilegítimo ó abusivo. Ciertamente, la mayor parte de los contenidos plantean problemas a:

- Los **usuarios:** padres y educadores, temiendo que sus hijos ó alumnos se encuentren con pornografía ó racismo.
- Los **gobiernos** tropiezan con inciertos obstáculos en la lucha contra las informaciones ilícitas y nocivas, y de ofrecer garantías a los usuarios en el comercio electrónico (claves, contratos, pagos, pedidos, etc.). No es fácil localizar a un autor anónimo en la red.
- Las **empresas** que ofrecen sus servicios a través de Internet y contribuyen a la difusión de la información también comparten estas preocupaciones, por poder ser considerados responsables y verse así perjudicada su actividad comercial y por tanto, el despegue del comercio electrónico.

Todo ello ha sido motivado por el propio carácter del Internet:

1.- Su carácter transacional y alcance global.

2.- La ausencia de regulación, sin embargo en el ultimo año tanto España como la COMUNIDAD EUROPEA (C.E.) está haciendo un gran esfuerzo.

3.- Por la ausencia de una autoridad, que controle los contenidos de Internet.

CONTENIDOS LÍCITOS Y NOCIVOS EN INTERNET

Aclaremos cual es la diferencia que existe entre los contenidos de Internet lícitos y nocivos: los contenidos **ilícitos** son merecedores de una respuesta penal: pornografía, contenidos racistas, etc. Los contenidos **nocivos**, estos aunque dañinos para determinadas personas en base a sus valores éticos, religiosos o políticos, no son merecedoras de respuesta penal.

Los proveedores, según el principio general del Derecho, del derecho de contenidos son responsables civil y penal. El problema surge cuando se ampara en el anonimato.

En España, en 1999 se reforma el Código Penal para así adaptarlo a estos nuevos delitos. En

• José Carlos Jiménez Sabio
Ingeniero de Telecomunicación e Ing. Tec. Industrial y Gerente del Centro Comercial Radiovisión S.A.

el Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico 29-09-00, se recogen la responsabilidad contraída por los prestadores de servicios de la sociedad de la información, relaciones de ciertos contenidos atentado salud publica; motivos de raza, sexo, etc.; orden publico, seguridad publica; protección de menores; necesidad de inscripción (en el Ministerio de Ciencia y Tecnología); supervisión de los contenidos y comunicación a la autoridad si es ilícita y nociva, aunque siempre amparado en el principio de no supervisión y obligación de información; códigos de conducta; etc.

Además, se han creado organismos especializados como los departamentos creados en la Guardia Civil y la Policía Nacional.

Gracias a la Directiva 2000/31/CE de 8-06-2000, directiva sobre el comercio electrónico, ha supuesto convertir Internet en un espacio seguro dentro de Europa. La directiva supone una armonización respecto de las exoneraciones de la responsabilidad penal y civil de los proveedores de servicios en Internet, muy en línea con la DMCA estadounidense, que establece el régimen de responsabilidad de los prestadores de servicios por la vulneración de los derechos de la propiedad.

COMERCIO ELECTRÓNICO

Podemos decir de forma general, que comercio electrónico es el intercambio electrónico de datos e informaciones correspondientes a una transacción.

El comercio electrónico puede tener varias definiciones, veamos:

Desde el punto de vista de las empresas, (tecnología, automatización, etc.).

Desde la perspectiva de las comunicaciones (productos, servicios o juegos, redes, etc.).

De los servicios, (mejorar calidad, rebajar costes, etc.).

Desde el punto de vista del Internauta (comprar- vender, productos e información, etc).

El modelo de comercio electrónico se refleja en la figura 1.

En éste modelo, la entrega del producto vendido ha sido sustituido por un Flujo de información que hace referencia a la descripción del producto, entrega, fecha de envío, transporte, etc.

Según Ravi Kalakota, catedrático de la Universidad de Rochester define el comercio electrónico como "el proceso de conversión de inputs digitales, en outputs de valor añadido". El comercio electrónico puede considerarse como un proceso de producción en línea que pertenece a los intermediarios. Los productores (vendedor) de información interactúan con intermediarios (procesos en línea). El outputs resultante (comprador) Toma la forma de un producto ó servicio digital u otro tipo de información procesada, como pedidos, pagos o instrucciones. Este modelo es el de la figura 2.

A través de este marco podemos observar el conjunto de factores que intervienen en este proceso.

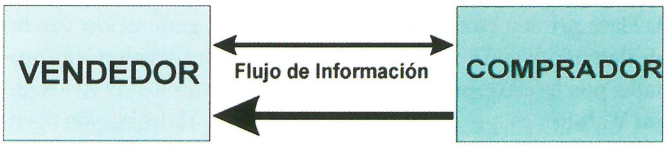

Fig.1. Modelo Comercio electrónico

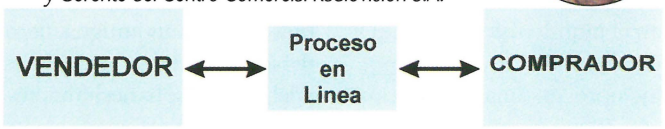

Fig. 2. El proceso de creación de valor digital

MODELO DE COMERCIO ELECTRÓNICO

Podemos separar el Comercio electrónico en dos grandes áreas:

1) Comercio electrónico cerrado (es el que se desarrolla entre empresas por acuerdos entre ellas).
   - B2B: El realizado entre empresas; ∑ B2A: Transacciones entre empresas y Administración.
2) Comercio electrónico abierto (es la que se realiza sobre la WEB de una forma no programada por compradores compulsivos)
   - B2C: se realiza entre empresa y consumidor fiel.; ∑ A2C: Las transacciones entre Administración y ciudadano. ∑ C2C: Operaciones de trueque o ventas entre ciudadanos.

LA IMPORTANCIA DE SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Es cierto que Internet no se concibió pensando en el comercio electrónico; sin embargo su gran fortaleza y fiabilidad han aumentado exponencialmente en los últimos años.

Soluciones Off line versus soluciones On Line.

En el cuadro que detallamos a continuación sintetizamos las

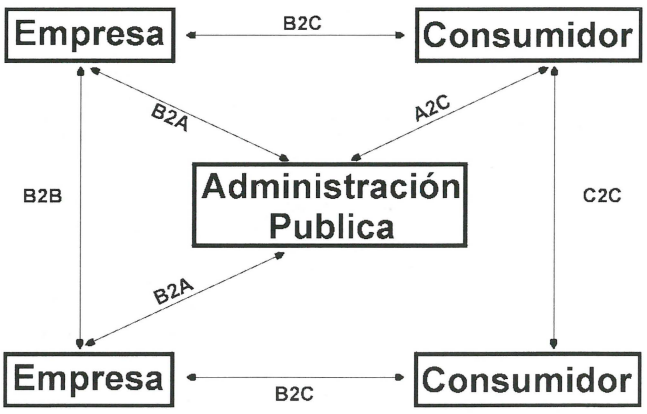

Fig. 3 Modelos de comercio electrónico

distintas soluciones empleadas en el mundo físico (off line) y en el mundo virtual (on line). Siempre en una transacción comercial o mercadera, es algo más que vender, es la relación entre unos y otros (vendedor y comprador) generando una discusión dialéctica entre vendedor y comprador, tal como se puede resumir com o en la figura 5.

LA CRIPTOGRAFÍA: CONCEPTOS BÁSICOS

La criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. Esta es una ciencia muy antigua, pero debido al uso de los ordenadores y del Internet, se ha hecho imprescindible para preservar al ciudadano su intimidad.

El esquema fundamental de un proceso criptográfico (cifrado/descifrado) se muestra en la figura 6.

Las técnicas criptográficas debe conseguir varias metas por este orden:

* Mantener la confidencialidad del mensaje: Es decir, que la información allí contenida permanezca secreta.
* Garantizar la autenticidad tanto del criptograma (Integridad) como del par remitente/destinatario.

	SOLUCIONES OFF LINE	SOLUCIONE ON LINE
CONFIDENCIALIDAD	Sobres	Encriptación
INTEGRIDAD	Firmas	Firmas digitales
AUTENTIFICACION	Notarios	Certificados digitales

Fuente: Global Intergrity

Fig. 4. Soluciones de seguridad

	Vendedor	Comprador
Autentificación	Saber la identidad del que compra antes de realizar la compra	Confirmar la identidad del vendedor antes de comprar.
Certificación	El vendedor puede necesitar una "prueba" de que el comprador esta capacitado para comprar.	
Confirmación	El vendedor necesita saber ante cualquier 3º (emisor tarjeta de credito) que el comprador autorizó el pago	El comprador necesita un "recibo" de la compra realizada.
No repudio	El vendedor quiere protegerse de que el comprador niegue injustificadamente haber realizado la compra o haber recibido el producto	El comprador esta interesado en poder recurrir en el caso de que el vendedor no cumpla las obligaciones acordadas.
Pago	El vendedor necesita asegurarse de que si cumple con lo acordado se efectuara el pago.	El comprador quiere asegurarse que no se pueda realizar ningún pago sin su consentimiento.
Privacidad		El comprador puede estar interesado en que no aparezca su nombre o identidad en la transacción.

Fig. 5. Requerimientos de Seguridad

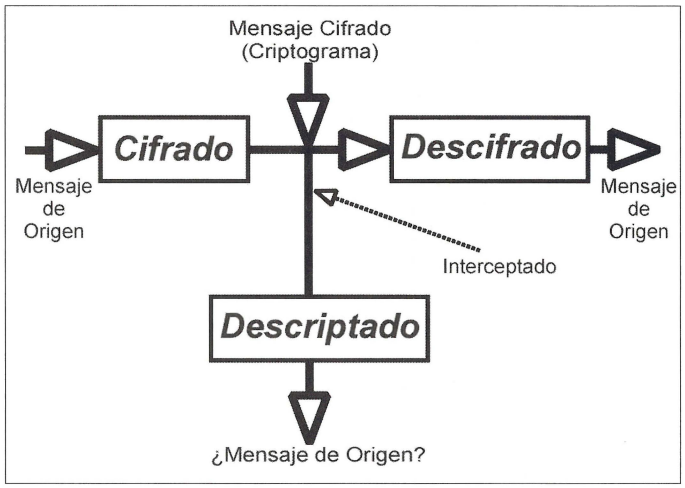

Fig. 6. Proceso General Criptografico

Una primera clasificación en base a las claves utilizadas puede desglosarse así:

* Métodos simétricos o criptografía en clave secreta: son aquellos en los que la clave de cifrado coincide con la de descifrado.
* Métodos asimétricos o criptografía de clave publica (PKI): son aquellos en que la clave de cifrado es diferente a la de descifrado.

Los algoritmos mas usados actualmente son el DES, RC2, RC4 (algoritmo simétrico) y el RSA, DSS (algoritmo asimétrico).

FUNCIONALIDAD DE SISTEMA PKI

Los sistemas criptográficos de clave pública funcionan como dos claves: una clave pública utilizada para encriptar el mensaje, y otra clave privada, que es la que se utiliza para desencriptarlo. La razón por lo que la clave privada (secreta) puede desencriptar el texto encriptado por la clave pública (en un Website) es que ambas claves están relacionadas matemáticamente a través de una función HASH o unidireccional.

Según figura 7, vemos necesario una "Infraestructura de Clave publica" (Public Key Infraestructure, PKI) que haga funcionar el sistema de forma eficiente y segura.

El sistema PKI debe crear confianza (Trust) entre empresas y consumidores en las comunicaciones electrónicas (Internet), en los aspectos comerciales, legales, oficiales, personales, etc., a través de entidades centrales o TRUST@.

De esta forma las funciones de una PKI tendrá tres facetas:

Tecnológicas Una PKI es un conjunto de Software, hardware, sistemas criptográficos y tecnologías de Interface; 2) Bussiness. Es el sistema que integra las distintas organizaciones que participan en la gestión de una PKI de forma que ahorre costes y genere confianza; 3) Legal. Es el conjunto de entidades y servicios de autentificación, certificación, generación (de las claves), contratación, etc. proporcionando los servicios: de acuerdo con la legislación vigente; por interés de los usuarios.

La firma digital debe generar

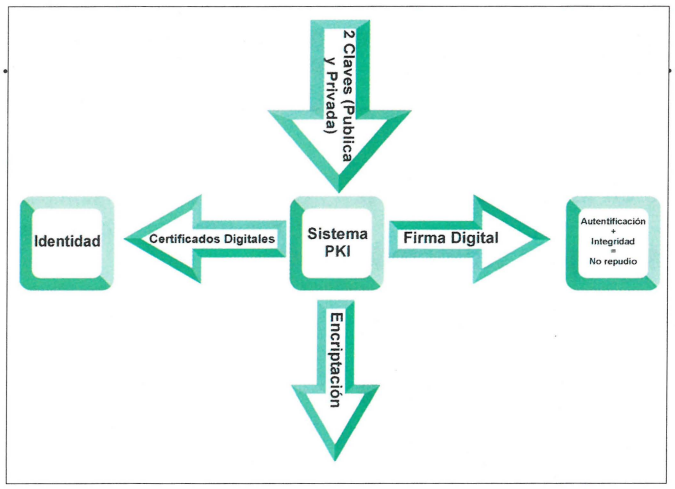

Fig. 7. Sistema PKI

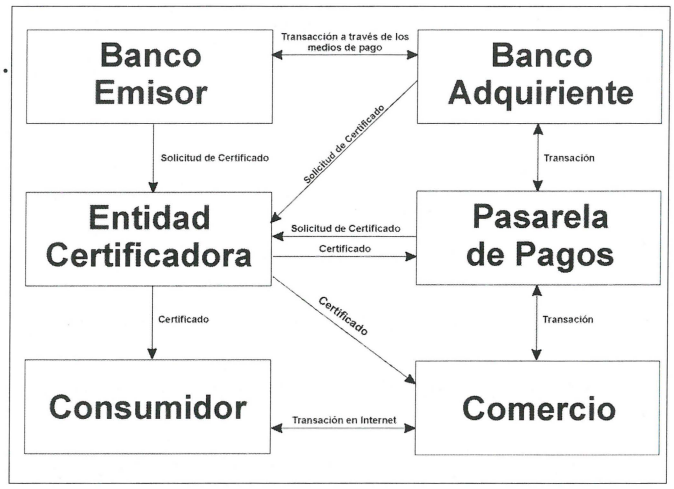

Fig. 8. Funcionamiento SET

confianza, evita que el comprador tenga que introducir su numero de tarjeta, basta con teclear una clave que, una vez validada por el banco o entidad del certificado activara la orden de pago. Esto nos lo va a proporcionar el Secure Electronic Transaction (SET), de Visa y Mastercard, junto con IBM, Microsoft, etc., ver figura 8.2. Vemos que SET define certificados a los tres intervinientes en las transacciones comerciales: * El comprador, * El Comerciante y * La Pasarela de pagos (Payment Gateway).

Los componentes esenciales de una PKI:

a) La Autoridad de Certificación (AC), es la entidad emisora de Certificados digitales. En España están: Agencias de Certificación Electrónica (ACE); Certificación Española (CERES) es de la administración publica; FESTE de los notarios, Camerfirma, de las Cámaras de Comercio; Eurociber de Banesto; Ipsca, Filial de Internet Publishing Services. Y Autoridad de Registros (AR) dedicada al registro de usuarios, para verificar su identidad.

b) El Directorio de contiene las claves publicas y los certificados.

c) El Magnagement del sistema.