MAESTRIA EN INFORMATICA

UNIVERSIDAD NACIONAL DE LA MATANZA

TRABAJO DE TESIS
SEGURIDAD EN E-COMMERCE

LIC.SUSANA VAQUER

svaquer@arnet.com.ar
2001

INDICE

PROLOGO

Internet permite el acceso a grandes volúmenes de información, pero también representa un peligro para los datos y archivos de una empresa, lo que obliga a disponer de un sistema de seguridad que proteja el sistema informático de distintos tipos de ataques. Su influencia alcanza tanto a las empresas, que se benefician de una presencia global y un acceso a nuevos mercados y clientes, como a la sociedad en su conjunto, que se beneficia de un acceso mayor y más rápido a todo tipo de información y productos.

El aumento de la oferta de productos y servicios financieros a través de Internet ha cambiado la forma de relacionarse entre las entidades financieras y sus clientes. Además, ha convertido a la Red en un canal alternativo para las compañías tradicionales, pero lo que de verdad ha propiciado el despegue de este tipo de transacciones ha sido, sin duda, el acceso a Internet del público en general, algo que está revolucionando el ámbito del comercio global y la economía.

Todo parece indicar que el comercio electrónico será uno de los mercados primordiales en el mediano plazo y uno de los aspectos que más preocupa en el desarrollo del mismo es la seguridad que las transacciones electrónicas ofrecen de cara al usuario y la empresa. Los temibles hackers, los robos de datos o la manera de configurar un servidor seguro no están claros para prácticamente nadie. Los usuarios siguen sumidos en el desconocimiento y esto hace descender la proyección de negocio de cualquier empresa.

En la actualidad, la forma de pago más frecuente entre los compradores virtuales es la tarjeta de crédito, que se utiliza en un 46% de los casos, seguida del contra reembolso en un 35%, y tan sólo en un 13% la transferencia bancaria. La plena implantación de los medios de pago cuenta con varios frenos, entre los que destaca la seguridad en este tipo de transacciones, un problema que preocupa tanto a las entidades financieras, por el alto porcentaje de denegación de pago que reciben, como a los consumidores, que temen comunicar sus datos bancarios por Internet. Por ello, los expertos en materia de seguridad establecen cuatro

requisitos fundamentales para conseguir que una transacción comercial por Internet pueda considerarse segura: identificar al comprador y al vendedor, asegurar la integridad de la información que se intercambia; asegurar su confidencialidad y garantizar el no rechazo.

Hoy en día el comercio electrónico está más allá de la etapa inicial pero aún no está establecido ampliamente como una parte de la tendencia de los procesos de las empresas. Faltan regulaciones y protecciones legales en muchas áreas, especialmente en las transacciones de los consumidores sobre Internet. Existe limitada experiencia de cómo definir contratos en el entorno electrónico; las empresas no saben que políticas implementar y hay una carencia de historia a largo plazo sobre las relaciones y contactos que no son frente a frente. No es exagerado decir que la confiabilidad más que la tecnología, dirige el crecimiento del comercio electrónico en todas sus formas.

Los negocios en la Red están creciendo de manera espectacular y todos quieren estar ahí, pero antes de dar ese paso, es necesario comprender cuales son las tecnologías, estándares y las regulaciones con las que se manejan hoy en día los negocios en línea para brindar la seguridad necesaria a todos los involucrados.

Esta investigación tiene como finalidad mostrar las tendencias, tecnologías y debilidades de los principales elementos implicados en los intercambios seguros de información en Internet, y más concretamente en los escenarios propios de lo que se ha dado a conocer como Comercio Electrónico. El objetivo concreto de la misma es dar a conocer de forma amplia los distintos componentes tecnológicos relacionados con la seguridad informática, tanto desde el aspecto de protección de entornos como de protección de información, así como las últimas tendencias y propuestas en el ámbito del comercio electrónico.

CAPITULO 1

LOS RIESGOS DEL E-COMMERCE

1. INTRODUCCION

Los servicios basados en las telecomunicaciones son de por sí arriesgados por la simple razón que, debajo de cada aspecto de su uso como parte del comercio, hay un conflicto entre acceso y control: cuanto más se favorece el acceso se debe proporcionar mayor control; el comercio significa acceso y por definición, administrar el riesgo significa control. El comercio electrónico ha podido asegurar, en general, grados razonables de control por medio de la utilización de redes cerradas, como por ejemplo las redes de valor agregado (*VANs*) que manejan pagos en bancos, seguros y otras actividades.

La WWW, que se ha convertido en la base de cada vez mayor cantidad de comercio electrónico, es lo más nuevo que se utiliza como acceso; cualquiera en cualquier parte no sólo puede accederlo, sino que puede preparar una presencia en él, como comerciante, recurso de información, de forma individual y por supuesto como comercial incompetente. Las *VANs* protegen contra el riesgo limitando quien puede ser parte de las actividades de la Web y pueden imponer procedimientos y cierres herméticos contra fuentes conocidas de riesgo. Las redes bancarias, por ejemplo, no sólo proporcionan mecanismos especializados de seguridad en todos los puntos de entrada a la red, en los enlaces de transmisión y sistemas de procesamiento sino también establecen acuerdos de cómo exactamente se reglamentan las transacciones electrónicas entre las partes. Esto es mucho más difícil que se logre en la Web, donde nadie tiene por completo el control de preservar el acceso total.

Internet es la red distribuida más grande; estas redes han hecho que el medio se utilizara para transmitir información no relevante. El enlace de transmisión puede ser cables de fibra óptica, un radio enlace inalámbrico, un enlace de TV por cable ó a través de vía satelital. Cualquier cosa que pueda codificarse digitalmente, es decir, información personal, comercial, financiera, video, fotografía, llamadas telefónicas, programas de radio, etc., es decir cualquier producto de información, puede transmitirse lejos más fácil y rápido que antes. En el ámbito de las redes distribuidas aparecen agentes de todo tipo que intentan una explotación negativa de Internet; el enlace a una red puede fácilmente retransmitirse a cualquier número de destinos, puede ser infiltrado y también usarse para crear software sofisticado que daña ó puede producir robos de otras computadoras.

El alcance de automatización del proceso comercial ha evolucionado desde las funciones básicas en una computadora al modelo complejo de procesamiento distribuido, como por ejemplo, fondos transferidos de un banco a otro, el enlace mundial de todos ellos, más enlaces de muchas redes entre sí vía Internet. Las redes distribuidas han permitido, a un proceso comercial, medir múltiples sistemas independientes, en ciudades ó países separados que contribuyen a un objetivo común; sin embargo, a pesar de todas sus virtudes, tienen su porción de riesgos. Como otros sistemas de información, los riesgos están relacionados con la privacidad de la información, la integridad y la disponibilidad, sólo que aquí los riesgos relacionados se multiplican dado que es el grado de distribución que crea el mayor riesgo.

2. ADMINISTRACIÓN TRADICIONAL DE LOS RIESGOS

En las redes distribuidas, el manejo de las amenazas y riesgos se trata con una reducción de las amenazas de riesgos y el establecimiento de protecciones de defensa; esto se logra a través de programas de seguridad y control rígidamente estructurados. Estas técnicas, en los sistemas distribuidos, tienen sus ventajas y desventajas. Dentro de las ventajas se incluyen:

- Que están constituidas por requerimientos bien establecidos, comprendidos y no ambiguos.
- Tienen requerimientos estándares que son fácilmente monitoreados y auditados.
- Se hacen análisis y evaluaciones de ambientes únicos para determinar cuales son las medidas y necesidades no necesarias.

Dentro de las desventajas se incluyen:

- Todos los sistemas se tratan de igual forma, con todas las medidas de control, sean ó no éstas requeridas.
- La línea de negocio no tiene control para determinar cual es el riesgo razonablemente aceptable.

- El sistema implementado no responde a cambios rápidos de tecnología y evolución.

La limitación de un tratamiento de la administración tradicional de los riesgos es que asume que todas las posibles amenazas asociadas a una aplicación, están contenidas en la misma aplicación y son contrarrestadas con el conjunto de medidas conocidas. Dada la proporción y la complejidad del cambio de la tecnología, ésta es una visión muy escasa, puede funcionar bien para sistemas herméticamente cerrados, siguiendo políticas estrictas y limitadas, pero no es lo que sucede. La gran tasa de cambio tecnológico y de técnicas para proporcionar soluciones son condiciones inapropiadas para estos métodos tradicionales.

El comercio electrónico proporciona a los sistemas distribuidos la posibilidad de realizar las transacciones que involucran el intercambio de bienes y servicios entre dos ó más partes; se está extendiendo y contribuye sustancialmente a la economía global. Considérese por ejemplo, el intercambio diario de billones de dólares en la bolsa de comercio y el mercado de valores de USA; mercados de dinero que existen sólo como bits y bytes almacenados en sistemas bancarios y que circulan alrededor del mundo a la velocidad de la luz sobre redes de fibra óptica; cajeros automáticos que están siempre en línea; redes de tarjetas de crédito que validan miles de compras por segundo.

2.1 Administración de la relación

El comercio electrónico ha extendido el modelo tradicional de los sistemas distribuidos a un espacio social sin precedentes; estas redes forman relaciones que están por todas ó en ninguna parte, infinitamente flexibles y escalables en un rango de pocas a miles y en esto descansa la diferencia entre el intercambio tradicional de información sobre redes distribuidas y las relaciones del comercio electrónico. Aquellas estaban garantizadas firmemente y éstas son muy abiertas. Para que el comercio electrónico alcance su punto de equilibrio entre la expansión de las relaciones con el manejo de problemas enlazados con la confianza, se necesitan resolver múltiples problemas complejos. Uno que es clave, incluye encontrar métodos aceptables para la autenticación y protección de la información (privacidad e integridad), acomodando necesidades para mejorar la performance y fiabilidad de las transacciones y creando los medios necesarios para resolver problemas.

Aunque se han producidos grandes adelantos en el uso del comercio electrónico, estas iniciativas, hoy en día, están limitadas principalmente a definiciones exactas de las relaciones entre las partes. Para que el comercio electrónico pueda extenderse fuera de estos límites, los sistemas y políticas de las empresas deben permitir la creación de relaciones confiables, dinámicas y efímeras. Esencialmente el comercio electrónico es el establecimiento de relaciones dinámicas, a través de la inclusión de interacciones de las partes por medio de tecnologías, políticas y metodologías. Los partes incluyen clientes, proveedores, socios e intermediarios. El desafío del comercio electrónico es la formación y dirección apropiada de estas relaciones; la administración de estas relaciones comienza con la definición del flujo de información entre distintas partes; los flujos de información están compuestos de funciones

de negocios discretas que, cuando se combinan, establecen transacciones comerciales. En el caso de las operaciones ***SET*** (Secure Electronic Transaction), operaciones electrónicas seguras, una tecnología y herramienta estándar para asegurar las operaciones seguras en Internet, las funciones de flujo / negocios de información para una demanda de compra entre un poseedor de tarjeta y un comerciante, incluyen demanda, respuesta, requerimiento de compra y respuesta de la compra.

3. EXPECTATIVAS DEL COMERCIO ELECTRÓNICO

El comercio electrónico constituye una mejora importante sobre el comercio tradicional basado en papel en términos de velocidad, costo, exactitud y simplicidad. La automatización de procesos de negocios colaborativos sobre redes ha proporcionado a los clientes mejores opciones, disminuyendo el costo de la operación comercial, extendiendo los mercados, facilitando la producción y el pago en tiempo. A pesar que el comercio electrónico puede brindar muchos beneficios no llega sin un desafío siendo el manejo de las expectativas entre las partes el más grande de ellos. La siguiente lista incluye elementos que contribuyen típicamente a deficiencias en las expectativas si éstas no son bien manejadas:

- La definición de mensajes estructurados (formato ***EDI***, formas electrónicas, contactos y reglas de contacto, especificaciones de diseño, etc.).
- Contabilidad, base de datos contables y reglas de contabilidad.
- Definiciones de operaciones y funciones.
- Intermediarios (filtros de información, traductores, terceras partes confiables).
- Soporte de modelos de decisión.

En algunos casos, estas deficiencias se administran por medio de estándares de comercio electrónico entendibles, tales como aquellos para manejar mensajes estructurados, estándares tales como ***EDIFACT***, ***ANSI x.12*** y ***CSIO***, entre otros. Con el tiempo, cada uno de estos elementos serán más universales y aparecerán estándares industriales para terminar con estas deficiencias y disminuir el riesgo de confianza, perdida en las relaciones del comercio electrónico. Hoy el grado que ha alcanzado el comercio electrónico, necesita de estándares que contribuirán a estrechar las deficiencias de las expectativas.

4. CONFIANZA EN EL COMERCIO ELECTRÓNICO

Al comercio electrónico le falta el aspecto formal necesario y la estructura legal para proteger sus operaciones que pueden llevar a una relación de negocios más predecible. Las relaciones del comercio electrónico no pueden simplemente darse por sentadas; por ejemplo,

si una información confidencial cae en manos inapropiadas, ¿ a quién se culpa? ; se rompió el sistema y ¿dónde se rompió el mismo?; ¿ cuáles fueron las consecuencias del robo de documentación u otros valiosos datos, de la destrucción, corrupción de datos, destrucción de la integridad de la red, rechazo de servicios y/o disminución de la reputación?; ¿podría ser vendida la información por una de las partes que intervinieron en el comercio electrónico?; ¿ de ser así, se permite eso?

Debido a que las soluciones del comercio electrónico están formadas por el conjunto de muchos socios, se forma una relación tenue entre cada socio que crea un tejido de confianza. Dado que estas operaciones de negocios conectan a múltiples socios, romper una sola relación confiable puede transmitirse en cascada a los otros socios y puede comprometer a todo el tejido. Las repercusiones de este tipo de incidente pueden ocasionar riesgos financieros y, lo que es más importante, riesgos en la reputación. El desafío consiste en como se puede crear y mantener una solución de comercio electrónico confiable; el objetivo es reforzar las relaciones confiables de forma tal que puedan soportar la agresión de intrusos, el mal funcionamiento tecnológico y la ignorancia.

Para lograr esto, las empresas deben establecer procesos de seguridad, políticas y prácticas seguras. La seguridad se traduce en reputación; los errores de seguridad se producen al no encontrar el compromiso implícito y explícito, en la relación. Los procesos descritos previamente, se deben implementar para eliminar la desconfianza entre los participantes de las soluciones de comercio electrónico. Las políticas y prácticas normalmente establecen reglas entendidas y aceptadas, que definen responsabilidades y conductas para cada parte involucrada en una operación de comercio electrónico. Dependiendo de los riesgos, estas políticas y prácticas pueden entenderse de manera general ó de forma legalmente enlazadas. Se necesitan dirigir los siguientes temas comunes:

- Comunidad y aplicabilidad
- Registración
- Seguridad local, técnica, operacional y políticas legales

Ellos deben verse como ejercicios para reducir los riesgos, en lugar de ejercicios de defensa.

5. POLÍTICAS DE COMUNIDAD Y APLICABILIDAD

Definen quienes son las distintas partes y cuales son sus roles en la solución de comercio electrónico. Se establece un conocimiento común de qué papel juega cada parte en el cumplimiento de las operaciones comerciales; se pueden establecer entonces, responsabilidades para cada uno, con pautas para prácticas aceptadas que se ratifican entre todos los participantes.

El registro de políticas define como los nuevos socios pueden participar en una solución de comercio electrónico; la verdadera naturaleza del mismo, es una base continua de expansión de las relaciones. Cada una de estas relaciones contribuye a la confianza global de la solución de comercio electrónico. Como tal deben definirse y rectificarse reglas para el registro, expiración y nueva registración para alejar el riesgo de arruinar relaciones.

6. POLÍTICAS DE SEGURIDAD LOCAL

Son políticas de seguridad no técnicas para administrar controles físicos, de procedimientos y personales. La comunidad del comercio electrónico estará formada de participantes, cada uno con distintas políticas de seguridad local, lo cual introduce problemas de subjetividad e insensibilidad y una falta global de confianza en el sistema por lo que deben definirse conjuntos de principios aceptados e implementados por los distintos participantes. Estas prácticas se definirán según las distintas comunidades.

7. POLÍTICAS TÉCNICAS DE SEGURIDAD

Estas políticas están focalizadas directamente en las mismas tecnologías de la información. La seguridad técnica controla que se defina, para un equipo de computación, la seguridad de la red, la encriptación, etc. El grado con que se definen e implementan estos controles está relacionado directamente con los riesgos potenciales. Nuevamente, estos controles se definirán según las distintas comunidades.

7.1 Políticas de funcionamiento

Se relacionan específicamente con las distintas responsabilidades de los participantes involucrados en cada operación comercial. Debido a que la entidad operativa de cualquier solución de comercio electrónico se compone de distintos participantes, se debe definir, llevar a cabo y supervisarse una política de operación común tal como en una simple empresa.

7.2 Políticas legales

Simplemente ayudan a relacionar a los distintos participantes con las condiciones de las políticas. Dado que el lenguaje en sí mismo es ambiguo en aquellas circunstancias donde el riesgo es alto, constituye una buena práctica involucrar a la comunidad legal puesto que las obligaciones son entonces claramente articuladas y asignadas entre los distintos participantes, así como en la propia solución de comercio electrónico. Para los clientes, todos los

intermediarios y terceras partes son transparentes, ellos no saben cual es la parte que falla y en esas circunstancias considerarán que la empresa falló. El riesgo de perder clientes no reside en el entorno que se controla sino en aquellos entornos extendidos donde no se tiene el control directo.

Estas pautas pueden utilizarse no sólo para crear una solución de comercio electrónico sino también para evaluar cual de todas las soluciones posibles deben considerarse con relación a los riesgos que quiera afrontar la empresa.

CAPITULO 2

TIPOS DE RIESGOS

1. RIESGOS TECNOLÓGICOS INDUCIDOS

La informática barata, fiable y la tecnología de redes representan un doble peligro para los beneficiarios del comercio electrónico; por un lado están las virtudes de dirigir, conveniente y rápidamente, operaciones comerciales sobre una infraestructura completamente electrónica habilitada por la adopción extendida de tecnología; por otro lado esta tecnología introduce nuevos riesgos que simplemente no son aplicables a las operaciones que se hacen en una estructura completamente física. Cuando se reemplazan personas humanas con electrónica, la posibilidad de ataques electrónicos, errores complejos ó intrusiones de corta vida, pero costosas, aumenta dramáticamente.

2. RIESGOS TÉCNICOS ORIENTADOS A PROCESOS

Los nuevos riesgos tecnológicos inducidos, presentes en el mundo del comercio electrónico caen en cuatro categorías:

1) ***Problemas relacionados a transacciones automatizadas y manejos de mensajes***: surge un nuevo riesgo de aquellos que usan computadoras y listas de correo para llevar a cabo atentados masivos, negar servicios y enviar muchos pe-

didos paralelos que traen como consecuencia un robo electrónico de bienes y servicios.

2) ***Redes intermediarias, múltiples y desconocidas***: sin el control punto a punto de una *VAN*, común en el mundo ***EDI***, las operaciones de comercio electrónico sobre la Web, pasan a través de cualquier número de sitios intermedios no controlados. Además de los problemas de integridad inherentes, las redes pueden agregar el problema de la latencia (un retraso creado por un mensaje que procesa sobrecarga) ó perder datos contribuyendo a una pobre calidad de servicio ó a la percepción de una falla del sistema remoto.

3) ***El misterio de los componentes de software de caja negra***: que están integrados en los puntos finales del sistema. Las interacciones entre los componentes pueden que no se conozcan ó comprenderse totalmente. Condiciones tales como capacidad ó limitaciones de interfase en componentes individuales, pueden provocar errores de forma desconocida. Estos errores se duplican fácilmente a través de las distintas capas de aplicación hasta que aparecen en un sistema que se audita regularmente.

4) ***Procesos para manejar problemas de naturaleza electrónica mal entendidos***: los riesgos del comercio electrónico no están sólo limitados a robo potencial ó casos de fraude. Cuando un negocio se hace más dependiente de procesos electrónicos, el procedimiento fiable de esos elementos es un requisito previo para las funciones diarias. Los delitos electrónicos pueden cometerse repetida y rápidamente e involucran grandes sumas de dinero; los riesgos del comercio electrónico no están limitados sólo al robo potencial ó fraude, un fracaso operacional causado por una caída no reparada del sistema, una demora prolongada por un ataque al servicio ó una combinación de problemas que llevan a una caída efectiva de los datos de la red, pueden ser sumamente dañinos.

3. RIESGOS DE LAS COMUNICACIONES PÚBLICAS

A primera vista, la raíz de la mayoría de las preocupaciones de seguridad en el comercio electrónico parece ser el uso de redes públicas; si se limita la exposición de los datos en canales inseguros ó desconocidos, los riesgos estarán limitados. Sólo la mejora de un camino de comunicaciones público permite que el proceso electrónico sea tan fiable como una comunicación telefónica ó un sistema basado en fax. Además los procesos de comercio electrónico pueden sufrir debido a los retrasos excesivos de la red, por pérdidas en el tráfico de la misma y por rechazos de ataques al servicio.

3.1 Evaluación de los riesgos de las redes

Las infraestructuras comerciales electrónicas, como aquellas basadas en el estándar Ethernet sobre redes distribuidas, aparecen siempre igual, con la misma disponibilidad de los datos y ancho de banda desde cualquier punto de la red. Esta flexibilidad es el núcleo del riesgo interno en redes corporativas y el riesgo más grande en redes públicas: una red puede violarse ó supervisarse desde cualquier punto de acceso, con un equipo tan simple como una PC.

Utilizando un software específico, disponible libremente, que permite mirar y copiar datos de una tarjeta adaptadora de interfase de red, usuarios comunes pueden examinar el tráfico que cruza la ruta de información local. Cualquier intruso con habilidades básicas de instalaciones eléctricas, puede armar una extensión de la línea digital a un dispositivo colector. Sin embargo, todas estas amenazas pueden manejarse y controlarse usando encriptación con lo cual se logra que cualquier dato recuperado ó extraído de la red sea inútil excepto para el destinatario real.

Un intruso, personificando a otro usuario ó host de la red, ("haciéndose pasar por"), emula la facilidad de los datos de la red, lo cual constituye una preocupación importante para la seguridad. Un usuario remoto puede robar ó pedir prestada la identificación y contraseña de un usuario válido; un host remoto puede hacer lo mismo con la dirección de IP de un servidor conocido e interceptar el tráfico destinado a la máquina real. El engaño puede producir accesos no autorizados a los sistemas designados lo cual constituye un problema de autenticación.

El rechazo del servicio cubre: desmantelamiento físico del equipo ó saturación de las redes de comunicaciones por olas de tráfico de mensajes. Sistemáticamente se atacan servicios ó recursos necesarios para hacerlos inútiles. El rechazo del servicio puede lograrse a través de aplicaciones maliciosas (virus y gusanos) ó mediante el uso de aplicaciones de servicios que directamente afectan los componentes del entorno operativo.

Violaciones de las comunicaciones y de la seguridad de los datos son ataques, sobre los datos y el software que maneja dichos datos de los usuarios finales; permiten accesos no autorizados (copiado, daño, etc.) a datos confidenciales, mientras que las violaciones al software hacen uso, en los programas, de las llamadas "puertas trampas". Un ejemplo de esto lo constituyen los programas conocidos como troyanos. Para defenderse de este tipo de ataque es necesario contar con una encriptación y barreras (firewalls) adecuadas.

3.2 El rendimiento como un riesgo

La comunicación se puede definir como el movimiento de información entre un origen y un destino; todas las aplicaciones de comercio electrónico incorporan un elemento de comunicación y necesitan del uso de redes públicas ó descentralizadas las cuales no son controladas por un solo grupo lo que hace necesario que los proveedores de servicio extremen sus

habilidades en el control de las demandas solicitadas. Los riesgos de proporcionar servicios de comunicaciones pueden dificultar la provisión de soluciones para el comercio electrónico. Dentro de los factores que atentan contra ellas podemos mencionar: la imposibilidad de proporcionar un ancho de banda apropiado que sea económico y soporte el flujo de información en tiempo real. Mantener el ancho de banda apropiado es la tasa que determina cual será el promedio de intercambio de información desde el origen al destino, en un determinado período de tiempo. La única forma que se pueda garantizar el ancho de banda y los niveles deseados de servicios sería controlando cada uno y todos los enlaces dentro del servicio deseado. Esto es costoso y altamente imposible que se dé satisfactoriamente, ya que los servicios de comercio electrónico se hacen para servir a un gran número de usuarios finales.

Esta dificultad se intenta resolver creando estándares que deben respetar los proveedores de servicio, para asegurar un nivel de calidad en las telecomunicaciones. El flujo de información en tiempo real se refiere a operaciones de usuario final a usuario final enviadas en tiempo real y con ciertas propiedades que son de particular interés debido al precedente que sentaron en las operaciones sin fallas con sistemas tales como los cajeros automáticos. Una solución posible es crear una red cerrada donde todas las técnicas y comunicaciones desconocidas puedan controlarse con eficacia; sin embargo esto limita la flexibilidad y no puede responder satisfactoriamente a las demandas del mercado.

En el futuro, los transportadores (transportadores de intercambio local, operadores de cable, satélites, etc.), fabricantes (módems, tecnología de redes, switches, servidores de información, desarrolladores de software, etc.) y los proveedores de servicios (Internet y en línea), deberán colaborar para encontrar un servicio de comunicaciones de alto nivel, manteniendo un ancho de banda apropiado y capacidades de tiempo real lo cual llevará un cierto tiempo dados los costos, la calidad de la infraestructura existente y la competencia entre las tarifas de los proveedores existentes.

3.3 Robo de bienes y servicios

La automatización introduce la posibilidad de ataques automáticos en las soluciones de comercio electrónico siendo uno de los mayores la posibilidad de automatizar el robo de bienes y servicios. Estos tipos de ataques se pueden traducir en intrusiones disimuladas que se llevan a cabo durante procesos tales como accesos (login deficiente, imitación); consentimiento (préstamos, tarjetas de crédito, etc.) y compras (fraudes con tarjetas de crédito). Existen dos métodos conocidos para ejecutar este tipo de robos: ***repetición*** y ***paralelo***.

Repetición: estos ataques constan de dos pasos, recordar la información y repetirla. El objetivo del ataque es examinar procesos existentes, básicamente procesos de acceso, y recordar tanto la información como la secuencia de entrada. Esto proporciona al intruso no sólo información crítica sino también un enlace con procesos de negocios que proporcionan una visión agregada dentro de la propia área de trabajo de la aplicación. Algunos días más tarde, el intruso puede repetir la información y obtener acceso al sistema. Este tipo de ataque se puede abortar usando la terminología de encriptación y mediante una mejor autenticación. Sin em-

bargo esto no evita los ataques llevados a cabo por usuarios legítimos del sistema que tratan de acceder a partir de los servicios a los que no están autorizados.

Paralelo: estos ataques manejan intrusiones sincronizadas sobre un perfil determinado. Junto con los ataques de ***repetición***, los intrusos varían la información relacionada con el comercio electrónico con el objeto de obtener el resultado deseado.

4. MEDIDAS A CONSIDERAR PARA REDUCIR EL RIESGO

Las siguientes son medidas que deberían tomar los líderes en comercio electrónico para reducir riesgos:

- *Autenticación segura*: instalar los métodos más sofisticados de autenticación, utilizando métodos de encriptación para los distintos tipos de negocios, su naturaleza y partes involucradas.

- *Tolerancia y punto inicial*: incluyen, dentro de sus aplicaciones, "triggers"(disparadores de acciones) que esperan potenciales actividades maliciosas para activarse. Estos disparadores están relacionados a las operaciones comerciales y se manejan por medio de parámetros lo que permite cambios, si se detectan nuevos problemas.

- *Sistemas actuales de detección de fraudes*: aseguran que los sistemas de detección de fraudes existentes (árboles de decisión, ingeniería de inferencia, etc.) no sean engañados. Aunque estos sistemas pueden no detectar todos los posibles problemas, ponen límites a los métodos de fraude existentes y aún a los nuevos.

- *Detección de fraude oculto*: estos sistemas se utilizan para aquellos sistemas calificados como de alto riesgo, desarrollándose un sistema de decisión básico y redes neuronales que se ajusten a los propósitos de los perfiles y modelos de detección. Con el correr del tiempo, estos sistemas, pueden evolucionar de acuerdo con las nuevas funcionalidades de los negocios.

- *Registros de auditoria*: se mantienen registros de este tipo, tanto a bajo nivel de detalle, como de las operaciones comerciales individuales. Esto proporciona una información excelente para los objetivos planeados de análisis de datos para detección de fraude.

- *Dinámica*: cualquier aplicación pública (Web ó cualquier otra) es susceptible de ataques automáticos, que son un método efectivo para sistemas comprome-

tidos. Basta con agregar una interfase fiable y estándar lo que puede crear un servicio para facilitar el fraude.

- *Ocultar las reglas del negocio*: Permite la posibilidad de automatización. A menudo, la encriptación sólo se considera durante de la transmisión de información clasificada. Las técnicas de desarrollo de encriptación basadas en la Web, tales como HTLM y Javascripts, no se diseñaron para ocultar el contenido de la lógica del negocio. Todos las medidas de conveniencia y decisión acerca del proceso, dependiendo de la sofisticación de la aplicación, son conocidas por el público en general. Tal metodología puede representar un riesgo significativo para una empresa por lo cual es necesario tener en cuenta la posibilidad de ocultar pautas adicionales del proceso de negocio.

4.1 Ningún sistema de encriptación es infalible

Procesamiento cooperativo, es la coordinación programada de computadoras interconectadas que trabajan en una tarea común y constituye la esencia de Internet y del comercio electrónico a gran escala siendo también de interés para los estafadores.

La clave asimétrica facilita la distribución de claves simétricas; las claves simétricas se usan entre un remitente y un destino con el objeto de encriptar la información que se va a intercambiar. Para reducir las posibilidades de comprometer las claves, las soluciones de comercio electrónico deben limitar el uso de una clave simétrica particular, a una sesión de operación comercial; esto requiere que se genere e intercambie una nueva clave simétrica, por cada sesión que, aunque parezca excesivo, limita el riesgo a un nivel aceptable. Existen algoritmos fiables y seguros disponibles, pero el manejo de claves constituye aún un problema. Desde hace tiempo se manejan las claves a través del protocolo X.509, cuya parte más importante es su estructura para certificados asimétricos (conocidos también como clave pública).

4.2 Aspectos legales

En el comercio electrónico, las sociedades manejadas por el progreso tecnológico se entrelazan con las leyes comerciales tradicionales; las leyes aplicables al comercio tradicional ya no se aplican al comercio electrónico. Las leyes, en un contexto social, construyen relaciones entre personas y acciones, el comercio convencional define el contexto para estas regulaciones en términos de entorno físico, conexiones, relaciones, etc. La sociedad digital del comercio electrónico crea propiedades nuevas muy distintas; los administradores de comercio electrónico deberían considerar las complicaciones legales que pudieran presentarse en los siguientes contextos legales:

- ***Marketing y comunicaciones*** es la distribución de cierta información a través de las páginas Web, de los servicios alternativos de mensajería (por ej. e-mail) o enlaces de hipertexto. En esta implementación, es importante, tener en cuen-

ta las falsedades de ideas ó conceptos que puedan llevar a litigio ó a dañar reputaciones.

- ***Asesores***: estos servicios involucran el uso de fuentes de información de terceras partes con el propósito de realizar descubrimientos, análisis, avisos, etc. y pueden llevar a problemas legales.
- ***Servicios de transacciones***: son aquellos que tienen en cuenta todo el conjunto de bienes y/o servicios, incorporando ambos ó no, operaciones financieras. La importancia de la auditoria y consejo legal crece a medida que las soluciones de comercio electrónico se mueven del marketing al asesoramiento y luego a niveles de operaciones de interacciones entre empresas comerciales.
  Muchos de los problemas alrededor del comercio electrónico se focalizan en el anonimato de las personas en el ámbito digital. Los certificados ó firmas digitales ayudan a resolver estos conflictos, pero falta mucho todavía por hacer para establecer la estructura legal apropiada que lleve adelante esta tecnología.

  La ***UNCITRAL*** (United Nations Commision on International Trade Law), adoptó en junio de 1996 una ***ley modelo*** para el comercio electrónico, intentando darle una estructura legislativa para desechar las barreras legales que pudieran hallarse en el comercio electrónico. La ***ley modelo*** hace hincapié en aquellos casos donde la normativa requiere una firma que autentique lo actuado; estos requisitos podrían encontrarse electrónicamente, si la firma electrónica proporciona un enlace tanto entre el firmante y los datos como evidencia del intento de ser asociada con el registro.

  La realidad es que, el avance, aceptación y utilización de la tecnología, hace necesario un marco legal; existe un período donde los primeros que adoptan las nuevas tecnologías, están sujetos a riesgos no conocidos en su verdadera magnitud al no haber un marco legal efectivo, pero el administrador de comercio electrónico debería conocer lo que es posible hacer para minimizar los riesgos para todos los involucrados.

4.3 Profesionales de control y auditores

Una auditoria de un proceso de comercio electrónico, de una aplicación, de una interfase ó de un módulo, siempre implica manejar un riesgo: cuanto mayor es el riesgo mayor es la estafa. Valorar un riesgo de gran amplitud, determina la naturaleza, el alcance y la extensión de la auditoria. Entender los riesgos comerciales del comercio electrónico, es un prerrequisito para llevar a cabo un trabajo de auditoria. Cuando un auditor controla un aspecto técnico de algo, por ejemplo del sistema operativo **UNIX** ó ***MVS***, debido a que el tema es autónomo, la valoración del riesgo se centrará alrededor de las debilidades conocidas de seguridad, rendimiento, soporte, cambio en la administración, copias de seguridad, recuperación y utilidades asociadas con el producto. Este enfoque es puntual y específico. Pero este mismo tipo de estudio, no parece efectivo cuando se audita el comercio electrónico; por ejemplo

auditar el protocolo ***SET*** (Secure Electronic Transaction), no es lo mismo que auditar ***UNIX*** ó ***MVS***; aunque hay áreas técnicas de infraestructura de clave pública (***PKI***), que se deben revisar, enfocándose en la robustez técnica de ***SET***, el riesgo que rodea a este producto no será evidente. Las fallas del protocolo ***SET*** para autenticar es sólo uno de los riesgos claves. La gran meta de las empresas de tarjetas de crédito para poner un estándard, como forma de pago sobre Internet, lleva una serie de riesgos, teniendo una sola norma. Si hay un "bug" ó un error cuando se implementa ***SET***, todos los pagos de tarjetas de crédito que usan el protocolo, se verán afectados sin ninguna excepción. Por lo tanto, lo primero que hay que hacer son las preguntas fundamentales que están asociadas con los riesgos de una norma simple y ver cuales son los problemas que deben tenerse en cuenta para cubrir los peores escenarios.

Cualquier riesgo identificado para el comercio electrónico como competitividad, tecnología, reputación ó regulación no tienen sentido si no se los coloca en el contexto comercial correcto, por lo cual no se pueden comenzar a evaluar los mismos, en una aplicación de comercio electrónico particular, sin un amplio conocimiento de las relaciones e interacciones entre los riesgos locales de un producto ó servicio de comercio electrónico con el comercio electrónico mundial.

4.4 Tercerizar los riesgos

Existe una gran confianza en casi todos los productos ó servicios de comercio electrónico que son tercerizados para proporcionar parte de la solución total. De esta forma los riesgos relacionados se extienden y debe incluirse como tal la inhabilidad de los vendedores tercerizados para cumplir con las políticas de seguridad de la información de la empresa y la dependencia del vendedor para procesar ó administrar algo importante del negocio.

Para la búsqueda de riesgos, ayuda responder las siguientes preguntas:

- ¿ Cuántos componentes del comercio electrónico son tercerizados?
- ¿ De los componentes tercerizados, cuántos son críticos?
- ¿ Cuál es la capacidad / experiencia de los vendedores tercerizados?
- ¿ Están estos vendedores registrados, desregulados o cumplen con las normas ***ISO***?
- ¿ Están controlados, por administradores competentes, en las funciones críticas?
- ¿ Hay un grupo especializado y con la dirección adecuada dedicado a trabajar en un plan contingente en caso de falla de un vendedor?
- ¿ Hay tareas de revisión adecuadas sobre los que hace la tercerización?
- ¿ Cuáles son los términos del contrato, especialmente con un agente que se encuentra fuera del país de residencia?

4.5 Separación de tareas

La parte más importante del control es la separación de tareas: los cheques son consignados, las claves están bajo debida custodia, los pagos se ingresan y verifican por distintos individuos. Estos controles clásicos pueden verse comprometidos por interferencias entre las personas que recién se inician.

Las formas tradicionales de división no funcionan en el mundo del comercio electrónico; los cheques son reemplazados por débitos electrónicos; las claves por firmas digitales y las transferencias de fondos incluyen la opción de "hágalo Ud. mismo". ¿Qué pasa sí una operación falla por una mala autenticación?, ¿cuáles son las consecuencias de un error en la implementación de una nueva versión de un software estándar de encriptación?. Las consecuencias son, por supuesto, más serias dado que se pierde la intervención humana y manual, por lo tanto hay que evaluar las formas electrónicas de separación como por ejemplo, el rol de la Autoridad Certificante, el tratamiento electrónico de la auditoria y un entorno técnico apropiadamente controlado "in situ", con el objeto de proteger las relaciones, sistemas y aplicaciones de comercio electrónico.

CAPITULO 3

CONTROLES EN EL COMERCIO ELECTRONICO

1. INTRODUCCIÓN

Una de las barreras de las empresas que implementan programas exitosos basados en comercio electrónico, es que ellas no ven a los procesos de auditoria y el control como la parte principal del negocio sino a las relaciones del cliente y a la calidad de los productos. En muchas empresas, los administradores consideran a las funciones de auditoria y control como males necesarios, inclinándose a una disposición general negativa hacia estos procesos. Las organizaciones exitosas son capaces de reconocer que, asegurando la implementación de procesos bien administrados, controlados y auditados, generarán un valor a largo plazo de sus empresas. Los controles son simplemente los que hacen que una organización sea fiable para lograr sus objetivos y cuando se aplican inteligentemente, no son sólo un costo sino un perfeccionamiento del negocio.

2. BENEFICIOS E IMPORTANCIA DEL CONTROL

Como el comercio electrónico llega a ser una parte de todo proceso de negocio, la empresa está obligada a actualizar y rever la importancia de sus procesos usando herramientas apropiadas y procesos reconocidos. Aunque el establecimiento de la confianza es crítico en el desarrollo de las relaciones con los clientes, mantener y hacer crecer esta confianza se logra

asegurando que existe un entorno consistente y fiable que continúa garantizando esta confianza; proporcionar evidencia de un entorno bien controlado y administrado requiere una revisión constante de los procesos y hacerle ver al cliente que la empresa está atenta al mantenimiento de sus procesos de control. La confianza se basa en la creencia de la que la empresa está comprometida y es capaz de mantener la fiabilidad e integridad de su información y de la estructura tecnológica que la soporta.

Cuando se introducen procesos de comercio electrónico, ya sea para acceder a la información (como productos y servicios de la Web) ó para procesos de transacciones, tales como transferencia electrónica de fondos, no sólo se necesitan medidas adecuadas de seguridad sino que debe haber una inversión en la declaración pública de problemas y soluciones que tienen lugar. Los procesos de control son parte del marketing y el contenido de las relaciones públicas que una empresa utiliza para establecer y mantener sus marcas y la satisfacción del cliente tanto como la calidad de la relación producto / servicio ó precio.

3. OBJETIVOS DE CONTROL DE UN SISTEMA COMERCIAL

Para establecer un entorno efectivo de comercio electrónico que soporte las metas de negocios de la firma, lo primero que se necesita establecer son los objetivos para ese entorno. Algunas veces los componentes están dentro de la propia tecnología de base de la empresa y se va en esa dirección, para establecer la necesidad de niveles internos de control que aseguren la calidad y confianza. El comercio electrónico enlaza electrónicamente su firma con sus proveedores y clientes lo que significa que los clientes pueden ingresar directamente, a través de formularios de entrada ó personal interno entrenado, datos y requerimientos, dentro de sistemas que tradicionalmente estaban aislados de los accesos externos. Ya sea que se refiera a un proceso ***EDI*** ó a una compra basada en la Web, no puede asegurarse por mucho tiempo la absoluta integridad de sus datos de entrada sin manejar un control adecuado que hace necesaria una revisión de la actitud externa y un proceso interno de revisión para el comercio electrónico.

La revisión externa realiza las preguntas necesarias para saber quien puede obtener acceso al entorno, bajo que autoridad ó nivel de acceso y como se puede asegurar que estos accesos no comprometen las metas del negocios y los objetivos de control de la empresa.

Simultáneamente, el proceso de revisión interno, confía en el concepto de que la velocidad y el impacto del comercio electrónico requiere una continua verificación de que todos los sistemas están logrando sus objetivos de rendimiento y mantienen sus procesos de control activos mientras se está trabajando. Para una empresa que confía en sus sistemas y para los clientes y proveedores que confían en las relaciones del comercio electrónico, el control constituye la base para el diálogo y la prueba.

Un sistema es confiable cuando se tienen las herramientas para resolver problemas tales como: los firewalls fueron superados, los datos extraviados ó no ejecutados y las líneas de producción fueron silenciadas debido a distintas averías en las comunicaciones ó la logística.

4. CONTROLES EN EL COMERCIO ELECTRONICO

Tanto el trabajo del administrador de las tecnologías de la información como el del auditor, en toda forma de tecnologías nuevas ó emergentes, comienza con la búsqueda de las características únicas que distinguen los nuevos métodos de comercio electrónico, tales como operaciones basadas en Internet (dinero electrónico), de otros productos similares tales como: ***EDI***, ***EFT***, ***Fax***, ***E-mail*** para verificar si. los controles existentes y probados, se pueden aplicar satisfactoriamente a una nueva forma de comercio electrónico ya que constituyen los mejores controles al menor costo de desarrollo.

Los controles internos se deben implementar si son relevantes para la empresa según los objetivos de negocios de la misma. Los controles no existen aislados: la más sofisticada técnica de encriptación no tiene ningún valor si no hay ninguna demanda de ella y la demanda se crea por las necesidades de la empresa. Por consiguiente, la seguridad es responsabilidad de la empresa, no del proveedor de servicios. El control es un proceso evolutivo; la aparición de Internet ó de otro nuevo canal de entrega, no invalida ninguno de los objetivos de los negocios, de la administración ó del control que ya existan en una empresa.

5. PRIMERAS FORMAS DEL COMERCIO ELECTRONICO

Tal como el ***EFT*** y ***EDI***, el comercio electrónico basado en Internet, se caracteriza por tres factores: la desaparición de la auditoria de papeles, gran velocidad y baja intervención humana. Las nuevas formas de comercio electrónico tienen un alcance global inmediato, volumen potencial elevado y múltiples relaciones simultáneas entre clientes, comerciantes, instituciones financieras y todo aquello asociado como terceras partes vendedoras, empresas de outsourcing, transportadoras de telecomunicaciones, etc.

Los controles preventivos son más efectivos que los que pueden descubrirse; en el diseño de controles para el comercio electrónico del nuevo entorno, toda validación, certificación, autenticación ó prueba de privacidad debe llevarse a cabo en tiempo real. Los auditores deben participar desde el comienzo, en un proyecto de desarrollo de comercio electrónico; ellos gastarán una cantidad considerable de tiempo evaluando y testeando controles, antes de que estos sean implementados.

6. ENTORNO DE COMERCIO ELECTRONICO SEGURO

Antes de decidir que controles son apropiados para el comercio electrónico, se deben conocer cuales son los riesgos potenciales a los cuales se debe en enfrentar el mismo. La evaluación de riesgo comienza con la identificación de cuales son los bienes de mayor valor que deben protegerse primero. Los controles que son apropiados en un entorno pueden no serlo en otros. El descontrol puede exponer a una empresa de comercio electrónico a riesgos descontrolados pero tampoco es muy efectivo mucho control; el enfoque está en proteger aquellos componentes que son más críticos comercialmente.

Un estudio afirma que más de la mitad de los datos de una empresa típica son incompletos, se pierden o son inconsistentes. El concepto de los datos como un recurso de la empresa y por lo tanto, la responsabilidad de la misma sobre aquellos, es muy reciente. El comercio electrónico incrementa la importancia vital referida a la calidad de los datos puesto que no pueden guardarse aislados dentro de la empresa ya que se utilizan por fuera de la misma, incluyendo clientes, proveedores, distribuidores y aseguradores.

Cuando el comercio electrónico se incorpora al ámbito del administrador de *IT*, es necesario contar con buenas prácticas de control para prevenir los riesgos globales alrededor del producto o servicio.

7. ADMINISTRACIÓN DE CONTROL

Hay objetivos básicos de control que pueden aplicarse universalmente a todo tipo de operaciones electrónicas: exactitud, integridad, autenticidad, seguridad, auditoria, oportunidad y recuperabilidad. Dado que estos atributos también son perseguidos activamente por los administradores de negocios y operaciones, en el trabajo diario, se establece una ecuación entre los mismos que podría resumirse como:

Objetivos de control = objetivos empresarios = objetivos de administración

En la realidad, la vara con que se miden estos atributos de control varía de administrador a administrador, de auditores al personal de comercialización y entre los expertos en seguridad. La administración tiene la responsabilidad global de asegurar que la empresa trabaja fácilmente, tanto a corto como a largo plazo. Como la tecnología de computadoras y telecomunicaciones cada vez es más crítica para lograr estos objetivos, es importante que los administradores hagan hincapié en el desarrollo de nuevas tecnologías.

Para asegurarse que las implementaciones de comercio electrónico son manejadas adecuadamente, los administradores deben jugar un rol importante en los procesos de im-

plementación y los administradores de rango superior se deben comprometer con la tecnología.

Para lograr los beneficios del comercio electrónico los administradores necesitan evaluar que cambios específicos son necesarios hacer, tanto en los sistemas como en la administración y estructura del personal, lo que significa cuanto personal se requerirá y que nuevas o distintas habilidades necesitan tener los mismos; que personal puede reentrenarse para trabajar en otras áreas y que entrenamientos requieren. Estos problemas son críticos para asegurar que se logrará un retorno de la inversión. Sin embargo, la consideración más importante para el éxito del comercio electrónico será la magnitud de lo que la alta dirección está dispuesta a comprometer, en tiempo y recursos en el proyecto, desde su inicio hasta su finalización.

Tanto los usuarios como los desarrolladores técnicos deben trabajar juntos para asegurar que conocen las necesidades de los sistemas y que éstos operan según se diseñaron. El papel del usuario es crítico dado que la tecnología lleva a cabo la mayor parte de la decisión operativa, por lo cual debe entender como trabaja el negocio y trabajar junto al personal técnico. La mayoría de los procesos organizacionales se construyen para trabajar de manera bastante independiente unos de otros, pero, en un entorno de comercio electrónico, tienen que trabajar como un todo integrado.

8. CONTROLES SEGUN LA TECNOLOGÍA (HERRAMIENTAS)

El comercio electrónico ha impreso mayor velocidad a todos los pasos relacionados con el comercio tradicional, a punto tal, que los mismos no pueden controlarse más por métodos convencionales. Para las empresas líderes, las operaciones están en el orden de los billones de dólares y constituyen la mitad de los negocios de las firmas; una vez que la empresa alcanza el volumen crítico, los grados de crecimiento del 40% - 100% no son inusuales. Los negocios nunca encontraron tal grado volátil e impredecible de crecimiento de las operaciones.

Adicionalmente, la flexibilidad del comercio electrónico permite que las operaciones, mucho más complejas, se automaticen incorporando múltiples jugadores independientes y muchos componentes interactuando simultáneamente por lo que, las soluciones de comercio electrónico, se deben complementar constantemente con una serie de herramientas de software que ayuden en la administración de condiciones tales como controles de entorno y negocios. El control no es algo opcional sino que es un requerimiento integral de diseño de confianza.

Dado que las soluciones de comercio electrónico son arreglos complejos de relaciones entre procesos de negocios independientes, las condiciones que se originan por estas relaciones deben manejarse con medidas apropiadas.

Las herramientas no son otra cosa que controles electrónicos y los administradores de comercio electrónico, antes de considerar su uso, deben entender el contexto donde se van a aplicar. El punto de partida son los controles de responsabilidades que requieren algún nivel de esfuerzo; estos incluyen:

- Identificación del origen de la fuente y el destino
- Control de acceso
- Contabilidades precisas
- Seguimientos discretos
- Estado de la operación
- Registros de auditoria

Estos controles se pueden automatizar utilizando herramientas para incrementar el nivel de confianza en una solución de comercio electrónico. Las herramientas se pueden clasificar en las siguientes categorías:

- ***Herramientas de autenticación basadas en credenciales***: emplean la criptografía como forma de implementar credenciales seguras; se obtienen mediante la utilización de un par de claves pública y privada que identifican a una única persona.

- ***Herramientas de control de acceso basadas en políticas***: refuerzan la integración de políticas del negocio dentro de soluciones de comercio electrónico. Las políticas del negocio incluyen reglas de listas de control de acceso, pero no se limitan sólo a eso sino que incluyen también detección de virus en tiempo real, filtrado de mensajes y manejo de intromisiones.

- ***Repositorios o depósitos de auditoria robustos***: registran las señales vitales de las operaciones de los sistemas de comercio electrónico para posteriores revisiones.

CAPITULO 4
MANTENIMIENTO DE LA CONFIANZA

1. SEGURIDAD, CONFIDENCIALIDAD Y PRIVACIDAD

La seguridad en el comercio electrónico se centra en las operaciones; existe toda una disciplina tecnológica para asegurar que los datos se mantienen seguros y precisos; que se previenen los accesos no autorizados a los datos; que las operaciones se cumplimentan según se intentan; pero estas herramientas, a menudo, no tienen en cuenta las relaciones de confianza en el contexto de cual de las partes se daña por una falla.

1.1. Definiciones e implicaciones para el comercio electrónico

1.1.1.*Integridad*: es un proceso que asegura que la información entregada no ha sido manipulada, lo que significa que es la misma en la que estuvieron de acuerdo todas las partes; la integridad implica seguridad y en las soluciones de comercio electrónico asegura que la información, como por ejemplo, pagos, acuerdo entre bienes y servicios, sólo se puede cambiar de una manera determinada y autorizada; es necesaria para asegurar la consistencia de la transacción.

1.2.1.*Confidencialidad*: ayuda a asegurar que la información importante está disponible sólo para aquellas partes que estén incluidas en una lista de control de acceso. El intercambio de información entre partes se debe regular para prevenir la divulgación de información privada.

1.3.1.*Privacidad*: significa que el sujeto (individuo o entidad) de información puede participar en el control de la información. Se puede considerar al sujeto como el originador de la información: alquileres, compras con tarjetas de

crédito, reservas de pasajes y cualquier otra transacción electrónica que defina o represente los hábitos de las personas. Por ello la privacidad requiere mecanismos de seguridad, políticas y tecnología para brindar control sobre la información.

1.4.1.*Protección*: los items que tienen cierto valor están sujetos a alguna medida de protección. El valor asociado con el comercio electrónico es la información que manejan los procesos que permiten concretar las transacciones de negocios y se puede vincular con los controles adecuados para proteger la información.

2.1. Integridad

La integridad de los datos del comercio electrónico comienza con una definición de la transacción comercial en la que están de acuerdo las partes comprometidas. La transacción comercial puede involucrar múltiples participantes y puede ser modificada por cada uno de ellos, por lo que es importante que las partes estén de acuerdo con todos los estados de la información (inicial, final y todos los intermedios).

Toda transformación o modificación de la información debe ser hecha de acuerdo a una función comercial legítimamente acordada; la comunidad / participantes, establece un método estándar de interacción que no es un estándar ***EDI*** sino la inclusión de las reglas de transformación y modificación del negocio, dentro del estándar.

El comercio electrónico incluye interacciones basadas en redes, a menudo sobre redes públicas, por lo que, conociendo los distintos estados de la información, se pueden planear mecanismos para verificar su correcto intercambio sobre redes; uno de esos mecanismos incluye el uso de algoritmos criptográficos generales conocidos como algoritmos hash. La función de un algoritmo hash es tomar el mensaje de entrada y crear datos de salida conocido como "mensaje digesto", que está relacionado matemáticamente al mensaje de entrada.

Los algoritmos hash se basan en estándares para validar la consistencia de la información desde un origen a un destino. Calculando el hash en el origen y proporcionando el "mensaje digesto" resultante con la información transmitida, el destinatario luego es capaz de recalcular y comparar el resumen resultante con el enviado para verificar la consistencia. Si los resultados son iguales se puede decir que la información es consistente, caso contrario, la información fue modificada en alguna forma. El "mensaje digesto" tiene la propiedad de ser sólo de ida (no se puede determinar la información fuente desde el mismo) y único (hay una muy baja probabilidad de encontrar dos

mensajes con el mismo "digesto"). Cuando la función hash se combina con encriptación, la información puede intercambiarse con integridad entre un origen y un destino. Para ello se sigue el siguiente procedimiento:

- Un origen o fuente crea un mensaje y genera un digesto asociado al mismo.
- El mensaje y el digesto se encriptan y se envían al destino.
- El destino recupera la información encriptada y la función hash.
- El destino genera otra función hash del mensaje fuente y la compara con la hash recibida; si son iguales, la información no fue alterada durante la transmisión.

En ese momento se tienen todos los elementos necesarios para asegurar la integridad de las transacciones comerciales de comercio electrónico. Lo que resta es la implementación de los algoritmos hash y de encriptación y la definición de las operaciones comerciales a través de la tecnología; esta última debería proporcionar la información necesaria para saber cuando aplicar algoritmos hash.

Según que riesgos se perciban se determina el grado de utilización de algoritmos hash; En la siguiente lista se enumera en que momento se puede usar hashing, siendo la sofistificación e integridad de la misma en grado creciente:

1. ***Con cualquier información que se mueva sobre una red pública***: esta es la forma más básica de integridad para una solución de comercio electrónico. Aunque se respalda la integridad de la información entre la fuente y el destino, no se puede garantizar la misma, más allá del perímetro de la fuente y del destino. Tal tipo de implementación debe confiar en procedimientos operativos internacionales para asegurar que las redes y los sistemas internacionales intervinientes no comprometan a los datos.

2. ***Con cualquier información que se mueve sobre una red privada:*** este enfoque no asume que las redes corporativas están libres de problemas de integridad sino que el modelo descrito en el punto anterior se extiende a las redes internas.

3. ***Con cualquier información que se mueva entre sistemas de una red local (LAN, redes seriales, etc.):*** las redes locales son el nivel más bajo de redes entre computadoras; aunque los riesgos son locales, cualquien proceso que tenga enlaces débiles, puede vulnerar la integridad de los datos.

4. ***Con cualquier información que se mueva entre procesos independientes dentro de una computadora:*** es común encontrar sistemas de computación que ejecutan aplicaciones independientes, cada una de las cuales contribuyen a un objetivo común.

5. ***Con cualquier información que se almacene en un sistema:*** este enenfoque está relacionado con el manejo de la información (datos o aplicaciones) almacenada en una computadora. Las operaciones entre las partes residirán en un sistema de archivos o en una base de datos. A menudo la información se almacena temporalmente para luego moverla a la siguiente parte involucrada en el proceso comercial; en este estado la información es susceptible de un compromiso potencial en su integridad (caída del sistema, sabotaje, etc.). Sin embargo, si se genera y mantiene un mensaje digesto en un sistema independiente, previamente al almacenamiento de la misma, se puede validar la integridad de la información. Si se descubre que la información ha sido modificada se puede abortar la transacción o bien se pueden recuperar los datos de los back-up fuera de línea de los más recientes en línea.

Antes de determinar que tipo de método se utilizará para asegurar la integridad de los datos en el sistema, se deben analizar los detalles de algunos riesgos, para considerar el impacto y los costos relacionados a la protección.

3.1. Confidencialidad

La información es el medio a través del cual se intercambian conceptos e ideas. La interpretación de la información por parte de las personas crea conocimientos de los cuales resultan o pueden resultar acciones.

El comercio electrónico no propone resolver el simple intercambio de información sino que explota dichas facilidades para mejorar, extender y ofrecer nuevas oportunidades para la cooperación. Por, ello se deben establecer mecanismos para garantizar la confidencialidad de tales transacciones para que las mismas sean fructíferas. La cooperación consiste en establecer relaciones dinámicas entre las partes involucradas a través de tecnologías, políticas y metodologías; la condición clave para el establecimiento de dichas relaciones es que la información que se intercambie entre las partes permanezca confidencial.

La protección de la confidencialidad de la información normalmente se hace a través del control de acceso a la misma y redefiniendo las reglas de representación de la misma. En el comercio electrónico, la confidencialidad

de la información requiere encriptación, un lenguaje especial que abarca los siguientes puntos:

1. Un sistema de lenguaje único que representa, de forma consistente, información de manera no ambigua.

2. Un sistema de lenguaje lo suficientemente complejo que no pueda ser interpretado fácilmente y, en consecuencia, sólo puede divulgar el contenido de la información aquel que tiene privilegios de acceso.

3. Un sistema de lenguaje que pueda cambiar fácilmente sus reglas basándose en un algoritmo comúnmente entendido. Con el tiempo todos los sistemas de lenguajes basados en un conjunto de reglas, se pueden descifrar por lo que se requiere que el sistema no esté atado a un único conjunto de reglas.

La encriptación proporciona un mecanismo para lograr los requerimientos mencionados y la misma se puede pensar como un sistema de lenguaje dinámico para representar información de manera confidencial ya que permite la creación de un lenguaje nuevo y único que se puede emplear para cada nivel de intercambio de información entre las partes.

Las tecnologías que facilitan los procesos de encriptación convierten la información en lenguaje humano al lenguaje compartido y recién creado entre las partes involucradas. El proceso de encriptación consiste en un algoritmo y una clave; el algoritmo produce distintos resultados (texto cifrado) dependiendo de la clave específica que se utiliza. La seguridad del sistema de encriptación depende de la confidencialidad o secreto de la clave única y la fortaleza del sistema, depende del algoritmo. Los sistemas que ofrecen flexibilidad, como longitudes variables de claves para incrementar la complejidad del texto cifrado, están entre los algoritmos más exitosos y útiles que son adoptados en las soluciones para comercio electrónico.

Los sistemas de encriptación, a través de sus algoritmos y claves, entregan un sistema de lenguaje único (claves únicas y algoritmos disponibles públicamente), complejo (algoritmos y longitudes de claves variables) y dinámico (sistema de clave variable), que cumplen con los requerimientos del comercio electrónico.

4.1. Privacidad

A menudo, confundida con la confidencialidad, la privacidad se refiere al mantenimiento de la confidencialidad de la información asociada a una

persona. Facilitar procesos de negocios a través del comercio electrónico crea una serie de riesgos que pueden comprometer la privacidad de las personas.

1. La información, que inicialmente fue inaccesible (información guardada sobre papel de una manera no estructurada) fue estandarizada (utilización de estándares de intercambio electrónico de datos) y se hizo accesible a través de redes abiertas (Internet, intranets y extranets).

2. Los procesos de comercio electrónico crean nuevas fuentes de asociación de información que revelan los hábitos de las personas. Los sitios de la Web se han transformado en el medio que permite realizar operaciones financieras, operaciones de seguros, consultar literatura, viajar, etc.; cada una de estas facilidades permiten generar un almacenamiento de perfiles de información con el objeto de brindar mejores servicios a los consumidores. Esta actividad es particularmente evidente en aquellos sitios Web que piden datos de registración antes de poder acceder a los servicios que brindan.

Los problemas de privacidad no son nuevos pero, en el contexto del comercio electrónico, están intensificados; la solución para lograr privacidad es a través del anonimato, disociando al individuo del contenido de la información. El anonimato de la información dentro de los lugares de almacenamiento, se puede lograr con una combinación de encriptación y configuración de las estructuras de Bases de Datos (por ej. tener por separado los registros de los pacientes separados de los registros de su salud y que ambos puedan relacionarse a través de la clave personal encriptada del paciente).

2. DATOS DE LA EMPRESA E INTERACCIONES

Las empresas rápidamente están adoptando la tecnología Internet para crear redes privadas que reciben el nombre de intranets que reemplazarán a las redes locales; las mismas se implementan para cubrir con una variedad de propósitos incluyendo e-mail, grupos de servicios, acceso a fuentes de datos de las empresas como así también para la compra y venta de bienes y servicios. La diferencia entre la intranet de una empresa e Internet es que la primera constituye una red interna que puede ser sólo accedida por las personas pertenecientes a la empresa. Los límites entre estas dos redes son impuestos y controlados por firewalls, una combinación de hardware y software que prohíbe accesos no autorizados a la intranet.

Las intranets tienden a perder el control de la información y representan un proceso de aprendizaje para aquellas empresas que se esfuerzan en ingresar al mundo del comercio elec-

trónico. La tabla 4.1 muestra las áreas donde los administradores de comercio electrónico deben enfocar su atención para establecer los controles necesarios que aseguren una implementación segura.

Tabla 4.1 Medidas de control para aplicaciones de e-commerce

Servicio Intranet	Operación general	Riesgos relacionados con Integridad, Confidencialidad y Privacidad	Protección a considerar
Servidor Web y datos	La Web trabaja con un modelo cliente / servidor. Se corre un cliente Web browser como por ej. El Netscape Navigator o el MS-Internet Explorer sobre nuestra computadora. El cliente contacta un servidor Web y solicita información o recursos. El servidor Web los encuentra y envía luego la información al browser Web, el cual muestra el resultado.	El servidor Web se encuentra en una zona que es accesible públicamente (normalmente fuera de la firewall) y por lo tanto los datos están en riesgo.	El uso de Secure Socket Layer (SSL) y Secure Electronic Transaction (SET). Toda la información delicada debe colocarse detrás de firewalls y sólo debe ser accedida a través de interfaces comunes Gateway (CGIs) cuidadosamente desarrolladas (incluyen tecnologías middle-tier inteligentes)
Servidor de mail	Los servidores de mail trabajan como una facilidad excelente para manejar la distribución de información no estructurada. Al mensaje de correo se le pueden adjuntar archivos binarios como por ej. programas ejecutables, video y sonido. Estos archivos se codifican normalmente usando un método conocido popularmente como MIME y un programa uencode que se utiliza para transmitir un fichero binario en un e-mail o en un grupo de discusión.	El acceso a la información, generalmente, sólo es protegido por un sistema de user-id y password. La información es fácilmente accesible por el personal administrativo y por hackers inteligentes. De esta manera, la información no sólo puede ser leída sino también modificada y destruida.	Distribución de certificados digitales que emplean el S/MIME (Secure/Multipurpose Internet Mail Extensión) y Pretty Good Privacy como fuente para la distribución de correo delicado.
Telnet	Telnet sigue el modelo cliente / servidor lo que significa que se corre una parte de software en nues-	Puede circular información altamente confidencial como por ej. identificación del usuarios y claves a otro sis-	Para lograr una implementación Telnet segura, emplear certificados digitales. También se pueden reducir los riesgos

Servicio Intranet	Operación general	Riesgos relacionados con Integridad, Confidencialidad y Privacidad	Protección a considerar
	tra PC para usar los recursos de un servidor distante (host).	tema interno. La ejecución de comandos nativos puede provocar un daño importante a los datos internos y a los sistemas.	utilizando Telnet dentro de una red privada virtual (VAN) con participantes conocidos.
FTP	FTP trabajo bajo el modelo cliente / servidor. Corremos el software cliente FTP en nuestra PC para conectar a un demonio FTP, que nos permite bajar y subir archivos. FTP permite a los usuarios buscar archivos disponibles mediante el cambio de directorios y podemos ver una lista de todos los archivos disponibles en cada directorio.	Los servicios FTP son excelentes caminos para sistemas ricos en datos. Aunque los comandos están restringidos a aquellos ofrecidos por el protocolo, éste permite crear transmitir, recibir y destruir información.	Para implementaciones FTP seguras utilizar certificados digitales. Alternativamente, se pueden reducir los riesgos, usando FTP dentro de una red privada virtual (VAN).
Conversación en línea y mensajes instantáneos	La conversación en línea consiste en conducir en directo, a través del teclado o mouse, conversaciones con otras personas en Internet. También es posible el uso de aplicaciones blancas (white board applications)	Las fuentes de información interactiva proporcionan una dimensión extra a la información. No sólo a través del contenido que proporciona en sí misma sino también por la interacción con otras partes. Todas las acciones pueden grabarse y revisarse posteriormente para un análisis más profundo. La privacidad es importante en esta aplicación.	Se debe realizar sobre conexiones de redes privadas virtuales ó, por lo menos pasadas por un canal SSL.
Video	Consiste en el intercambio de video sobre en Internet. El proceso involucra una tecnología que se refiere a una cinta de video, fraccionando el video en pedazos controlables para la transmisión y ensamblado y su posterior visón en el destino.	Es una fuente de información visual y auditiva muy importante. El riesgo más importante puede ser el que está ligado a la privacidad	Se debe realizar sobre conexiones de redes privadas virtuales ó, por lo menos pasadas por un canal SSL. Debido a la cantidad depurada de información que se pasa en estas sesiones puede no ser un servicio efectivo una vez que se usa la encriptación.
Interfase	Son protocolos de comuni-	El entendimiento de estos	Todos los procesos de respal-

Servicio Intranet	Operación general	Riesgos relacionados con Integridad, Confidencialidad y Privacidad	Protección a considerar
de puerta Comun (CGI)	caciones por los medio de los cuales un servidor Web se puede comunicar con otras aplicaciones. Por ej. una aplicación CGI se usa a menudo para acceder información que reside en bases de datos.	procesos proporciona especialmente accesos a servicios en los cuales han sido ofrecidos. El riesgo mayor viene dado por el reemplazo o modificación de los procesos para permitir un acceso o manipulación posterior de la información.	do incluyendo las aplicaciones deberían ~~ser~~ reforzarse. Se deben realizar los procesos responsables para hashing, el mantenimiento en un repositorio seguro y la verificación de la integridad (comparación hash) de CGIs y agentes de una forma automática y frecuente. Se deben realizar test de penetración a través de terceras partes para validar la integridad de la implementación.
Java y ActiveX	Consiste en la habilidad de correr aplicaciones que residen en Internet antes que en una computadora.	El procesamiento de la información en el cliente somete a riesgos potenciales a la información del cliente.	Los applets Java y los controles Actives se deben acompañar con certificados digitales o deben ser distribuidos por servers con certificados digitales de buena reputación. Por ej. cuando aceptamos el uso de un applet Java firmado, recibimos un certificado del pedido de acceso del applet.

3. METODOLOGÍAS PARA LOGRAR CONFIANZA

La lista siguiente enumera los distintos métodos que pueden utilizar los administradores de comercio electrónico para incrementar y representar, de una forma normalizada, el nivel de confianza en sus soluciones de comercio electrónico.

- *Controles de auditoria e infiltración.* Todas las implementaciones de comercio electrónico deben incluir una revisión de auditoria, desde el principio a fin, como así también un test de infiltración para asegurar que el sistema no será comprometido. Actualmente, la mayoría de las grandes firmas de auditoria ofrecen tales servicios y certifican como segura y confiable a la implementación si éstas superan todos los controles.

- *Cajas blancas.* Aquellas empresas que deseen realizar comercio electrónico pueden utilizar un enfoque de *caja blanca* que implica comisionar a una ter-

cera parte confiable y con probada reputación, auditar todos los sistemas comerciales para lograr un acuerdo mutuo de un estándard de "alto nivel". El objetivo de este enfoque es permitir la normalización de estándares de confianza mientras que se mantiene la confidencialidad entre cada una de las partes comerciales.

- *Intermediarios*. Los proveedores de servicios de terceras partes para el comercio electrónico, ofrecen mecanismos que permiten ayudar a resolver problemas de confianza entre socios comerciales. Un ejemplo de esto lo constituyen los *escribanos electrónicos*: la información que se intercambia entre socios comerciales puede autenticarse a través de una tercera parte confiable. Otro ejemplo es el de las *autoridades certificantes* que realizan operaciones de pago y publicación de certificados para personas, servidores Web y para descarga de software.

- *Certificación acreditada*. Cada vez más, las empresas obtienen certificaciones ***ISO 9000*** que definen una obligación de calidad. Aunque no es un indicador definitivo, ***ISO*** y algunas certificaciones acreditadas otorgan una medida de credibilidad y habilidad organizacional para realizar negocios con la mejor calidad en mente.

- *Grupos estándares*. La adopción de estándares bien definidos y en algunos casos de aquellos que recién se están comenzando a usar, también ayudarán para normalizar las expectativas entre las empresas. Asociaciones tales como la ***IETF*** (Internet Engineering Task Force), ***OMG*** (Object Management Group) y ***W3C*** (World Wide Web Consortium) están entre aquellas que contribuyen de forma importante a la interoperabilidad de las transacciones de Internet.

CAPITULO 5
SEGURIDAD EN E-COMMERCE

1. INTRODUCCIÓN

A menos que las operaciones comerciales sean seguras en cuanto a intrusiones, mal uso, sabotaje y robo, las mismas no pueden generar relaciones basadas en la confianza. El comercio electrónico tiene que ser seguro ya que con el mismo no se ve a la otra parte, cara a cara.

Se puede esperar un gran crecimiento y sofisticación de los ataques a la seguridad del comercio electrónico. Cada forma nueva de comercio trajo consigo grandes amenazas para las cuales debieron construirse protecciones. Hoy en día, existe una industria integral de fraudes de tarjetas de crédito y teléfonos celulares que buscan la vulnerabilidad del complejo conjunto de enlaces comerciales.

Las redes electrónicas actuales son difíciles de proteger por sus propios diseños y objetivos. Ofrecen accesos, al mundo, en el caso de la Web y a servicios comerciales, en redes de intercambio de datos, controlados más ajustadamente. El problema fundamental para la seguridad es entonces el intercambio entre acceso y control: en su mayor parte uno aparece como riesgo del otro.

Permitiendo el acceso a todos, se permite el acceso también a bromistas maliciosos, hackers aficionados, estafadores profesionales y ladrones y aún a peligrosos terroristas. Las amenazas son reales pero se pueden prevenir o protegerse de ellas. El desafío del comercio electrónico consiste en lograr este objetivo de protección y al mismo tiempo mantener la libertad de acceso.

El mundo digital de las redes de telecomunicaciones, software y propiedad de la información es muy distinto del mundo de las redes comerciales que tienen entidad física; en éstas, el producto es físico y existen puntos de control bien definidos, regulaciones bien establecidas y códigos de buenas prácticas. A pesar de que el contrabando es un problema mundial, el sistema sabe donde, porque, como y que monitorear. Muy pocas de estas condiciones tienen aplicación en las redes de comercio electrónico.

El aspecto más desconcertante del mundo de las redes digitales del comercio electrónico, especialmente Internet, es la ausencia de una autoridad central y de una forma en que esta pueda regular a aquellos que la usan. Internet es fundamentalmente un conjunto internacional de redes independientes que pertenecen y son operadas por muchas organizaciones. No hay comités culturales, legales o legislativos uniformes para manejar malos comportamientos. Tampoco conocemos, en muchos casos, que leyes tienen aplicación menos aún como deben cumplirse e implementarse.

2. CUIDAR LA INFORMACIÓN

Ocuparse primero y principalmente de la información que le pertenece y de la que es el dueño es el componente clave de los esfuerzos de una empresa para manejar la seguridad; si la información no se puede robar, no puede ser usada o modificada. Independientemente del nivel y naturaleza del servicio, y por lo tanto del acceso, un principio fundamental de seguridad, es la encriptación de los datos de forma que ninguna persona pueda piratearla.

La encriptación es una disciplina muy compleja y es un área de especialización técnica, pero sus principios son tan simples como su matemática compleja. Básicamente implica el uso de un algoritmo para convertir datos en lo que parece una cadena aleatoria de bits, 0 y 1 mezclados. Utiliza una clave para llevar a cabo esto y la misma u otra clave para decodificar la cadena de bits a información original.

Aunque los administradores de negocios no necesitan saber como se realiza este procedimiento, es importante que tengan un conocimiento básico del mismo dado que son criterios tanto para la seguridad de la empresa como para el sentido que de la misma tengan los clientes.

Así como hay una relación acceso / control, también existe una relación seguridad / costo. Si se quiere ver el proceso de encriptación en acción, basta con llevar a cabo una transacción con algunos de los sitios líderes de comercio electrónico, por ejemplo, Amazon.com; este sitio, cuando se requiere la mayor de las seguridades, se mueve sin que sea notado, de un nivel sin encriptación a un enlace de nivel ***SSL*** encriptado. La encriptación ***SSL***, significa que el enlace entre una PC y los servicios que brinda el sitio será seguro y por

lo tanto el envío del número de tarjeta de crédito a través de la red será y permanecerá de forma privada.

De igual manera, en cualquier momento que se usa una tarjeta electrónica, la red bancaria utilizará el esquema de encriptación estándar ***DES***, el cual ha trabajado bien por alrededor de dos décadas, pero el algoritmo y la clave que emplea no son completamente seguros: alguien con una computadora, suficientemente potente, podría probar deducir la clave y de esta manera conocer el código. Una de las realidades de la encriptación es que, así como las herramientas que permiten obtener algoritmos y claves cada vez más complejas para ser utilizados en la codificación y decodificación de datos, cada vez son más poderosos y certeros los intentos de conocer los mismos.

La encriptación descansa en el uso de claves, las que son números primos (aquellos que no pueden dividirse por ninguna combinación de otros números excepto por sí mismos o por 1); cuanto más largo es el número de bits que utiliza una clave de encriptación, mayor será el tiempo que una computadora necesitará para descifrarla..

Teniendo en mente que el esquema de codificación binario (0 y 1) de la tecnología digital representa números que son potencias de 2, una clave de 128 bits puede representar un número muy extenso y utilizándola en algoritmos matemáticos, que son muy complejos, se obtiene un sistema que transforma los datos en incomprensibles para cualquier intruso. Por otra parte, los nuevos intrusos tienen computadoras de mucha potencia que pueden poner a trabajar para intentar el calculo inverso y esta es la razón por la cual muchos expertos argumentan que las claves y cálculos usados en el sistema ***DES***, que es el núcleo para las operaciones de cajeros automáticos, no son los adecuados para la nueva generación de comercio electrónico.

El argumento opuesto sostiene que no se justifica en muchos casos dado que es suficientemente bueno y que el costo de agregar poder de procesamiento y el tiempo que lleva encriptar y desencriptar datos no son necesarios para la mayoría de las situaciones.

3. CLAVE PUBLICA VERSUS CLAVE PRIVADA

Los sistemas modernos de encriptación se clasifican en dos categorías : simétrica y asimétrica. La encriptación simétrica se basa en un modelo que requiere que exista una clave común (compartida secretamente) entre cada relación confiable. La integridad de tales relaciones confianza es altamente dependiente de los mecanismos de control para la distribución y manejo de las claves. Ese tipo de sistema se adecua a conjuntos bien definidos de transacciones, a relaciones muchos-a-uno administradas por la empresa central y con números de clave pequeños de las partes. De esta manera se forman redes de

reconocida confianza que están bien delimitadas y en actividad más que nuevas u ocasionales.

Por el contrario, las soluciones de comercio electrónico no son redes de reconocida confianza sino que constituyen un gran número de interacciones descentralizadas sin ninguna coordinación central. Algunas veces son para un propósito determinado y a menudo entre partes sin historia previa de trabajo conjunto. Para cada una de estas partes, tener claves de encriptación en el lugar mismo sería imposible; los nuevos clientes en línea necesitan llevar a cabo operaciones seguras de forma inmediata. No se puede otorgar a cada uno de los clientes una clave simétrica, compartida, cuando lo solicitan. Para un modelo simétrico, 1.000 usuarios necesitan del manejo de 1 millón de claves distintas, mientras que 10.000 usuarios requerirán 100 millones de claves, las cuales se deben distribuir antes que de que el usuario pueda hacer uso de su tarjeta de cajero automático.

Los sistemas de encriptación asimétrica (conocidos como sistemas de clave pública) resuelven el tema de distribución de clave anulando la necesidad de distribuir un secreto compartido. En este modelo tanto la matemática y la tecnología necesaria son complicadas; utilizan dos claves: una pública y otra privada. La información encriptada con la clave pública, distribuida libremente, sólo puede desencriptarse con la clave privada complementaria; las claves privadas nunca se distribuyen quedando en cada parte.

Por el contrario, la encriptación con clave simétrica necesita que los sistemas de clave secreta se transmitan introduciendo la posibilidad de que un intruso descubra la clave secreta; los sistemas de claves simétricas administran las relaciones a través de políticas rigurosas en sus procesos de distribución de claves.

Los sistemas de encriptación asimétricos, a través de firmas digitales y autoridades certificantes, crean relaciones altamente confiables y flexibles capaces de cumplir las demandas del comercio electrónico ya que las mismas son personales y privadas. Una de las desventajas de estos sistemas son sus dispares deficiencias de funcionamiento.

Normalmente los sistemas de encriptación simétrica disponibles son considerablemente más rápidos que los sistemas asimétricos de encriptación actuales (cien veces más rápido en software, mientras que entre mil y diez mil veces en hardware). Los sistemas simétricos son más eficientes, incluyendo la relación costo / eficiencia, mientras que los asimétricos son más efectivos incluyendo la relación costo / ineficiencia. Sin embargo combinando ambos sistemas se puede generar un método mejor como es el caso del protocolo de transacción segura ***SET***, de ***VISA*** y ***MASTERCARD***, que permite proteger las operaciones con tarjetas de créditos sobre Internet.

Los participantes activos en cada transacción ***SET***, incluyen: un poseedor de tarjeta (miembro registrado), un comerciante y el emisor de la tarjeta (distribuidor). En el mundo de las operaciones con tarjetas de créditos, es normal para los emisores administrar muchos cientos de operaciones por segundos por lo que es imprescindible que el proceso no sólo sea efectivo sino también eficiente.

Los siguientes pasos detallan la interacción básica entre un buscador de la Web y un servidor (los pasos se han simplificado para representar claramente las interacciones simétricas y asimétricas):

1. El buscador y el servidor intercambian claves públicas.

2. El buscador crea una clave simétrica (sesión de clave) y encripta la misma con la clave pública del servidor y envía un paquete del mensaje al servidor.

3. El servidor desencripta el paquete y obtiene la clave simétrica.

4. Se establece una sesión confiable y se intercambia la siguiente información, utilizando la clave simétrica durante la duración de la sesión.

Todos los sistemas de encriptación son susceptibles de ataque, práctica conocida como criptoanálisis; estos ataques dependen del tipo de algoritmo y de la longitud de la clave secreta utilizada. A medida que la longitud de la clave aumenta, el tiempo requerido para descifrarla también aumenta. Los algoritmos de encriptación asimétrica permiten, a diferencia de los simétricos, longitudes dinámicas de claves lo cual agrega flexibilidad intrínseca en los mismos haciéndolos más robustos que los simétricos.

La tabla 5.1 indica las distintas propiedades para los sistemas de clave simétrica y asimétrica basadas en la robustez de la encriptación (probabilidad de someterse a un compromiso), desempeño (gasto en computación y tiempo empleado), funcionalidad (servicios principales) y distribución (claves y otros elementos criptográficos).

	Simétrica (Clave Privada)	**Asimétrica (Clave Pública)**	**Perspectiva para el e-commerce**
Potencia / versatilidad	- Fallas bien comprendidas. - La estructura de las técnicas de encriptación se ajusta a eficientes implementaciones en hardware. - Rapidez para encriptar y desencriptar mensajes. - Juegos de herramientas robustas.	- No se necesita intercambiar información secreta. - La versatilidad de los algoritmos los hace apropiados para una gran variedad de funciones relacionadas con la seguridad. - Poderoso conjunto de herramientas RSA.	- Se requerirá una buena mezcla de sistemas de clave simétrica y asimétrica.

	Simétrica (Clave Privada)	Asimétrica (Clave Pública)	Perspectiva para el e-commerce
	provistas por una gran variedad de vendedores. - Tamaño de clave relativamente chico para el nivel de seguridad ofrecido.		
Protección soportada (defensa contra ataques)	*Longitud de clave* 56 64 80 112 128 El 17 de julio de 1998, la Fundación Frontera Electrónica, rompió una encriptación DES en 56 horas.	*Longitud de clave* 384 512 768 (personal) 1792 (compañía – ejecutivo) 2304 (Autoridad Certificante) En 1997, con un costo de 1 millón de dólares y en menos de 8 meses, un conjunto de datos encriptados RSA, con clave de 512. bits pudo ser desencriptado.	- Las claves asimétricas son obligatorias para la autenticación, integridad, no-repudio y distribución de claves simétricas. - Se debe usar clave simétrica en una sesión u operación básica. - La longitud de la clave simétrica es una función del desempeño versus el compromiso de riesgo.
Desempeño tiempo requerido para encriptar y desencriptar datos	- En software, el algoritmo simétrico es por lo menos 100 veces más rápido que un sistema de clave pública. - En Hardware, el algoritmo simétrico es 1.000 a 10.000 veces más rápido.		- Se requerirá una mezcla de sistemas de clave simétrica y asimétrica. - La encriptación en hardware ayudará para el establecimiento de redes virtuales (autenticación entre intranets de empresas que se basan en acuerdos mutuos de política).

	Simétrica (Clave Privada)	Asimétrica (Clave Pública)	Perspectiva para el e-commerce
Funcionamiento - firmas digitales	- No puede ser gestionada sin un par de claves pública y privada.	- Se encripta con la clave única privada del remitente. - La desencriptación se logra con la clave pública del remitente que confirma el origen de los datos ó mensaje.	- Sólo la confianza universal acepta la existencia de un identificador único. - Necesario para el establecimiento de relaciones confiables.
Funcionamiento - no repudio (acción de la obligación de las partes en una transacción).	- Procesos rigurosos de distribución de claves simétricas. Es posible repudiar una transmisión afirmando que el secreto de la misma fue comprometido.	- Aplicar una firma digital. Dado que existe una única copia de la clave privada del remitente, la operación no puede ser repudiada.	- Las firmas digitales limitan la responsabilidad de todas las partes. - Las firmas digitales son una parte fundamental del protocolo SET (transacciones con tarjetas de crédito en Internet).
Funcionamiento – integridad	- Si los datos desencriptados no son visibles se puede asumir que, ó bien los datos se modificaron después de su encriptación ó que la clave privada que se usó es incorrecta. - En cualquiera de los dos casos, se debe notificar a la parte remitente que ocurrió un problema. - Si este problema continúa, se debe notificar de una posible intromisión (hacking), al gru-	- Si el chequeo de la firma digital falla, entonces la clave de encriptación fue incorrecta ó los datos fueron alterados después que se creó la firma (por ej. durante la transmisión). - En cualquiera de los casos, la parte emisora debe ser notificada que ocurrió un problema. - Si este problema continúa, se debe notificar de una posible intromisión (hacking), al grupo de seguridad de la empresa	- Es una función crítica para el transporte de datos sobre redes públicas o redes de baja confiabilidad.

	Simétrica (Clave Privada)	Asimétrica (Clave Pública)	Perspectiva para el e-commerce
	po de seguridad de la empresa.		
Funcionamiento - clave privada inviolable	- A pesar de que los tamaños de las claves son pequeños, los sistemas simétricos están mal ajustados a las técnicas de gran potencia de inviolabilidad cuando el número de claves crece dadas las funciones cuadráticas del número de usuarios. 1.000 usuarios requieren el manejo de un millón de claves distintas, mientras que 10.000 usuarios requieren 100 millones.	- A pesar de que las clave son más largas (generalmente más de diez veces el tamaño) que aquellas de los sistemas simétricos, el número de claves necesario crece linealmente como función del número de usuarios. Por ello, los requerimientos de complejidad y espacio son considerablemente menores en operaciones de gran potencia.	- Medios de recuperación de la información encriptada (por ej. las claves privadas de los empleados de una empresas se mantienen inviolables). - Para los sistemas asimétricos, la clave privada no es más única y hay problemas abiertos de disputas de no repudio.
Distribución / publicación de clave	- Las claves se generan normalmente en el servidor y se distribuyen al usuario a través de canales seguros. Las técnicas de encriptación asimétrica se usan a menudo para encriptar claves simétricas para su distribución.	- Las claves públicas se pueden anunciar en un sistema de directorio público. Las claves son generadas normalmente en forma local y luego, las claves públicas se registran con un directorio central o autoridad certificante (CA).	- Las claves asimétricas son fundamentales para el comercio electrónico.

Tabla 5.1 Clave Simétrica vs. Clave Asimétrica

Las técnicas de seguridad se han perfeccionado para incluir tanto encriptación simétrica como asimétrica. Cada una de ellas contribuye a distintas funciones que ayudaron a la proliferación del comercio electrónico. Ambos esquemas de encriptación, simétrico y asi-

métrico, se deben considerar para obtener soluciones seguras apropiadas de comercio electrónico.

Desde perspectiva de los administradores de negocios, la encriptación está bastante lejos del lado comercial del comercio electrónico, pero está muy cerca del cliente, aún si el cliente no sabe acerca de esto. Es el cliente el que inicia el flujo de información y envía y recibe datos de valor: información de tarjeta de crédito, órdenes e identificación personal.

Los datos disparan software que accesan la información privada, de la cual es dueña la compañía, sus bases de datos, sus sistemas de procesamiento y operaciones. Pueden también iniciar enlaces a otras compañías: procesadoras de tarjetas de crédito, suministrar cadenas o series de socios, proveedores de servicios, minoristas, fletes y otros. Cada socio en la cadena del comercio electrónico, depende de la seguridad de la información. Si uno de ellos tiene deficiencias en la adecuada capacidad de encriptación, es casi seguro que es dado de baja como socio. Justamente no se valora adecuadamente el riesgo, lo que hace que la seguridad sea realmente una condición del negocio. La cadena sólo es tan fuerte como sus enlaces más débiles y esos tipos de enlaces no deben ser su empresa.

4. ASPECTO ECONÓMICO DE LA SEGURIDAD
(análisis de riesgos versus costos)

Las inversiones en seguridad se ven casi siempre como un mal necesario. Sin embargo, en el caso del comercio electrónico, las mismas pueden hacer la diferencia entre el éxito ó fracaso. Además, los sistemas de comercio electrónico difieren de los sistemas tradicionales en que aquellos están en estado de flujo constante. Esta naturaleza dinámica del comercio electrónico es un símbolo de la rápida evolución de la tecnología que apuntala estas soluciones y una cultura del consumidor que espera constantemente innovaciones en productos y servicios.

Los administradores de comercio electrónico deben reflejar estas expectativas en sus inversiones sobre previsiones de riesgos. La pregunta que queda hacerse es ¿cómo y cuándo se debe invertir en la tecnología de seguridad para comercio electrónico? Históricamente las empresas han desarrollado de manera intensa software y procesos de seguridad como pensamiento posterior a la implementación de un sistema.

El problema con este tipo de enfoque es que el resultado a menudo involucra sacrificar algo en el funcionamiento o agregar gastos en el reajuste de las medidas de seguridad. Tales tácticas pueden encajar bien en implementaciones cerradas, pero no son prácticas para el comercio electrónico. La verdadera naturaleza del comercio electrónico es proporcionar servicios donde sea, en cualquier momento, sobre cualquier dispositivo. El comercio electrónico se extiende detrás de los límites de la empresa abriendo el sistema de la empresa y

las fuentes de información (almacenes estáticos y dinámicos), que a su vez agrandan los riesgos de la empresa. Como tal, las soluciones de comercio electrónico tienen una baja tolerancia para una seguridad posterior tanto que pueden socavar el éxito de una implementación. La experiencia ha demostrado que las implementaciones que tienen integrada un componente de seguridad antes que hacer luego un reajuste, pueden reducir significativamente las inversiones en seguridad, proteger la integridad funcional de la solución y mantener el nivel de confianza.

El objetivo es, entonces, realizar el análisis de riesgo conjuntamente con el diseño del sistema. Una vez que se ha definido el sistema de servicios, se pueden inferir problemas potenciales y se pueden incluir dentro del diseño medidas recíprocas. Los análisis tradicionales de riesgos son enfoques generalizados que emplean probabilidades y métodos poco sutiles. Estos métodos son metódicos y bastante caros, resuelven los problemas de seguridad ajustando hacia atrás ó enmascarando la funcionalidad. Alternativamente, analizar los problemas durante la etapa de diseño, permite aplicar seguridad a funciones de negocios relacionadas.

Consideremos a una empresa que se enfrenta a la implementación de una nueva y simple aplicación de comercio electrónico como por ejemplo agregar un catálogo en línea para que los clientes realicen compras a través de la Web en vez del centro de llamadas. Si previamente se implementaron soluciones de comercio electrónico, la empresa decide aprovechar las facilidades y servicios existentes (reducción de gastos a través del reuso de la tecnología, políticas y procesos existentes), como parte del diseño de la solución. Ya tiene un amplio sistema de manejo de inventario que se puede enlazar al servicio de catálogo.

Durante la implementación de la solución, se realiza una auditoria para determinar si el sistema existente de seguridad se verá comprometido por la nueva implementación. La auditoria determina que el funcionamiento del nuevo sistema introduce nuevos riesgos que se deben mitigar. El sistema de administración de inventario es un sistema cerrado; sólo puede ser accedido a través de la red interna de la empresa, la cual emplea una protección básica, tal como palabras claves. La red interna está protegida por un firewall.

El personal de los centros de atención telefónica, coloca pedidos desde sus puestos de trabajo que son parte de la red interna de la empresa y por ello no necesitan protección extra. La red utiliza una clave simétrica de 128 bits de longitud, completamente adecuada para el sistema cerrado pero no para uno que es abierto ampliamente a todo el mundo. Sería muy fácil, para un hacker experimentado, ingresar al mismo.

Sólo hay dos soluciones prácticas para resolver el problema: eliminar la nueva función o gastar bastantes fondos para proteger los recursos, el precio que resulta de la combinación de recursos para ambas soluciones. La inversión excede el valor de la oportunidad pero no la combinación de los recursos de ambas soluciones. Por eso, en esta instancia, los fondos necesarios. Los fondos requeridos hacen a la iniciativa completamente improductiva. Si el análisis de la amenaza fue bien dirigido frente al tipo de ataque, este problema se podría haber advertido por medio de una alternativa costo / efectividad que proporciona una

solución adecuada al comercio electrónico. El diseño del sistema debería incluir un nuevo firewall (cortafuego), construido para manejar el flujo público de tráfico con sus propias capacidades de encriptación más una nueva firewall enlazada dentro del sistema de red privado.

La lección que debe aprenderse de este ejemplo típico es que los problemas técnicos de seguridad son fácilmente dejados de lado en el diálogo sobre negocios de comercio Electrónico. En este caso, las oportunidades de negocios son claras y simples: permitir a los clientes ingresar a un catálogo multimedia. La justificación comercial asume el uso de la Internet pública para el acceso de clientes y el sistema interno para los pedidos. ¿Por qué deberían pensar en los problemas de seguridad los proyectistas de negocios, el software de la empresa que brinda el paquete de software de catálogo y el pequeño grupo que construye el sistema? Ellos sabían que la red interna era segura y asumieron que era todo lo que se necesitaba. Miraron a la seguridad como una utilidad, no como una respuesta a un riesgo y como un intercambio riesgo / costo. La nueva funcionalidad agrega un nuevo riesgo: que estaban desprevenidos. Y sus decisiones generaron un dilema, riesgo / costo, mayor que lo que pensaron.

Las opciones de negocios generan consecuencias tecnológicas y viceversa; los administradores lograrán soluciones de seguridad para comercio electrónico, efectivas y económicas, mediante la sincronización del análisis de los riesgos con los objetivos del negocio. Aún se necesita el análisis tradicional de la seguridad física y de entorno, de hardware, software, operaciones y comunicaciones, pero deben ser manejado por problemas de negocios y administración desde el *principio de la planificación.* Esto construye seguridad dentro del diseño de soluciones de comercio electrónico antes que defensas desarticuladas que requieren de coordinación compleja.

5. MARCO PARA LA CONSTRUCCIÓN DE CONFIANZA

El continuo crecimiento de las redes y la dependencia de ellas, de las empresas, atrae a sus adversarios a explotar sus vulnerabilidades. Para comprender los posibles problemas, se debe establecer primero un contexto en el cual se discutan estas cuestiones. La siguiente figura es un modelo simple que identifica los elementos clave que son susceptibles a problemas por parte de sus adversarios.

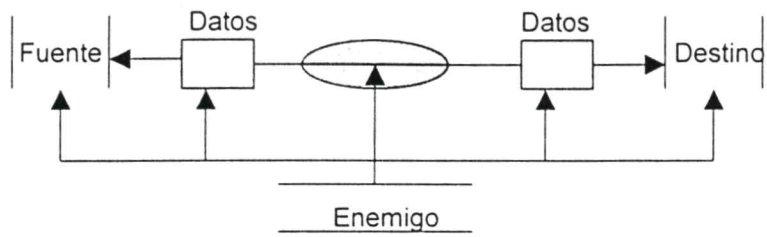


Fig. 5.1 Modelo generalizado para las operaciones de EC

Aunque es un dibujo simplificado que oculta la complejidad de los numerosos detalles y pasos intermedios, la imagen define tres componentes clave que pueden ser comprometidos por los adversarios: fuente, destino y red. Las dos partes cooperan para intercambiar datos / información y se crea un canal lógico (relación) entre la red e Internet por medio de la identificación de las direcciones fuente y destino, un proceso complejo manejado y enmascarado por protocolos de comunicación (por ej. TCP/IP para Internet).

Asegurar un sistema de comercio electrónico requiere colocar en su lugar las precauciones necesarias para prevenir problemas. Para lograr esto, los administradores de comercio electrónico, deben enfocar su atención sobre los elementos que pueden directamente afectar o controlar. El elemento más nebuloso en nuestro diagrama de contexto es la red.. El anonimato de las redes proporciona condiciones perfectas a los adversarios para crecer. Las áreas que están en contacto con la red deben tener especial consideración por parte de los administradores de comercio electrónico.

6. RIESGOS DE LOS SISTEMAS DISTRIBUIDOS

Las empresas, a menudo, fallan en entender los problemas potenciales que surgen con la implementación de un sistema de comercio electrónico; las amenazas son sutiles y difícilmente visibles. Los motivos que se encuentran detrás de un ataque enemigo pueden ser uno o una combinación de los siguientes: robo de documentos u otros datos valiosos, destrucción de datos, modificación de datos, destrucción de la integridad de la red, rechazo de servicios y empañar la reputación.

Antes que los recursos se puedan proteger, primero se debe entender como se llevan a cabo los ataques. Las siguientes figuras categorizan las distintas formas de ataque que se pueden llevar a cabo sobre sistemas distribuidos y constituyen formas comunes de ataques al e-commerce, retratadas sobre un modelo generalizado de operación de e-commerce:

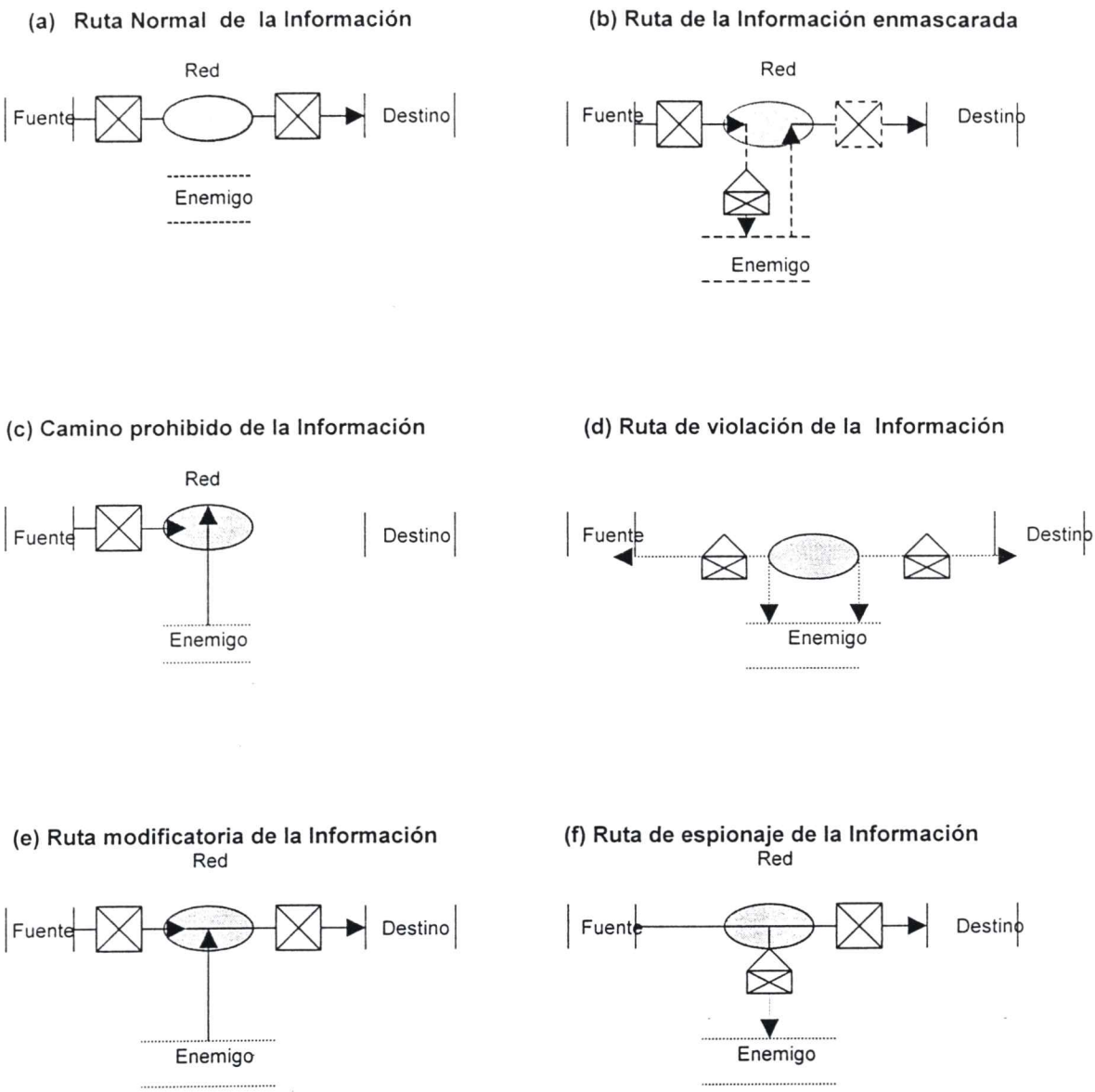


Fig. 5.2 Formas comunes de ataques al comercio electrónico

El enmascaramiento de la información (Fig. 5.2 b) es aquel en el cual se engaña al destinatario haciéndole creer que la información enviada por el enemigo se origina en el remitente. Los ataques enmascarados incluyen una ó más de las otras formas de ataque; tanto el destinatario como el remitente pueden verse afectados durante un ataque enmascarado. La información que se envía desde el origen se intercepta y puede ser susceptible de ser modificada y este mensaje modificado ó suplantado se envía luego al destinatario bajo el nombre del remitente. No sólo se ha descubierto la información, tal como por ejemplo, las secuencias de autenticación del remitente y el destinatario, sino que también la colaboración puede ser socavada como resultado del manipuleo.

La ruta prohibida de la información (Fig. 5.2 c), es un ataque puntual. La única intención de este ataque es hacer caer el sistema, degradar la performance, ó consumir recursos durante el flujo normal de la información. Un ataque de este tipo sería, por ejemplo, bombardear al origen y al destino con requerimientos ó introducir un virus en los sistemas de origen ó destino.

La violación de la información (Fig. 5.2 d), generalmente es el resultado de logins (inicio de sesión) no autorizados. La penetración, tanto en el origen como en el destino, pueden ocurrir por mal uso en el robo, contraseñas supuestas, aplicación de tácticas de ingeniería sociales ó falta apropiada de autenticación. El compromiso ocurre cuando un enemigo obtiene ilegítimamente una contraseña y la usa para estorbar en el sistema. Las contraseñas de los administradores del sistema son el blanco preferido para el robo, dado que tienen privilegios administrativos sobre el sistema y las cuentas de los usuarios. Si un enemigo tiene éxito en comprometer la cuenta de un administrador del sistema, puede asumir cualquier identidad que desee. Los enemigos astutos también crearán identidades ocultas para usarlas en días posteriores por si los descubren y se cambian las claves.

La ruta de modificación de la información (Fig.5.2 e) es la conducta maliciosa de modificar ó destruir archivos mientras pasan a través de la red. Aunque los archivos pueden encriptarse durante la transmisión, también pueden dañarse estando en tránsito. Los archivos resultantes, después de su arribo a destino, serían inútiles dado que la desencriptación no sería posible.

El espionaje de la información involucra a un enemigo pasivo que acumula información que se intercambia entre una fuente y un destino. El husmeo es una actividad encubierta que ocurre sin que lo conozca la fuente ó el destino. Las empresas que usan correo electrónico a través de Internet y que omiten proteger sus negocios críticos a través de la encriptación, son los blancos preferidos del enemigo que espía.

Los sistemas de comercio electrónico son vulnerables a cualquiera de estas formas de ataque. Además, los problemas tradicionales (físicos y de procedimientos), son todavía una parte muy importante de las implementaciones del comercio electrónico y deben ser repartidos con acuerdo. Cual forma de ataque es la más importante dependerá del tipo de aplicación de comercio electrónico implementada. El rango de enemigos varía desde bromistas, que quieren demostrar sus habilidades entre sus pares, hasta ladrones serios. Los bromista actúan pública y simplemente con acciones tales como modificación y rechazo de servicio, considerando que los enemigos peligrosos prefieren el anonimato para lo cual utilizan técnicas tales como enmascaramiento, husmeo y penetración (uso no autorizado de identificaciones y contraseñas).La siguiente tabla resume los problemas mencionados previamente aportando medidas preventivas para cada caso.

Ataques	Amenazas	Consecuencias	Medidas Preventivas	Consecuencias para el EC
Modificación	- Manipulación de los datos fuentes. - Manipulación del tráfico de mensajes en tránsito.	- Pérdida de información - Vulnera las operaciones comerciales.	- Firmas digitales	- Falsedad de la información - Reducción de la legitimidad de la información. - Potenciales problemas de pleitos.
Enmascaramiento y husmeo	- Escuchas secretas en la red. - Robo de información, tanto en el origen como en el destino. - Información sobre la configuración de la red. - Información sobre que origen habla a un destino.	- Pérdida de información. - Pérdida de privacidad.	- Autenticación - Encriptación	- Violación de la privacidad del cliente que pueden derivar en problemas legales. - Dificultades en las relaciones de confianza mutua.
Penetración	- Personificación de legítimos usuarios. - Falsificación de datos.	- Falsos usuarios. - Creencia de que la información falsa es válida.	- Autenticación - Encriptación	- Todo lo que se describió en las líneas superiores.

Tabla 5.2 Análisis de las amenazas al e-commerce

7. COSTO DE LA PROTECCIÓN DE RIESGOS

En todas las implementaciones de sistemas hay algunos gastos que deben asignarse a mejorar la seguridad. El gasto de la prevención de riesgos entra en una de dos grandes categorías: gastos técnicos y aquellos que no lo son.. Los gastos técnicos pueden incluir hardware, software, mantenimiento, capacitación, actualizaciones, suministros, requerimientos de espacio físico y autoridad. Los gastos no técnicos pueden incluir personal, entrenamiento, instalación. Administración, actualización y control de la solución. También deben con-

siderarse el momento y los factores convenientes que hacen necesaria la toma de esta decisión.

Debido a que no existe un mecanismo totalmente seguro, los riesgos del comercio deben sopesarse contra los gastos de prevenir las amenazas enemigas. Desdichadamente, evaluar la información sobre seguridad de riesgos no es tan precisa como uno desearía dado que la seguridad perfecta es imposible. En el comercio electrónico, el intercambio debe hacerse con una combinación de seguridad, funcionalidad, confiabilidad y costo. La expedición es uno de los riesgos de administración del comercio electrónico. La figura 5.3. muestra que las inversiones en seguridad en el comercio electrónico, significan compensar la inversión (considerando la actividad necesaria pero inútil) requerida para penetrar el sistema (mejoramiento de la seguridad).

La clave para seleccionar la combinación correcta es considerar el valor de lo que se quiere proteger y el costo que requiere hacer esto. Para un producto hay que considerar la posibilidad de la pérdida y el posible valor de esa pérdida para la empresa.

Los administradores de comercio electrónico deben también tener en mente los gastos en que se incurre por los impactos cruzados que se producen por la seguridad de los sistemas. Las soluciones técnicas y no técnicas pueden afectar adversamente la performance y calidad del servicio. En tales situaciones puede ser necesario apuntalar los sistemas (capacidad y facilidades) y/o los procesos (más personal) para compensar. El análisis de los riesgos debería llevarse a cabo durante la etapa de diseño de un nuevo sistema de comercio electrónico y así los administradores de comercio electrónico, para mayor precisión y seguridad, deberían conducir estas etapas durante la definición de la funcionalidad del sistema.

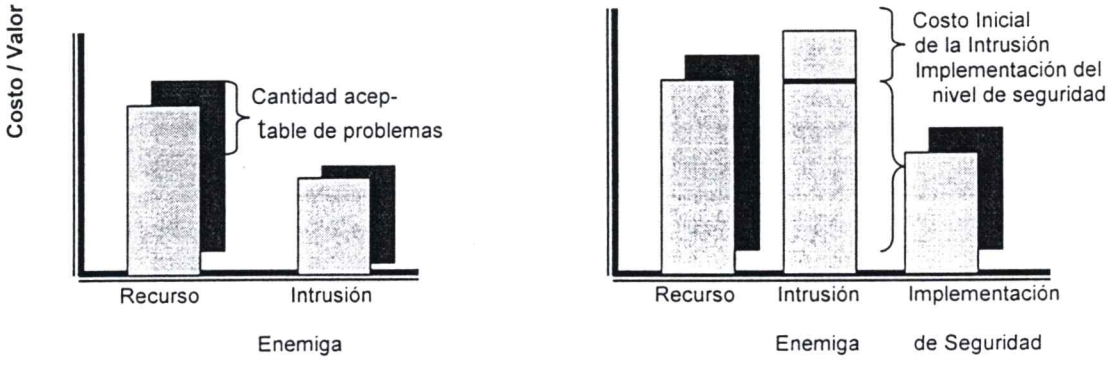


Fig. 5.3 Cobertura de Seguridad

8. MANEJO DE LOS RIESGOS

Hay cinco medidas principales que se deben considerar para lograr un manejo efectivo de los procesos para prevenir los riesgos: identificación, clasificación, planeamiento, seguimiento y ejecución. A menudo la madurez de la capacidad de la empresa para enfrentar el manejo de los riesgos es función de su habilidad para invocar estas medidas.

La ***Identificación de los riesgos*** y la fuente de los mismos se lleva a cabo creando un conjunto de información sobre riesgos. La actividad se realiza, comúnmente, solicitando información a través de sesiones de preguntas y respuestas. Los administradores de comercio electrónico son alentados a realizar preguntas tales como: ¿hay algún problema ó riesgo?, ¿qué incertidumbre rodea a este problema?, ¿cuáles son las suposiciones?. Para este proceso es importante asegurarse que el riesgo se discuta inteligentemente y con detenimiento. Los riesgos deben distinguirse de las oportunidades, emisiones y problemas. La causa del riesgo debe ser explícita en términos de su incertidumbre en el tiempo, control ó información.

Los métodos tradicionales en la determinación de los riesgos siguen aplicando, y deberían conducirse dentro del contexto de este marco. Métodos tales como la determinación del riesgo basada en su exposición, solapando una taxonomía de problemas conocidos al entorno a ser analizado, descubriendo áreas potenciales de posibles ataques por enemigos, pueden fija límites al análisis del riesgo a cantidades conocidas y permite una rápida clasificación de los riesgos. La determinación cuantitativa del riesgo, que emplea un enfoque teórico, incluyendo métodos matemáticos, permite identificar y clasificar los riesgos.

La ***clasificación de los riesgos*** es un proceso de normalización para conocer las cantidades. La normalización reduce el nivel de vaguedad entre todo lo concerniente con el manejo apropiado del riesgo. Los riesgos deben definirse en términos de:

- *Impacto.* La naturaleza (costo, planificación, satisfacción del cliente, etc.) y magnitud de las consecuencias del riesgo.

- *Probabilidad.* La probabilidad de la consecuencia de un riesgo se comprenderá si el diseño actual se va a llevar a cabo (proactiva) ó se continuará con la situación actual (reaccionable).

- *Tiempo del marco.* El tiempo durante el cual el equipo puede ejercitar alternativas proactivas asociadas con un riesgo. Después de este punto, las alternativas serán eliminadas porqué será demasiado tarde para hacerlas.

- *Acoplamiento.* El efecto de la ocurrencia de un riesgo acarrearía riesgos y oportunidades. Cuando el riesgo se vuelve un problema, puede incrementar la probabilidad de otros riesgos, incrementando su efecto, limitando las op-

ciones de repartirse entre ellos, ó reduce el tiempo del marco para hacer opciones sobre ellas.

- *Incertidumbre*. Falta de entendimiento sobre la naturaleza de la probabilidad de un riesgo ó de cómo puede variar con el tiempo.

Los administradores que emplean estos términos tendrán mayor éxito en entender la naturaleza del riesgo y por ello probar medidas efectivas de prevención.

Planificar es el proceso por medio del cual se conciben las estrategias para tratar con los riegos. La clasificación de los riesgos no debe ignorarse: se deben establecer pasos consistentes deben delinearse para contribuir a la definición global de riesgo para el sistema de comercio electrónico. Los administradores deberían considerar las siguientes cuatro estrategias de riesgo:

- *Moderar*. Reduce la probabilidad y/o el impacto del riesgo a través de la mejora del sistema.

- *Evitar*. Elimina la posibilidad de un riesgo específico, eligiendo un camino alternativo. A menudo esto significa cambiar un riesgo por otros que son más aceptables ó fáciles de tratar con ellos.

- *Transferir*. Dele la oportunidad a alguien más de compartir ó asumir la consecuencia del riesgo. Un seguro es una forma de transferir el riesgo.

- *Aceptar*. Planee una contingencia, Rastree el riesgo y promulgue el plan si este se vuelve un problema. Los administradores deberían ver estas tareas de estrategias como items a ejecutarse.

Seguimiento proporciona a los administradores, un método efectivo para garantizar que están actuando las estrategias contra los riesgos. Adicionalmente, pueden llevar a cabo revisiones precisas y efectivas, mediante el seguimiento, como una forma de establecer la previsión y exactitud en sus procesos de manejo de riesgos.

Ejecución es la ejecución de planes estratégicos administrados por los mecanismos de seguimiento. Los administradores, auditores, colaboradores ó aquellos que contribuyen actualmente con dinero deben adoptar este marco como forma de entender los riesgos asociados con los proyectos de comercio electrónico, el valor de lo que se puede perder y el costo de las decisiones y soluciones.

9. CAPAS DE PROTECCIÓN DE RIESGOS

Hay varias razones para implementar seguridad en capas antes que en un solo nivel. Las dos más importantes son efectividad y precio. Ningún software ó dispositivo de hardware es perfecto, por lo que sería simple depender de sólo un único software ó hardware que fuera la única protección de la instalación. Por medio capas de soluciones, un error en una de ellas puede no tener consecuencias debido a que otras capas soportan protección contra ese problema. Las soluciones simples tienden a ser menos costosas que las complejas, lo cual constituye otro beneficio para considerar el enfoque de capas.

Por ejemplo, una máquina puede ser segura instalando medidas de seguridad que abarquen todo ó sea que maneja la autenticación, detección de la vulnerabilidad, monitoree el intento de forzar la entrada al sistema y la protección de la red. Alternativamente, un firewall puede proporcionar protección para todas las máquinas de la red y cada una de ellas, se asegura por medio de instalaciones individuales, por el retiro de facilidades innecesarias y por paquetes que monitorean el intento de ingreso no autorizado. La mejor solución de una instalación dependerá de las necesidades de seguridad, la experiencia del personal y la evaluación de los riesgos.

10. LIMITES

Es importante determinar el perímetro de la seguridad, pero generalmente esto no es suficiente. Saber que un firewall está en su lugar frecuentemente es una señal psicológica que la seguridad interna está disminuyendo o algunas veces es ignorada completamente. Es necesario un conocimiento completo de la vulnerabilidad de tal instalación, para responder a este sentimiento de estar bien. Los perímetros son controles extensos de seguridad que controlan el tráfico entre interacciones de operaciones entre regiones independientes. La premisa es que existen individuos ó sistemas distinguibles (redes, computadoras, etc.) que pueden agruparse basándose en niveles variables de confianza.

Los perímetros pueden limitarse en dos regiones separadas, como externo e interno, ó se pueden crear modelos más sofisticados que incluyan perímetros dentro de perímetros. El grado en el cual uno crearía nuevos perímetros, es totalmente, una función del análisis de un riesgo y de los beneficios derivados relativos al valor del recurso. Por ejemplo, un perímetro obvio sería separar la Intranet corporativa de Internet. Además, una empresa puede elegir establecer parámetros adicionales dentro de su intranet para proteger los sistemas de información de recursos humanos de las fuentes de información general de la empresa (por ej. sitios Web de la intranet).

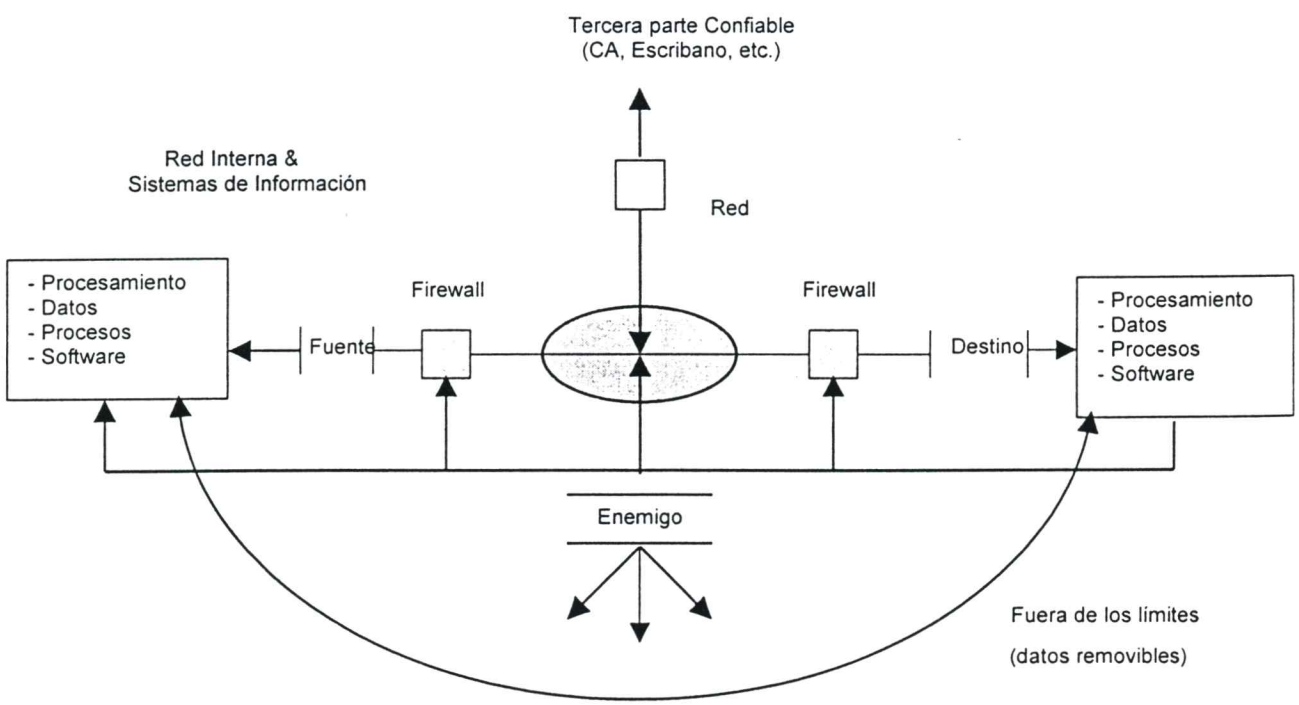
El primer paso para establecer un perímetro es entender que es lo que requiere protección. La figura 5.2 (*Ver pag.50*), retrata los problemas de la información en tránsito. La figura 5.4 muestra los flujos de información que representan puntos potenciales de acceso dentro de los sistemas internos de información de la fuente y el destino. Esta figura, un mo-

delo generalizado, pone de manifiesto detalles del origen y el destino, que deben considerarse en el modelo de perímetro.

El resultado es la necesidad de un modelo de perímetro tanto para la información de la red como para la seguridad de acceso. Las áreas importantes de interés incluyen los puntos de acceso a la red (facilidades de sintonización pública y privada), así como flujos de información alternativos que no caen dentro del dominio técnico. Un ejemplo de comercio electrónico, es una compra con tarjeta de crédito desde el sitio Web: como viaja y se protege la información y como el comerciante puede asegurar al cliente que es seguro comprar en su tienda en línea. La figura 5.4 debe considerarse el mapa que pone de relieve los puntos más importantes que requieren protección en un sistema típico de comercio electrónico.

Los firewalls son dispositivos efectivos para establecer las soluciones de perímetros en el comercio electrónico, ó sea cuales son los límites entre redes; establecen perímetros construyendo barreras entre dos ó más redes conectadas con la intención de crear una red privada y una externa (pública u otra privada); intentan controlar todo el tráfico que circula para permitir que sólo pase el que es autorizado y resistir cualquier forma de penetración. Los tipos comunes de firewalls que existen incluyen filtrado de paquetes de la capa de red, gateways (vías de acceso) para la capa de aplicación y para la capa de circuito; todas estas formas son importantes en el contexto del comercio electrónico y, raramente, ninguna de ellas es omitida en una implementación. Los firewalls no son impermeables a la transferencia de virus u otros tipos de archivos volátiles y además no pueden prevenir la intromisión de las personas con conocimientos para ello; son gateways (vías de acceso) entre redes y por consiguiente no agregan valor dentro del contenido de la red.

Fig. 5.4 Posibles puntos de ataque / compromiso



Cuando los firewalls se combinan con routers (ruteadores) protectores, se pueden crear configuraciones sofisticadas con capas variables de seguridad. Una de tales configuraciones no sólo establece regiones internas y externas, sino también una región intermedia entre ambas; esta área se conoce a menudo como zona "desmilitarizada" (DMZ). Los administradores de soluciones de comercio electrónico que utilizan los servicios de sitios Web, que se relacionan con los datos de la empresa, son remisos a no establecer una zona DMZ.

Una zona DMZ se puede pensar como una estructura de red, que a través de configuraciones y políticas, establecen regiones de seguridad (desde niveles bajos hasta altos) donde los dispositivos de red pueden conectarse físicamente. Una zona DMZ típica se divide en tres zonas: roja, amarilla y verde (Figura 5.5). La roja es la zona más riesgosa, estaría en el dominio público donde, tal vez, puede localizarse un router (ruteador) de la empresa. La zona amarilla alojaría los servicios, tales como la Web de la empresa y los sitios FTP y finalmente la zona verde sería la intranet de la empresa más firmemente controlada.

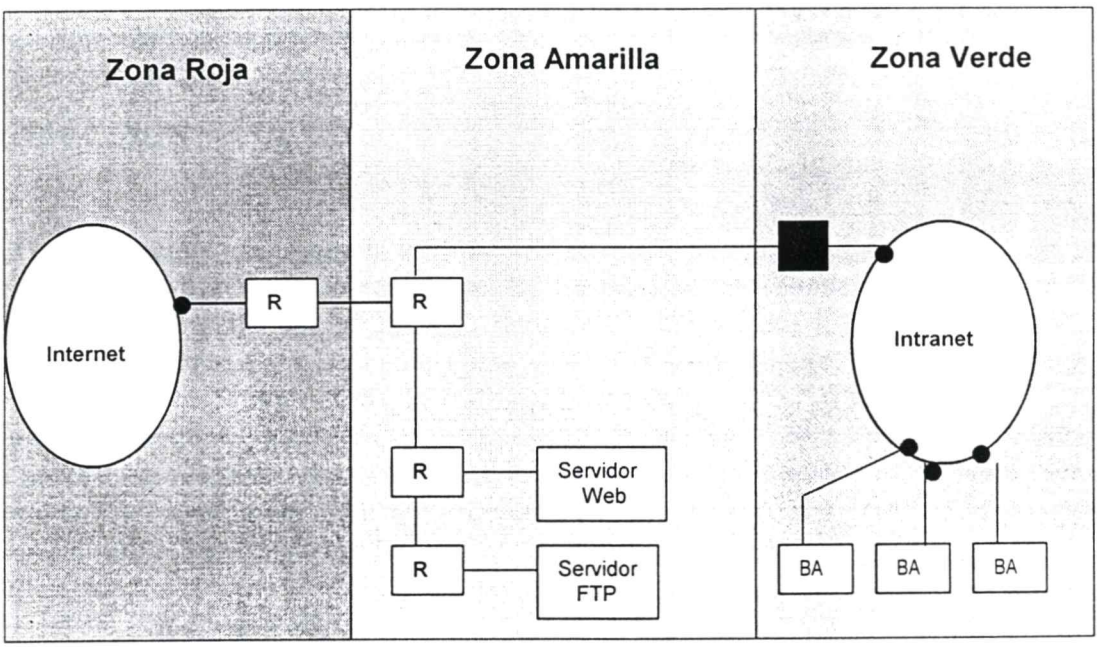


Fig. 5.5 Modelo de Seguridad DMZ

R Router de la Red

BA Datos de la Empresa / Sistemas Legales

Firewall

CAPITULO 6
AUTENTICACIÓN DE USUARIOS

1. INTRODUCCION

La autenticación valida que la información se recibe de una fuente deseada ó que se otorga a un destino correcto. Adicionalmente, las firmas digitales (conocidas también como certificados digitales) extienden el proceso de autentificación para incluir el no repudio (prueba irrefutable) tanto para la fuente como para el destino. El nivel de seguridad que ofrece la autenticación, proporciona medidas preventivas para las siguientes amenazas: husmeo, enmascaramiento, modificación y algunas medidas de protección para la penetración. Un proceso se reconoce como autenticado si requiere algo que se conoce tanto como "compuesto de" ó "poseído de". Un ejemplo diario es cuando un comerciante minorista nos pregunta por nuestra licencia para autenticar nuestro pago con cheque.

La forma más simple de autenticación se basa en el uso de una contraseña (passwords). El acceso a los datos o a los sistemas puede otorgarse a aquellos que poseen una identificación reconocible y una contraseña asociada y las mismas, no proporcionan ningún valor adicional más allá de una autentificación básica, son fácilmente blancos de enemigos y actúan como un nivel básico de seguridad.

Una forma más sofisticada de autenticación se basa en la posesión por ejemplo de un algoritmo encriptado con una clave única o token. El nivel de confianza de un proceso de autenticación se refuerza por medio del uso de dispositivos únicos administrados de manera centralizada. Además, dependiendo del dispositivo utilizado, puede incrementarse el valor agregado de la confidencialidad e integridad de los datos.

Los "tokens" son dispositivos físicos a los que se les agrega una clave simétrica compartida y un algoritmo. El proceso de autenticación de los tokens es incorruptible y comienza con la autenticación del usuario en el sistema con una identificación junto con un número generado por el token (utilizando la clave simétrica compartida). El sistema calcula un número con la identificación del origen y una clave asimétrica compartida y luego lo compara con el número que generó el origen. Si los valores son los mismos, el usuario es autenticado. Muchas empresas utilizan tarjetas de seguridad para este propósito; la tarjeta contiene información que se procesa antes de que se permita el ingreso.

Un desarrollo importante del trabajo de la criptografía asimétrica es la firma digital. No es una firma real, sino un conjunto de dígitos binarios, que sirven para el mismo propósito y que es más difícil de falsificar. Ellos asocian a un mensaje con una única fuente, que puede ser un dispositivo ó una persona, dependiendo de la función del comercio electrónico. Las firmas digitales proporcionan un conjunto único de características de seguridad que son diferentes de cualquier otra implementación; incluyen confidencialidad, integridad de los datos y no repudio. El no repudio significa que el destinatario tiene confianza en la legitimidad de la clave pública del remitente. La autenticación con el uso de las firmas digitales se lleva a cabo mediante el intercambio de mensajes encriptados con la clave privada del remitente y desencriptados por el destinatario utilizando la clave pública complementaria del remitente. La autenticación sucede si el mensaje logra ser desencriptado con éxito.

Una aplicación importante de este modelo es la aplicación de protocolos mutuos de autenticación. El protocolo mutuo de autenticación permite a las partes autenticarse mutuamente y hacer intercambios en la sesión de clave simétrica. Este tipo de sesión, extiende el nivel de confianza en el sistema de seguridad limitando la utilización de la clave sólo a la sesión actual.

Las firmas digitales solamente son efectivas si existe una relación de confianza entre el remitente y el destinatario; son costosas de desarrollar e implementar y por eso no son prácticas para una única sesión ó para interacciones ocasionales. Esto significa que este enfoque de seguridad anda bien para pequeñas interacciones de bolsillo entre el remitente y destinatario, pero no sucede lo mismo con grandes grupos y relaciones que carecen de la confianza necesaria. Una aplicación típica sería, por ejemplo, el intercambio de correo electrónico entre dos partes confiables.

2. ESTRUCTURA DE CLAVE PUBLICA

Un modelo de confianza que se encuentre en todas partes es necesario para el uso más extendido de las firmas digitales y ello se logra por medio de las autoridades certificantes que son firmas escrituradas en línea. Una tecnología extendida de clave pública para fines de seguridad necesita una infraestructura para administrar firmemente claves públicas para usua-

rios ó sistemas distribuidos de manera amplia. El estándard X.509 de la ***IETF***, constituye una base ampliamente aceptada para tal tipo de infraestructura, definiendo formatos de datos y procedimientos relativos a la distribución de claves públicas vía certificados digitales firmados por las autoridades certificantes. Un certificado se puede pensar como un pasaporte electrónico conteniendo información estandarizada para una apropiada identificación de una persona, sistema ó software.

El contenido de un certificado incluye: nombre, empresa, dirección, autoridad emisora (autoridad certificante) de la firma digital e información de identificación, clave pública de la persona que emitirá el certificado digital, fechas de validez del certificado, tipo de certificado (las subdivisiones posteriores se basan en privilegios) y número de identificación del certificado digital.

La autoridad certificante es una tercera parte, confiable en sus habilidades para registrar, certificar, emitir y revocar certificados digitales en nombre del público en general o de una comunidad con intereses comunes. La cuestión de si una autoridad certificante puede proporcionar el nivel de seguridad necesario para las soluciones de comercio electrónico depende de su capacidad y credibilidad para operar, medida con relación a los estándares de la institución que requiere el servicio.

El análisis de las autoridades certificantes tiende a enfocarse en la comunidad y pertinencia, identificación y autenticación, manejo de claves seguridad local, seguridad técnica y políticas operativas. Los bancos y las organizaciones legales son candidatas obvias para autoridades certificantes, pero pueden tener un conflicto de intereses, en sus roles en el comercio electrónico.

Las autoridades deben ser altamente confiables para jugar un rol central en relaciones confiables. El desarrollo de la infraestructura de clave pública no es una tarea sencilla; los servicios de PKI han evolucionado a través del modelo de outsourcing (tercerización de servicios) y provee de forma correcta a los negocios de tamaño pequeño y medio que no pueden darse el lujo de establecer una infraestructura de clave pública. Sin embargo, las grandes empresas tales como bancos gubernamentales, necesitarán determinar si actuarán ó no como autoridades certificantes por sí mismas o tercerizarán como en el caso de IBM, Equifax o VeriSign.

La confianza en la industria con PKI es muy alta; estas tecnologías están desarrollándose en una proporción importantísima y se espera que sigan creciendo. Por ejemplo la mayoría, sino todos los Web browsers y sistemas de correo electrónico, soportan certificados digitales e incluso tienen muchas de las más importantes infraestructuras de clave pública para certificados digitales (VeriSign, Microsoft, GTE CyberTrust, KeyWitness y otras) enviados con el producto.

3. OTRAS TÉCNICAS DE AUTENTICACIÓN

El intercambio de la información requiere, para las operaciones, la mayor de las seguridades y la forma más eficiente de autenticación de usuario es aquella que incluye características fisiológicas (huellas digitales, huellas de la mano y scaneo de retina) o de conducta (patrones vocales, firma y patrones de pulsación de tecla). La precisión de estos mecanismos de autenticación es muy alta y, aunque usualmente no se usan, se observa una tendencia hacia las mismas. Tales técnicas son comunes en el ámbito gubernamental, principalmente en el departamento de defensa comprometido con información altamente secreta relacionada con la seguridad nacional.

A medida que el uso de tales tecnologías de autenticación se vuelve más corrientes, las mismas, a menudo se oponen a las leyes, practicas ó aprobación de los clientes, en áreas tales como privacidad, discriminación y derechos civiles. Otra vez aquí existe un intercambio entre riesgo comercial y costo social.

4. CONTROL DE ACCESO Y AUTORIZACION

El florecimiento del comercio electrónico sobre redes públicas introdujo controles de acceso interesantes y autorizaciones complejas. El control de acceso está relacionado con el manejo de la capacidad ó derecho de una parte a entrar ó acceder a una zona ó servicio, mientras que la autorización otorga permiso ó poder a funciones ó servicios dentro de una zona determinada de acceso. Para el éxito de cualquier servicio que intenta lograr influencia sobre redes públicas, es importante que el mismo tenga un control de acceso adecuado.

Los elementos básicos de una política de control de acceso incluyen un objeto (sistema, programa, base de datos, etc.), un sujeto (entidades externas que acceden a los objetos) y derechos de acceso (la forma en que los sujetos acceden a los objetos). Estos tres elementos se organizan casi siempre en forma de matrices de acceso, listas de control y listas de capacidades y constituyen la base para una administración de control de acceso efectivo. Es importante esmerarse cuando se construyen estos dispositivos, dado que los mismos deben aguantar las violaciones de los enemigos.

La matriz de acceso es una representación conjunta del control de acceso y de la lista de capacidades. La matriz se pude descomponer en distintas listas de control de acceso (*ACL*). Para cada objeto, hay una *ACL* con una lista de sujetos que tienen derechos de accesos permitidos. La matriz se descompone además en distintas listas de capacidades. Para cada sujeto, hay una lista de capacidades con una lista una lista de objetos y operaciones autorizadas.

Mientras que las políticas de control de acceso son cruciales en cualquier esquema fuerte de autenticación, es en la aplicación de las mismas donde se esfuma el éxito. Las aplicaciones tradicionales de control de acceso tienen que ser y continúan siendo administradas principalmente por aplicaciones sencillas de negocios, cada una con sus propias versiones de funciones ***ACL***. Una empresa ante cuatro aplicaciones de negocios y un sistema operativo de redes, puede esperar que su personal tenga como mucho cinco únicas identificaciones de usuarios y contraseñas.

El comercio electrónico incrementa el problema proporcionando un acceso amplio a muchas aplicaciones. La figura 6.1 muestra una estructura genérica de control de acceso.

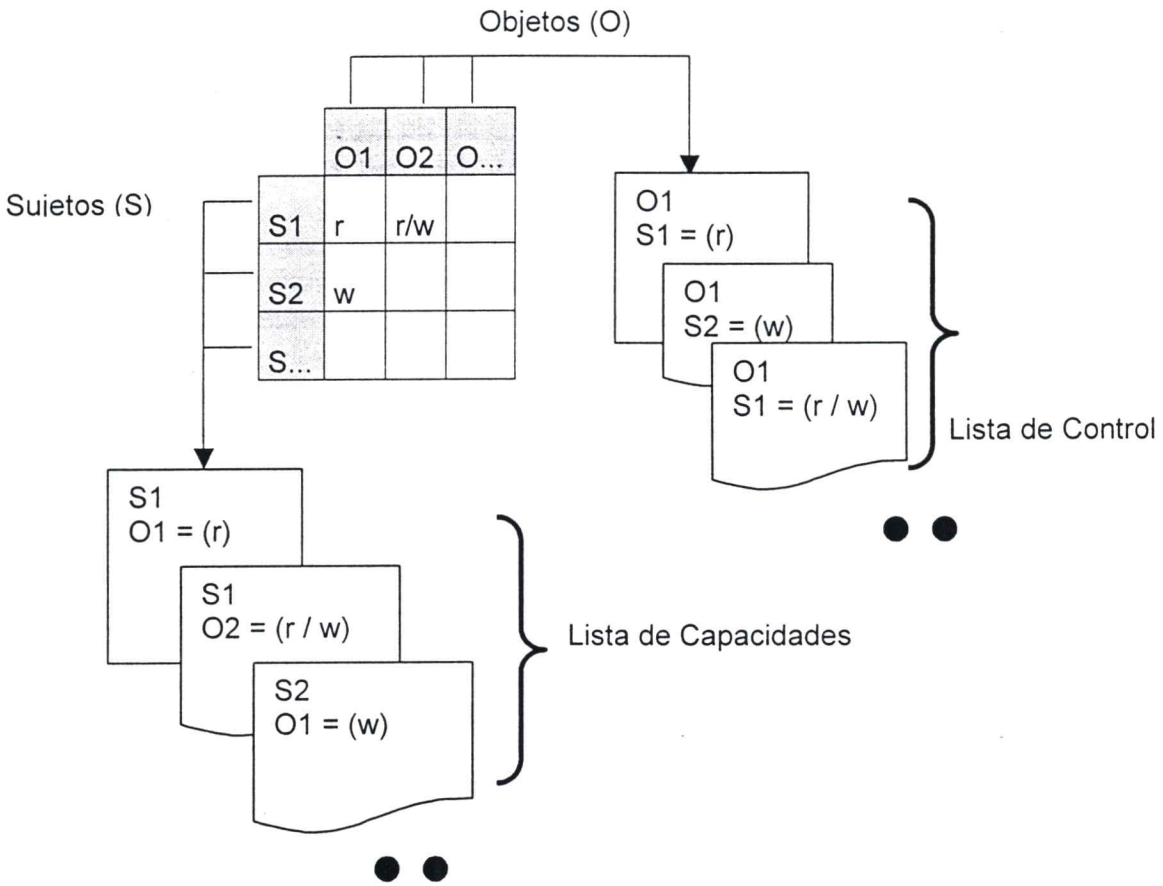


Fig. 6.1 Composición e interrelaciones de elementos de control de acceso

Los servicios de directorios, principalmente base de datos X.500, junto con el protocolo de autenticación ***LDAP*** (Ligth Weight Directory Acces Protocol), fueron la base para un mecanismo de autenticación centralizado. El protocolo ***LDAP*** se basó originalmente en el ***DAP*** (Directory Access Protocol), protocolo de acceso a directorio, que soportaba un conjunto extenso de funcionalidades, mientras que ***LDAP*** soporta sólo autenticación (tanto tex-

to plano y ***Kerberos***), permitiendo el acceso de usuarios autenticados a información delicada, a través de los directorios de la empresa. ***LDAP*** proporciona acceso seguro a contraseñas en un directorio / depósito central. Este depósito puede ser usado luego por aplicaciones independientes de las empresas como una forma de autentificación de usuario.

El protocolo ***LDAP*** fue diseñado inicialmente por proveedores de redes de Internet y es muy fácil de implementar. Hoy en día, la mayoría de las aplicaciones de negocios ofrecen la posibilidad de utilizar un mecanismo externo de control de acceso, dejando de lado el protocolo ***LDAP***. Algunos fabricantes proporcionan a los usuarios de ***LDAP i***nterfaces sobre sus directorios en un intento de obligarlos a establecer una dependencia con sus productos. Esto puede ser un enfoque viable para algunas empresas; sin embargo, estos directorios no ofrecen la flexibilidad y rendimiento necesario para las aplicaciones de comercio electrónico. Además, los sistemas operativos de redes no están diseñados completamente para control de acceso y tienden a ser no tan seguros como las soluciones especializadas.

El protocolo ***Kerberos***, extiende el modelo de autenticación ***LDAP*** proporcionando privilegios de control de acceso a aplicaciones de sistemas, ofreciendo uno de los más altos niveles de control de acceso de usuario y sistema disponible hoy en día. ***Kerberos*** utiliza el cifrado de clave secreta para autenticación y encriptación y se está convirtiendo en el estándar de facto para la autenticación remota en un entorno cliente / servidor. El diseño cliente / servidor de ***Kerberos***, centraliza el proceso de autenticación para múltiples sistemas de una manera segura, una propiedad importante en los entornos de redes

Kerberos proporciona el servicio ***SSO*** (Single-Sign-On, única identificación): la posibilidad de acceder múltiples sistemas computacionales ó redes después de logonearse una única vez con una identificación de usuario individual y una contraseña. Esta forma de setearse resuelve la situación general donde las claves e identificaciones de usuarios separadas son necesarias para cada aplicación. El servicio ***SSO*** tiene tres ventajas importantes para las empresas:

- Es útil para el usuario
- Es útil para el administrador
- Mejora la seguridad

Los beneficios del ***SSO*** se han demostrado ampliamente. Teniendo sólo una única identificación por usuario en vez de, por ejemplo diez, la administración resulta más fácil ya que también elimina la posibilidad de que los usuarios escriban en papel sus diez claves para recordarlas y de esta manera comprometan la seguridad. Finalmente, ***SSO*** mejora la productividad reduciendo la cantidad de tiempo que utilizan los usuarios para obtener acceso a un sistema.

5. CAPAS DE TRANSFORMACIÓN DE LA INFORMACIÓN Y ESQUEMAS DE SEGURIDAD ASOCIADOS

La información que viaja por la red debe atravesar distintas capas: La capa de aplicación, la de transporte y la de red. Estas capas no sólo ofrecen flexibilidad en el manejo de los mensajes en las redes sino que introducen áreas donde la seguridad está comprometida. Como resultado de esto, se diseñaron e implementaron varios mecanismos de seguridad para cada una de las capas dado que las mismas son distintas y necesitan conjuntos de habilidades diferentes.

Los administradores de comercio electrónico deben considerarlas como una prioridad, lo que implica que su hardware, redes y comunicaciones y especialistas de aplicaciones las manejen en todos los niveles de la fase de diseño de la solución. Descuidar este aspecto puede llevar a comprometer la efectividad del análisis y manejo del riesgo.

La figura 6.2 es una muestra de las capas mencionadas y sus implementaciones de seguridad relacionadas (las áreas sombreadas representan implementaciones de seguridad).

Podría llegar a imaginarse la combinación de las capas de red, transporte y aplicación para una mejor seguridad. Tal tipo de implementación debe examinarse cuidadosamente para no agregar complejidad y costo a una solución que poco deparará a la seguridad.

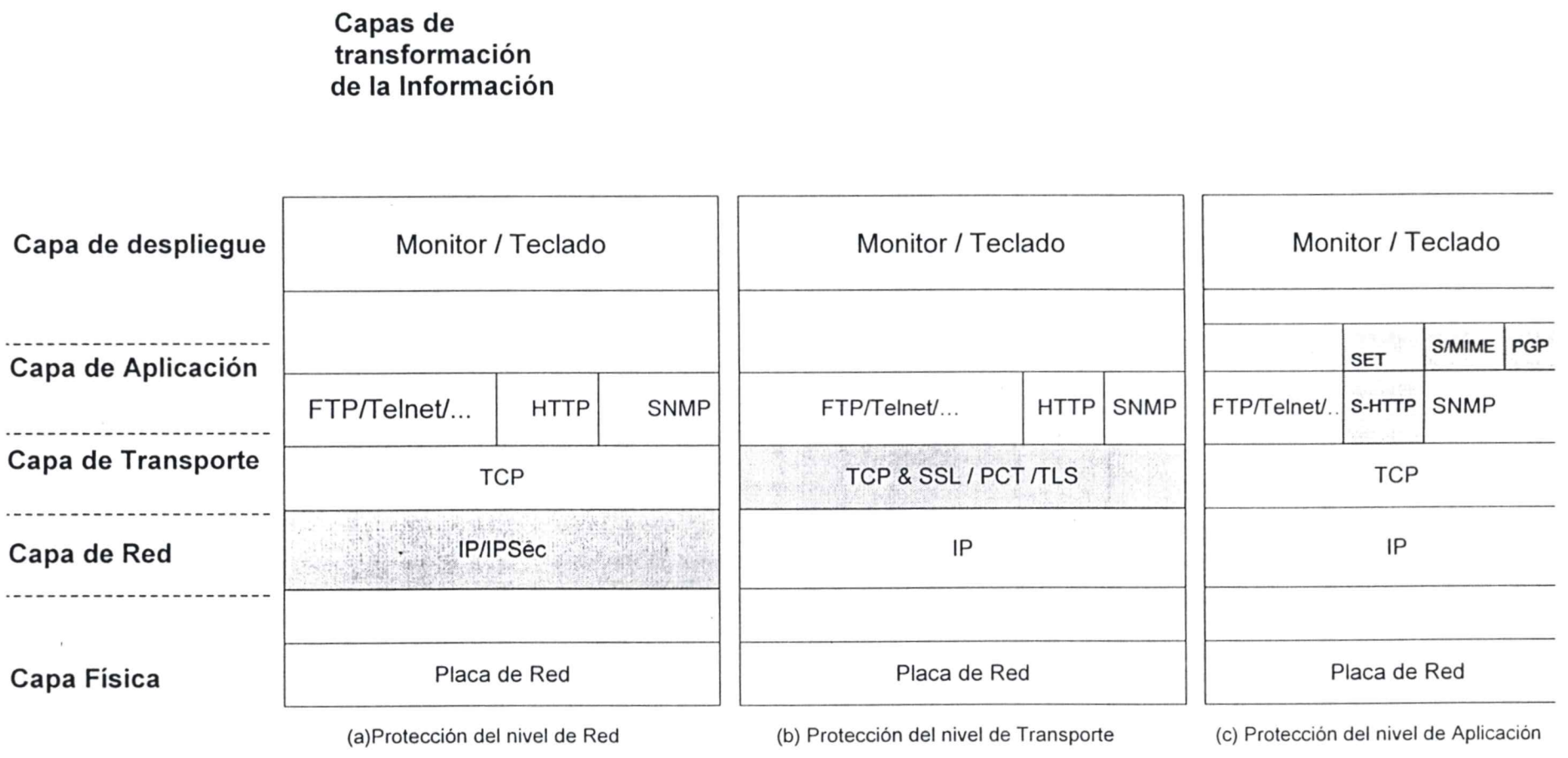


Fig. 6.2 Capas de transformación de la información en el comercio electrónico y técnicas de seguridad asociada

Capa de red (Fig. 6.2a). La protección de la misma atraviesa todas las capas y ofrece métodos no invasivos para el intercambio seguro de información. El protocolo de Internet IP es el responsable del manejo de los paquetes de información en nombre de aplicaciones de alto nivel siendo además una de los medios más populares de manejo de paquetes y tiene gran importancia en el contexto del comercio electrónico; es no sólo el núcleo de las comunicaciones de datos para el comercio electrónico sino que también lo es para los servicios conocidos como voz sobre IP.

Por sí mismo el protocolo IP, no garantiza la entrega, integridad ó el origen de los paquetes de información, estas funciones son manejadas generalmente por aplicaciones de alto nivel. Al aplicar seguridad en el nivel IP se pueden tener redes seguras no sólo para aplicaciones que tienen mecanismos de seguridad sino también para aquellas aplicaciones que ignoran a la seguridad. La seguridad del protocolo IP utiliza la tecnología de claves simétrica y asimétrica para facilitar las funciones de autenticación, confidencialidad e integridad. Una aplicación común de seguridad IP sería obtener redes virtuales privadas seguras (***SVPNs***).

La seguridad de la capa de red generalmente es rápida, costosa y rígida; necesita tecnología especializada asociada para su configuración y utilización y es una medida excelente para establecer comunicaciones seguras entre partes confiables, sobre redes públicas para soluciones de comercio electrónico.

Capa de Transporte (Fig. 6.2b). Al igual que la capa de red, la seguridad de esta capa atraviesa todas las otras capas; la capa de red maneja información en forma de paquetes, mientras que la capa de transporte lo hace basándose en sesiones. La protección para esta capa se implementa por medio de ***SSL*** (Secure Socket Layer); una sesión ***SSL***, se define como la asociación segura entre un cliente y un servidor (entre los puntos sobre una red).

SSL, proporciona *autenticación* (normalmente sólo para el servidor) a través de certificados digitales, *confidencialidad*, mediante la utilización de sesiones de claves simétricas, como así también *integridad* y *no repudio* por medio de firmas digitales. También ayuda a evitar negociaciones costosas para nuevas sesiones seguras para cada aplicación, permitiendo múltiples conexiones por sesión. Soluciones que pueden compararse con ***SSL*** son las Tecnologías de Comunicaciones Privadas (***PCT***, Private Communications Technology), la entrada de Microsoft en la pelea por la seguridad y el ***TLS*** (Transport Layer Security), un estándard de la ***IETF*** (Internet Engineering Task Force).

PCT y ***TLS*** son virtualmente copias de ***SSL***, con muy pocas diferencias; dado que se desarrollaron mucho más tarde que ***SSL*** y éste último es ampliamente reconocido y utilizado en la comunidad de negocios, es muy difícil que cualquiera de los otros logre mucha aceptación y uso. La utilización de ***SSL***, es realmente un método efectivo y de mucha penetración en las soluciones de comercio electrónico, para afianzar la seguridad de sesiones basadas en la Web.

Capa de aplicación (Fig. 6.2c). La seguridad de esta capa es simplemente la incrustación de seguridad dentro de aplicaciones comerciales ó programas. A diferencia de las capas de red y transporte, los mecanismos de seguridad de esta capa no pueden compartirse entre aplicaciones; cada aplicación maneja su seguridad de manera independiente de las otras, algunas veces reproduciéndose como funciones. Las implementaciones de seguridad en la capa de aplicación se puede comparar, en funcionalidad, con implementaciones de otras capas. Además, no están agobiadas por el progreso de estándares y son libres de explorar nuevas aplicaciones innovadoras de criptografía.

Un ejemplo de esto es ***SET***. El protocolo ***SSL*** no podría ofrecer la funcionalidad necesaria para las operaciones seguras de tarjetas de crédito sobre Internet, por eso se emprendió una implementación a nivel aplicación para facilitar soluciones rápidas. Con toda probabilidad, ***SET***, cambiará desde la capa de aplicación a la capa de transporte y se transformará en un servicio genérico para otras aplicaciones.

Algunas otras aplicaciones importantes son Secure Mime (***S/Mime***) y Pretty Good Privacy (***PGP***); es importante destacar que ***S/Mime*** con el uso de certificados digitales emitidos por una autoridad certificante confiable, jugará un rol importante en el comercio electrónico comercial, mientras que ***PGP*** (y tecnologías parecidas), jugará un papel importante con interacciones no comerciales (correo electrónico personal).

6. ASPECTOS SOCIALES DE LA SEGURIDAD

Las medidas de información segura se diseñan para evitar que personas y sistemas no autorizados, permitan afectar, ver, acceder ó permitir el acceso a los sistemas o datos de una empresa. Desdichadamente, la actitud nociva de los adversarios no se limita a infiltraciones técnicas. Además, el comercio electrónico tiene una tendencia a amplificar estos problemas sociales.

7. INGENIERIA SOCIAL

El término de ingeniería social se aplica a los intrusos que extraen información confidencial de seguridad (identificaciones de empleados, contraseñas, códigos de entrada, etc.) a través de interacciones sociales. Las empresas con estructuras sociales complejas se enfrentan al desafío de contar con personal que no está completamente consciente con las políticas y las pautas de seguridad IT. Los intrusos, por medio de métodos casuales, aparentemente en forma aleatoria antes que en una forma predecible, ponen en peligro las debilida-

des, a través de ataques planificados, del personal no preparado convenientemente. Estos ataques pueden variar desde llamadas telefónicas aleatorias inquiriendo al personal sobre sus identificaciones de usuarios y contraseñas hasta intrusos que se hacen pasar como guardias de seguridad ó de limpieza para obtener el acceso a las áreas seguras.

Aunque las tácticas de ingeniería social no siguen ningún método, se pueden definir algunos enfoques generales. En el ámbito del comercio electrónico, los ataques son generalmente misiones de reconocimiento, que localizan con precisión recursos generalmente disponibles como por ejemplo base de datos de Internet, directorios de teléfonos y publicaciones de las empresas. Los intrusos, mediante la recolección y combinación de información, construyen una visión amplia de la empresa que incluye la estructura de la misma, los nombres del personal senior (incluyendo su dirección y número de teléfono), los proyectos claves y cualquier otra información relacionada. Una vez que tiene información suficiente, el intruso puede "fabricar" una persona ó asumir la identidad de uno ó varios de los miembros influyentes del personal.

Mediante interacciones básicas con el personal interno, se crea confianza, autoridad (soborno y confabulación) ó intimidación sobre las relaciones de los mismos y todas estas acciones pueden llevarse a cabo personalmente, por teléfono ó por correo electrónico. En este punto, el intruso intenta simplemente obtener información crítica que le pueda permitir penetrar el sistema de información de la empresa; algunos lugares comunes de ataques pueden ser: los mailrooms (una buena fuente de números importantes e identificaciones de usuarios de los empleados), soporte de red (solicitando el restablecimiento de claves olvidadas) y recepcionistas y secretarias (personal clave para el manejo de los números telefónicos).

Aunque estos ataques parecen complicados, los intrusos habilidosos logran el éxito en poco tiempo y sin esfuerzo. La clave del control más efectivo para prevenirse de la ingeniería social incluye el conocimiento de programas de seguridad, intensificación de los sistemas de seguridad y la realización de test de ingeniería social sobre intromisiones.

La información sobre ***programas de conocimiento sobre seguridad***, constituye un primer nivel efectivo de protección; la atención del personal interno debe dirigirse hacia los problemas relacionados con la seguridad y la influencia que los mismos pueden tener sobre ellos y la empresa. Como en cualquier programa eficaz de conocimiento, el personal debe conocer la política de seguridad y debe incorporar las políticas inculcadas durante las sesiones educativas.

Las soluciones de comercio electrónico también deben extender el programa a sus clientes; en algunos casos los conocimientos sobre seguridad están incrustados en la tecnología, los certificados digitales son un ejemplo de tales prácticas que incluyen informes de políticas y prácticas en forma muy estándar.

La ***intensificación de los sistemas de seguridad*** son mecanismos importantes para impedir la repetición de ataques frustrados dado que sin tales mecanismos, los intrusos de-

tectados pueden proceder ó escapar, sabiendo que el personal no tiene forma de modificar la infracción a la seguridad; además, las áreas dentro de la empresa con sistemas débiles de intensificación de la seguridad, representan el blanco predilecto para los intrusos. Los consumidores de sistemas de comercio electrónico también necesitan un canal de intensificación. Un servicio comparable con todo lo antedicho serían aquellos centros de seguridad de atención en línea, de las tarjetas de crédito.

Los ***tests de ingeniería social sobre intromisiones*** son efectivos para examinar las políticas instrumentadas de seguridad. El proceso se puede instrumentar como guía para la implementación de medidas preventivas; pueden establecer la capacidad y madurez de la empresa para frustar ataques futuros. Una vez que se establece una línea de acción, se pueden establecer nuevas políticas que concuerdan mejor con las características y dinámicas de la empresa. Se debe prestar especial atención a tales actividades, asegurando que mientras puedan usarse firmas con buena reputación, las políticas de la empresa pueden requerir la aprobación correspondiente por parte de los ejecutivos seniors. Además, dichos informes se deben proteger bajo cualquier costo, dado que revelarán las debilidades dentro de la estructura social de la empresa.

8. DATOS REMOVIBLES

El acceso a los datos no se puede ver más como una facilidad monolítica del centro de cómputos. Las laptops, la oficina en casa, el duplicado de base de datos (como por ejemplo Lotus Notes, donde se mantienen copias de bases de datos a través de la red, haciendo su acceso más rápido y fácil y difíciles de proteger), horarios flexibles, correo remoto, almacenes de datos (data warehouse), bases de conocimientos y el mayor culpable de todas ellas, el comercio electrónico, han creado un mundo de datos removibles. Aunque los beneficios asociados con lo anterior son de gran importancia, pueden socavarse fácilmente mediante accesos inapropiados a los datos distribuidos. Tales datos, si se consideran vitales para el éxito de la empresa deben manejarse de una forma que prevengan todas las amenazas potenciales.

Las medidas básicas tales como protección de virus, encriptación general (de sistemas y archivos) y copias de resguardo, demuestran que son mecanismos efectivos contra riesgos potenciales. Sin embargo, para que estos mecanismos sean efectivos se deben desarrollar y cumplir estrictamente políticas sencillas. El uso de una clave privada garantizada por la infraestructura de clave privada (***PKI***), es la única forma en que se pueden controlar los datos removibles. Todos los usuarios ó sistemas que manejan datos removibles, poseerían una clave pública y otra privada, junto con un certificado digital, con un agregado, la ***PKI*** no sólo mantendría una copia de la clave pública sino también de la clave privada. El diseño de este enfoque se utiliza para asegurar que la empresa (dueña de los datos) es capaz de recuperar los contenidos de los almacenamientos removibles (laptop o de otro tipo).

9. ASPECTOS LEGALES

Las operaciones comerciales sobre Internet, dominio del comercio electrónico, no tiene precedentes en la definición de obligaciones legales potenciales, riesgos y responsabilidades. Los problemas de horario, distancia y regulaciones regionales asociadas con formas tradicionales de comercio no se pueden aplicar al comercio electrónico. La ley comercial tradicional debe ampliarse para considerar las circunstancias únicas de llevar a cabo negocios vía comercio electrónico. Como directiva, las empresas que planean comprometerse con el comercio electrónico, deben considerar cuidadosamente los siguientes problemas legales claves: previsiones legales, restricciones legales, confiabilidad en los registros comerciales, transmisión de datos, protección de la propiedad intelectual y separación de la información privilegiada.

Las ***prevenciones legales***, están relacionadas con la interacción de los consumidores, se relacionan con el establecimiento de informes, términos y condiciones, compromisos, aceptaciones y advertencias. Dichas prevenciones son métodos breves y puestos de manifiesto en el momento de la comunicación entre las partes comprometidas en el comercio electrónico. Son mecanismos dinámicos (cuadros de diálogo, botones de confirmación, etc.) que se pueden insertar antes de llevar a cabo acciones que pueden significar un riesgo potencial u obligación.

Las ***restricciones legales*** son reglas y regulaciones que describen el comportamiento a seguir para operaciones comerciales nacionales e internacionales. Dado que el comercio electrónico se realiza en una sociedad sin fronteras, que no está bien protegida por controles legales bien establecidos, aquellas empresas que planeen comprometerse en una operación internacional, deben tener ó mantener copia de los antecedentes existentes para la conducta a seguir en los negocios internacionales.

La ***confiabilidad en los registros comerciales*** se refiere a cuales son los estándares adecuados para el mantenimiento de registros (impuestos, aduanas, etc.). Por lo tanto, las empresas con clientes en múltiples regiones, necesitarán adherir a los requerimientos legales de las mismas.

Los problemas de la ***transmisión de datos*** se deben negociar entre todas las partes que intervienen en una operación comercial. Debido a la naturaleza descentralizada de las redes y de Internet, las operaciones, llevadas a cabo a través de un transportador contratado, deben atravesar múltiples transportadores de telecomunicaciones lo que puede provocar un servicio ó flujo (regiones no deseadas) operativo menos que el deseable. Se debe poner especial cuidado en la selección del transportador de las telecomunicaciones prestando atención, especialmente, a sus subcontratistas y los arreglos establecidos con ellos.

La ***protección de la propiedad intelectual*** se refiere al mantenimiento de los derechos de propiedad de las empresas sobre sistemas y servicios que se ofrecen sobre Internet.

Los servicios de comercio electrónico, especialmente en la Web, son copiados fácilmente. Las empresas deben estar preparadas para aplicar sus derechos de propiedad intelectual en las distintas regiones.

El ***aislamiento de información privilegiada*** busca proteger la identidad y confidencialidad de la información asociada con las operaciones de comercio electrónico. Los servicios de comercio electrónico, por su naturaleza, acumulan inmensas cantidades de información las cuales representan un conjunto excelente para ser explotado (ya sea para bien o mal). Las empresas son responsables de contener dicha información y de responder por los riesgos asociados.

10. RETENER EXPERIENCIA

Se ha probado innumerables veces que la tecnología no puede reemplazar al conocimiento humano, el conocimiento es la incorporación de información en la mente de los seres humanos; el conocimiento mejora con el tiempo a través de la experiencia que incluye lo que se absorbe de cursos, de la lectura de libros y de la información que se obtiene de personas expertas que conocen con detenimiento un tema por qué lo han testeado y tienen experiencia.

La información sobre seguridad en el comercio electrónico es un proceso complejo que requiere experiencia y conocimiento para que tenga éxito en la protección de los recursos de la empresa mientras no comprometa su valor neto. Las empresas necesitan tener presente que la información relacionada con la implementación de la seguridad en el comercio electrónico se puede mantener por sistemas. No obstante, el conocimiento de la implementación de la seguridad sólo se puede mantener dentro de las mentes de aquellas personas involucradas (personal, vendedores, partes tercerizadas, etc.). El desafío para las empresas exitosas será como protegerán ó mantendrán el acceso al conocimiento de la información sobre seguridad.

Las recomendaciones para las empresas involucradas en el comercio electrónico son considerar lo siguiente:

- Seleccionar socios con habilidades demostradas.
- Construir relaciones estratégicas (incluyendo las relaciones legales)con socios especializados en configuraciones confidenciales de seguridad.
- Revalorizar las remuneraciones del personal basándose en las habilidades actuales requeridas en el mercado.

- Establecer un criterio de selección de personal basándose en encontrar los mejores expertos.

El comercio electrónico se encuentra en un momento crítico, después de un comienzo estimulante, los problemas de seguridad y confianza pueden resistir su constante crecimiento. La necesidad de seguridad está presente en todas las implementaciones de sistemas, sin embargo, debido a las complejas relaciones del comercio electrónico, los riesgos asociados son mucho mayores que en las implementaciones de sistemas tradicionales. Una parte importante del éxito de cualquier aplicación de comercio electrónico recae en la prioridad que se le da a la seguridad en la implementación y en la empresa.

Los nuevos controles a considerar, para satisfacer la integridad y confidencialidad del comercio electrónico, son los siguientes:

- Comunicar al personal y al público sobre cualquier política y práctica de seguridad que haya sido enmendada como resultado de construir un marco para el comercio electrónico que intensifique la confidencialidad de los potenciales clientes.

- Razonar y usar las distintas capas de protección: firewalls, servidores Web dedicados, servidores para redes privadas virtuales (***VPN***), líneas dedicadas, túneles seguros de Internet, Infraestructura de clave pública (***PKI***) o encriptación apropiada, autenticación y autoridad certificante.

- Establecer relaciones de seguridad con los vendedores y proveedores. Mantener los requerimientos de seguridad actualizados.

- Evaluar la seguridad desde distintas perspectivas: por ejemplo: mensajes mercantiles, mecanismos de contabilidad, pago y autenticación; software de pago persona-a-persona; procesos de registración y autenticación de clientes como además browser del cliente, aplicaciones del servidor y proveedor de servicio.

- Evaluar, en cualquier punto, la transmisión sobre Internet entre el remitente y el destinatario.

11. REGLAS IMPORTANTES EN E-COMMERCE

Las reglas importantes implican estándares, procedimientos y herramientas que llevan las políticas a la práctica. En el campo de la tecnología de la información, es importante saber cuales estándares son reglas importantes y que reglas necesitan de cuales estándares. Existen algunas reglas que son candidatas para asegurar un comercio electrónico seguro, entre las que se pueden mencionar las siguientes:

- Ninguna persona u organización externa podrá acceder al sistema de la empresa excepto a través de un firewall específico. Las razones comerciales decrecientes que obligan a esto son: las necesidades de protección en el punto de entrada a la red; en segundo lugar, el valor agregado de tener un sistema firewall instalado y que sirva de ayuda y finalmente, la ventaja en costo y administración, de la capacidad de distribuir electrónicamente actualizaciones de software según se necesiten.
- Todas las intranets deben usar servidores que puedan ínter operar con ***Windows NT***. Adoptar esto como una regla significaría no permitir el uso de servidores ***UNÍX*** que sigue siendo el hardware de opción de muchos servidores finales. Esto significa que hay una razón convincente para ello y es que la elección de servidores ínter operables ***NT*** asegura la integridad de las computadoras de escritorio a través de la plataforma de la empresa y reduce el costo de mantenimiento de las unidades intranets de negocios, las ***LANs*** y ***PCs***. Como agregado, se reducen los costos de la seguridad y administración de la red tanto para la empresa como para los administradores de las intranets.
- El software de encriptación será el estándard para cualquier aplicación de comercio electrónico que implique tanto operaciones que actualicen las bases de datos de la empresa o que involucren pagos. Las aplicaciones que sólo manejan flujos de información en una sola dirección, tales como información de producto y nombres de contactos, pueden utilizar el software ***RST*** (más débil) que emplea claves cortas.
- Las operaciones de comercio electrónico que implique cualquier forma de pago, tal como el uso de tarjeta de crédito, se procesarán fuera de línea. La razón que obliga a esto se debe a que el costo de asegurar la seguridad en estos casos se reduce significativamente si no hay procesamientos de pagos en línea que se puedan interceptar o puedan ser modificados.
- Antes que cualquier operación de comercio electrónico, incluyendo a las intranets, tome vida, la unidad de negocios responsables de las misma, debe demostrar que tiene registrada en línea una completa auditoria que per-

mite solucionar las debilidades de la seguridad y que es aceptada por los administradores seniors.

Si no hay ninguna razón comercial obligatoria, no habrá reglas importantes sino sólo recomendaciones, pero si las hubiera, se deben cumplir las enunciadas en al apartado superior y para que las mismas se cumplan es necesario que haya un informe claro de las responsabilidades y de las autoridades empresarias, resguardadas por medio de procedimientos apropiados de seguimiento.

1. Debe existir un punto sencillo de contacto para el apoyo orgánico: el mejor aliciente para que las unidades de negocios cooperen con entusiasmo, es proporcionar incentivos no demandas. Los dos principales incentivos en IT son el volumen de compras y el apoyo de la organización. Si la empresa IS establece un estándar o sistema como obligatorio, brindar apoyo completo, a través de: help-desk, especialización, manejo de las crisis y de las relaciones de los vendedores.
2. Debe existir un proceso bien definido para tratar las excepciones: inevitablemente, habrá situaciones en que las reglas legítimas no podrán seguirse o no son apropiadas para situaciones inusuales o no anticipadas y por lo tanto existe la necesidad de que haya algún mecanismo para manejarlas.

En conclusión podemos decir que hay tres preguntas directivas, a tener en cuenta: ¿quién establece las reglas importantes?; ¿Quién es responsable de que los recursos necesarios para que éstas se cumplan están disponibles?; ¿ y quién paga por ellos?; ¿Cuál es el mecanismo que utiliza la empresa para manejar las excepciones?.

12. SELECCIONANDO REGLAS IMPORTANTES

Los principios fundamentales para seleccionar las reglas importantes son, primero, asegurar claramente una coordinación central y, segundo, ofrecer ayuda e incentivos para lograr una autonomía local. La organización IS corporativa es responsable de la coordinación y es la que brinda autoridad y responsabilidad; también ofrece incentivos para lograr cooperación proporcionando una lista de productos recomendados para los cuales ofrece soporte, solución de problemas y acuerdos de compras en volumen; no ofrece productos donde las unidades de negocios están en libertad de elegir lo que quieran.

La elección de reglas importantes demanda una decisión muy cuidadosa. El objetivo es definir un conjunto mínimo de las mismas que alcancen los objetivos de coordinación y autonomía. Históricamente, la tendencia de IS y de las unidades de control es sobredimensionar los estándares e imponer lo que en realidad son regulaciones. Normalmente se puede decir que, es muy raro que se necesitan más de una docena de reglas importantes para el comercio electrónico. Todo lo expuesto hasta aquí , define la estructura de seguridad de la empresa. Existen dos tipos principales de relaciones en el comercio electrónico: Empresa-a-Empresa (B2B) y Consumidor-a-Empresa. En la tabla 6.2 se definen sus conocimientos técnicos, sus mecanismos propios de seguridad , equipos y experiencia con el comercio electrónico.

	Sencillos	**Expertos**
Empresa-a-Empresa	- Acceso básico a las PC para servicios estándares. - No tienen expertos en seguridad propios. - Reacios o incapaces de implementar procesos y sistemas complejos.	- Establecen acuerdos entre las partes comerciales para las principales relaciones de comercio electrónico. - Conocimientos completos acerca de las nesecidades de seguridad y sus mecanismos. - Tienen expertos en seguridad bien preparados.
Consumidor-a-Empresa	- Cometen muchos errores en el uso de las tecnologías. - No piensan en los riesgos. - Varían de tecnología. - Reacios o incapaces de invertir en nuevas herramientas o procedimientos. - Preocupados por la seguridad de las tarjetas de crédito y la privacidad.	- Muy conscientes de los problemas de seguridad. - Dispuestos a invertir en seguridad. - Conocimiento activo de elementos esenciales de la tecnología de seguridad. - Realiza la encriptación de los datos de las operaciones con tarjetas de crédito.

Tabla 6.2 Perfiles en las relaciones de comercio electrónico

CAPITULO 7
CONTROLES EN E-COMMERCE

1. CONTROLES INTERNOS

El control es el objetivo fundamental del negocio y es crucial para el éxito del mismo. Este concepto, hasta hace poco, ha sido estrechamente asociado con el contador, dentro del departamento del departamento contable y de auditoria. Antes de los 90, pocos directores de empresas se sentían que ellos eran responsables directos de la estructura de control interna de la empresa. Ahora, con un nuevo enfoque sobre el manejo de la empresa, se espera que los directores comprendan las estructuras internas de control de sus empresas y que reporten a sus supervisores si tienen alguna dificultad al respecto.

Existen cuatro desarrollos recientes, en el área de control interno, que tiene importancia significativa para los administradores en general y para los auditores en particular y que constituyen la base para evaluar los controles en el comercio electrónico y ayudan a los administradores a asegurarse que no se encontrarán con sorpresas desagradables en sus negocios. Ellos son los siguientes:

1.1. *Control Interno: Marco Integrado, 1994*

Este informe, publicado por ***COSO*** (Committee Of Sponsoring Organizations of the Treadway Comisión) en los Estados Unidos en 1992, y revisado en 1994, identifica cinco componentes de control interno interrelacionados:

1. ***Entorno de control***: las personas y el ambiente en que ellos operan.
2. ***Evaluación de riesgos***: visión integradora de los riesgos a los cuales debe enfrentarse la empresa y mecanismos para identificar, analizar y manejar los riesgos asociados.
3. ***Actividades de control***: políticas y procedimientos establecidos y ejecutados para ayudar a asegurar que los riesgos se manejan apropiadamente y que se llevan a cabo apropiadamente los objetivos de control.
4. ***Información y comunicación***: formas y medios que tiene el personal de la empresa, para capturar e intercambiar información necesaria para guiar, administrar y controlar las operaciones de la misma.
5. ***Seguimiento***: Forma dinámica de reaccionar, para cambiar según las condiciones de las garantías.

El componente novedoso de este marco es que pone énfasis en que el control interno es un proceso que debe integrarse con las actividades comerciales prolongadas y el mismo es visto como una parte del proceso comercial por lo que los administradores necesitan aceptar una visión vigente de estos elementos.

1.1.1.*Implicaciones de COSO en el contexto del comercio electrónico*

Debido a que el control interno es centrado en proceso, el comercio electrónico y las auditorias (que son parte del proceso de negocio), deben ser también centradas en proceso. La revisión de proceso necesita que los administradores y auditores entiendan el comercio electrónico de principio a fin: del cliente a la red y de la red a la empresa y viceversa. Por eso tiene sentido seguir el espíritu de ***COSO*** y delimitar los roles y responsabilidades (de los directores, administradores, auditores, etc.) para el control de problemas específicos en el comercio electrónico.

2.1. *Guía para evaluar el Control, 1999*

Luego de la publicación de la ***Guía de Control***, en 1995, el centro de control de criterios (***CoCo***) del Instituto Canadiense de Contadores Públicos (***CICA***) publicó su tercer guía de documentos relacionados con el control. La ***Guía para evaluar el Control*** ofrece ocho principios de evaluación y especifica claramente las responsabilidades del cuadro de directores, los CEO y de las personas designadas para conducir la evaluación, incluyendo a los auditores internos. También proporciona preguntas genéricas para cada grupo de asesores de control de modo que se utilicen como plataforma para personalizar sus propios cuestionarios de control. Este modelo de control constituye un primer paso para fijar el entorno

de control del comercio electrónico pero con la salvedad que se debe estar atento a no perder de vista los problemas ínter empresariales: (1) La naturaleza global del comercio electrónico; (2) dada la cantidad de comercio electrónico que es tercerizado y la resolución interna y articulación de los arreglos comerciales con entidades externas, el enfoque dela entidad legal sólo puede mostrar una parte de lo que se necesita; (3) ya sea que se trate de comercio negocio a negocio o negocio a consumidor, el mismo se basa en relaciones entre partes no entre empresas; (4) tal como con ***EDI***, no se puede evaluar la efectividad de la administración ínter empresaria utilizando sólo ocho principios, a menos que se preste una especial atención al entorno externo el que debe monitorearse constantemente y hacer los cambios donde sea necesario.

3.1. *Guía sobre Control, 1995*

En 1995, el consejo de Criterios de Control de ***CICA*** publicó su primera *Guía de Control* para directores, organizaciones gubernamentales, administradores, empresarios, inversionistas y auditores. Este documento es útil para cualquiera que sea responsable del control de la organización.

Conocido como el informe ***CoCo***, este documento define ampliamente el control (no los controles internos) como aquellos elementos de una empresa que, en su conjunto, ayudan a las personas a lograr los objetivos de la misma. ***CoCo***, trata de las relaciones entre todos los componentes de una empresa. Los controles internos, en términos ***CoCo***, se definen como aquellos chequeos, comparaciones, rutinas de análisis que se diseñan para proporcionar seguridad a las operaciones según se diseñaron.

Para establecer la confiabilidad, ***CoCo***, define 20 criterios de control básicos para comprender el control en las empresas y juzgar su efectividad. Estos criterios se agrupan en cuatro componentes:

1. **Objetivo**: brinda el sentido de la dirección de la empresa.
2. **Compromiso**: brinda el sentido de la identidad y valor de la empresa.
3. **Competencia**: brinda el sentido de la competencia de la empresa.
4. **Supervisión y aprendizaje**: proporciona el sentido de la evolución de la empresa.

El entorno ***CoCo*** proporciona información sumamente flexible de cómo será implementado el control.

3.1.1 *Influencia de CoCo en el contexto del comercio electrónico*

Desde el punto de vista de su aplicación en el comercio electrónico, son útiles los siguientes conceptos:

- La personas de la empresa participan en y tienen responsabilidad del control.
- *CoCo* pone mayor énfasis en aspectos sobre las personas, tales como: compromiso, capacidad, confianza mutua y la adopción periódica de desafíos.
- La definición de control, según ***CoCo,*** incluye la identificación y el debilitamiento de los riesgos de fallos para mantener la capacidad de la empresa a adaptarse a riesgos inesperados y a oportunidades.

4.1. *Objetivos de Control para la información y tecnología relacionada, 1998*

La ***ISACA*** (Information Systems Audit and Control Association: Asociación de Auditorias de Sistemas de Información y Control) de los Estados Unidos, desarrolló y mejoró el ***CobiT***, para que sirviera como marco para el control de las tecnologías de la información. Se diferencia de *COSO* y *CoCo* porque toma una visión tridimensional del control de la tecnología de la información: la interacción entre los procesos IT, los criterios de información y los recursos IT. Organiza 34 objetivos de control en dominios, procesos y actividades, los que están enlazados a los requisitos comerciales de información.

CobiT identifica cuatro dominios:

- **Planificación y organización**: cubre estrategias y tácticas comerciales principalmente relacionadas con la identificación de la forma en que la ***IT*** puede contribuir para el logro de los objetivos comerciales.

-**Adquisición e implementación**: se refiere a la necesidad de que las soluciones ***IT***, se integren en los procesos comerciales.

- **Entrega y soporte**: describe las actividades principales de las tecnologías de la información.

- **Seguimiento**: establece que los procesos *IT*, deben someterse a la evaluación de su calidad y cumplimiento con los requerimientos de control

4.1.1 *Influencia de CobiT en el marco del comercio electrónico*

CobiT brinda, a los profesionales de comercio electrónico, tres criterios de control que denomina requerimientos comerciales para la información:

- **Requerimientos de calidad**
- **Requerimientos de confiabilidad**
- **Requerimientos de seguridad**

Así mismo amplía los tres modelos de referencia, citados arriba, para incluir siete requisitos de criterios de información para administrar sus 34 objetivos IT de control de alto nivel. Estos incluyen: efectividad, eficiencia de las operaciones, confiabilidad de la información, cumplimiento de la ley y las regulaciones, confidencialidad, integridad y disponibilidad. Todos estas características son esenciales para el diseño de controles para el comercio electrónico.

Los controles existen para mejorar los negocios, son parte del mejoramiento de la estrategia comercial y no una estrategia de defensa.

5.1. Entorno de control para el comercio electrónico

Los conceptos de *CoCo*, *COSO* y *CobiT* se diseñaron para poder aplicarse ampliamente en muchas situaciones por lo que son muy flexibles cuando se aplican en la mayoría de los entornos comerciales. Los controles están relacionados con los riesgos; el manejo de los riesgos y la estructura de control asociada en una empresa tienen las siguientes características: junta de vigilancia; política de riesgo e identificación del riesgo por parte de los administradores seniors. La función de auditoria se ocupa del control de la estructura y su objetivo es proporcionar una evaluación independiente de los riesgos y los procesos de control. La inclusión del comercio electrónico dentro de una empresa no cambia la estructura de control sino el método de auditoria: en vez de buscar sólo dentro de la empresa cuales son los controles necesarios ahora deberán averiguar si las estructuras de control de sus compañeros comerciales son adecuadas y consistentes en la práctica.

Se debe alentar a los auditores a compartir con los administradores los resultados de sus riesgos en el comercio electrónico y la evaluación del control ya que es una forma práctica de asegurar que los objetivos y controles comerciales están sincronizados.

Objetivos comerciales: En el mundo del comercio electrónico, donde todos pueden estar potencialmente conectados con todos por intermedio de Internet, los requerimientos comerciales de confianza y responsabilidad son obvios. Estos requerimientos, a su vez, utili-

zarán tecnología que permita entregar información que se adecue a los requerimientos de calidad, seguridad y valores comerciales exigidos por *CobiT*. Doblemente importantes son los requerimientos de valores: en el caso de empresas públicas, permiten proteger los intereses de los depositarios y en todos los demás casos, pueden verse como una forma ética de cuidar la seguridad de los clientes quienes a su vez, inspirarán y mantendrán el vínculo de confianza y cuidarán las relaciones comerciales.

Objetivos de control: Los controles existen para cumplimentar algunos requerimientos comerciales importantes; pueden aplicarse cinco objetivos clásicos de control para alcanzar los objetivos comerciales del comercio electrónico: (1) control de administración; (2) confiabilidad de la información; (3) seguridad; (4) seguimiento y (5) oportunidad, disponibilidad y recuperabilidad. La evaluación de los riesgos comienza entendiendo cuáles son los problemas a enfrentar para lograr estos objetivos.

6.1. Guía para los administradores de IT

Lo primero que deben hacer los administradores de IT es diseñar políticas y procedimientos de control e integrarlos a la empresa y a sus objetivos comerciales como así también, relacionar los elementos de control para lograr decisiones coordinadas. Es importante incluir reglas de seguridad en las políticas comerciales para el comercio electrónico. *Debe haber una cantidad suficiente de actividades de planificación que permita incluir la seguridad dentro del diseño básico.*

Conocer los temas que son importantes para el comercio electrónico: declaraciones regulatorias, protección de la propiedad de la información, privacidad y seguridad. Cuando exista una regulación se deben realizar los mayores esfuerzos para cumplir con la misma.

Los procesos de comercio electrónico son altamente dependientes de muchos vendedores y proveedores externos, desde la adquisición de servicios de hardware y software basados en la Web hasta contratos y acuerdos con intermediarios tales como VANs, ISPs y portadores de datos a través de redes.

Se deben discutir, en etapas tempranas, las políticas IT existentes en las otras empresas sobre comercio electrónico y su relación con los componentes externos y obtener la opinión del departamento legal para saber si se pueden cumplir con las mismas.

En el comercio electrónico, lo más importante es lo referido a la privacidad respecto de la custodia y uso de la información del cliente en el lugar vendedor. Si el vendedor no está sujeto a auditorias regulares, *negociar el derecho de incluir una cláusula de auditoria, y antes de firmar el contrato, especificar claramente quién pagará la misma.*

La ***CSA*** (*Control Self Assessment*), es un método que está incrementando su aceptación como forma para que los administradores comuniquen sus responsabilidades de control

e informen el estado de las acciones de control. Se recomienda a los administradores IT resaltar y documentar los riesgos y controles claves en el comercio electrónico utilizando este método.

Comunicar interna y externamente: aunque la información está disponible en los sitios Web, el mejor recurso siempre es el colega en otra organización o el administrador con el cual se tiene una relación de comercio electrónico. Del mismo modo que EDI, los administradores de IT están desarrollando sistemas corporativos y deben mirar más allá de los límites de sus propias organizaciones para obtener soluciones ganadoras.

Apuntar alto para lograr una buena relación costo / efectividad de comercio electrónico: una buena relación de comercio electrónico es aquella que es simple, conveniente, siempre disponible, libre de error, fácil y libre. Dependiendo del tipo de aplicación de comercio electrónico, alguna de estas características son más importantes que otras.

Durante una implementación de comercio electrónico, hay veces que una regla de seguridad o una medida de control no se puede aplicar por distintas razones válidas. *Se deben brindar controles alternativos como soluciones provisionales, pero a medida que el comercio electrónico crezca o las actuales tecnologías se reemplacen en los años futuros, estos controles alternativos pueden ser ineficaces.* Asegúrese que se revisan periódicamente si es que cambia el entorno del comercio electrónico.

Incluir a los auditores desde el inicio de un proyecto de desarrollo de comercio electrónico: de esta forma los auditores tienen la oportunidad de ver en acción el comercio electrónico a través de las unidades funcionales o comerciales y pueden traer las buenas prácticas de control de una división para que se consideren en la próxima y cruzar los resultados. Donde los auditores pueden contribuir mejor son en las áreas de seguridad, auditoria y control.

7.1. Comparación entre COSO, CoCo y CobiT

	COSO	CoCo	CobiT	Implicación para el EC
Audiencia	Administradores	Aplicable a todos los miembros de la empresa, incluyendo a directores, administradores, empleados y otros.	Administradores, usuarios, auditores.	Los administradores de la IT, son miembros de un grupo de administradores de la empresa. Deben tener un alto nivel de conocimiento sobre estos modelos.
Definición, alcance	Visto como un proceso amplio de la entidad.	Concerniente a la organización, como un todo, para el logro de sus objetivos. Se consideran claves, las interconexiones y relaciones entre todas las unidades comerciales y el entorno externo.	Visto como un proceso, enfocado en las funciones de control de la IT.	El comercio electrónico debe verse primero como un proceso a ser integrado con las actividades comerciales en curso.
Conceptos fundamentales	El control interno se ve afectado por el conjunto de los directores, administradores y otro personal destinado a proporcionar una seguridad razonable con respecto al logro de los objetivos declarados	El control se refiere al futuro y al logro de la misión y la visión. CoCo se basa en la filosofía de que la empresa como un todo, es más grande que la suma de sus partes y que el todo tiene características que ninguna de las partes individualmente tiene. Las empresas se consideran sistemas orgánicos dinámicos que	El control, en la IT, se logra mirando la información que es necesaria para ayudar a los requerimientos comerciales y a los recursos y procesos asociados a la misma.	El control, en el comercio electrónico, debe enfocarse evaluando la información que se necesita para el apoyo de los requerimientos comerciales del mismo.

	COSO	CoCo	CobiT	Implicación para el EC
		cambian constantemente, se adaptan y aprenden en oposición a la visión mecanística, determinística y estática.		
Objetivos de control	Efectividad y eficiencia de las operaciones. Informe financiero fiable. Cumplimiento de las leyes y regulaciones.	En primera instancia, logro de la misión y visión de la empresa. Esforzándose en lograr esto, hay objetivos subordinados que caen en una de las siguientes categorías: Efectividad y eficiencia de las operaciones. Informes internos y externos confiables. Cumplimiento de las leyes, regulaciones y políticas internas.	Efectividad Eficiencia Confidencialidad Integridad Disponibilidad Cumplimiento Confiabilidad de la información	Los objetivos comerciales y de control son los mismos. Todos los atributos enunciados a la izquierda de esta columna contribuyen a establecer la responsabilidad y confianza en el comercio electrónico.
Componentes del control	Entorno de control. Evaluación de riegos. Actividades de control. Seguimiento de la información y la comunicación.	Propósito: ser guiado por la misión y la visión. Compromiso con el propósito. Capacidad de la empresa de lograr sus propósitos. Seguimiento y aprendizaje para adaptarse y cambiar según las necesidades.	Planificación y organización. Obtención e implementación. Entrega y soporte. Seguimiento.	Estos componentes se pueden usar para construir un marco integrado de control para el comercio electrónico.
Responsabilidad del control	Administración.	Función de la dirección de la em-	Administración.	Por extensión, cada uno en la empresa.

	COSO	CoCo	CobiT	Implicación para el EC
		presa. Cada uno, en la empresa, tiene una función de dirección. La responsabilidad final está en manos del plantel directivo, pero el mismo necesita movilizar a toda la empresa para este logro.		La dimensión del control no debe descuidarse.
Juicio de efectividad	Seguridad razonable de que se alcanzan los objetivos formulados.	Utilizando los 20 principios, agrupados dentro de los cuatro componentes de control, como guía. Los criterios no son estándares mínimos y son importantes por naturaleza.	Satisface los objetivos formulados.	Satisface los objetivos comerciales y de control planteados para el comercio electrónico.
Informe periódico de control	En un punto establecido.	De acuerdo con la capacidad futura de la empresa para lograr su misión y visión.	Para un período de tiempo.	Se recomienda que la auto evaluación del comercio electrónico se informe sobre un período de tiempo.

Tabla 7.1 Comparación entre COSO, CoCo y CobiT

CAPITULO 8
CONCLUSIONES

Cuanto más rápido sea el crecimiento del comercio electrónico, más importante se volverá todo lo relacionado con la seguridad tanto en el aspecto de la defensa del sistema como a la mejora comercial. El incremento de los riesgos tecnológicos significa riesgos comerciales como así también riesgos en las relaciones comerciales.

El comercio electrónico es completamente dependiente de las relaciones establecidas entre las partes involucradas y cambia muchas de las reglas básicas de los negocios lo que significa que cambiará muchas de las reglas de seguridad, contabilidad y control financiero. Esta es una consecuencia obvia pero lo que no se puede saber es cuales, cuando y como.

El desafío es planificar cuando no se puede predecir y ver cuales son las tendencias y evaluar sus influencias en la seguridad, auditoria y control. Estas tendencias se pueden clasificar en cuatro categorías de probabilidades: inevitables, fuertemente posibles, posibles y desconocidas ya sean: a corto plazo, en el mediano plazo o en algún momento aún desconocido.

Con estos elementos se puede construir una matriz que analice las consecuencias en cada una de estas dimensiones:

Tabla 8.1 Tendencias de seguridad en el comercio electrónico

	A corto plazo	A mediano plazo	A plazo desconocido
Inevitables	Módulos de software como componentes principales de los desarrollos de aplicaciones de comercio electrónico. Crecimiento rápido en Intranets, Extranets. Total confianza en el ANSI X12.	Uso extendido, en Internet, de tarjetas de crédito por parte de los consumidores.	Dinero digital. Desmaterialización total.
Fuertemente posibles	Uso de aplicaciones de redes. Estandarización de pagos seguros en el comercio electrónico. Crecimiento en el uso de software agente.	Reglamentación internacional del comercio electrónico. Leyes de protección al consumidor para las operaciones de comercio electrónico. Implementación total de una fuerte encriptación. Adopción plena del comercio electrónico en las operaciones comerciales gubernamentales.	Escasez de expertos necesarios para la seguridad del comercio electrónico. Necesidad de establecer terceras partes confiables. Tiene éxito la televisión interactiva.
Posibles	Uso extendido de los estándares y herramientas de comercio electrónico de Microsoft.	Desaparición de las VANs como la fuerza principal del comercio electrónico. Crecimiento del uso de la telecomunicaciones inalámbricas para el comercio electrónico.	
"Estallido" potencial	Juicios potenciales por problemas derivados del comercio electrónico.	Muchos fallos de Internet. Internet como el cielo del "cracker".	Muerte del copyright.

APÉNDICE A

ACRÓNIMOS

ACL	Lista de Control de Acceso (*Access Control List)*
ACM	Asociación para las máquinas de computación (*Association for Computing Machinery)*
ANS	*Advanced Networks and Services*
ARPA	Agencia de proyectos de investigación avanzados (*Advanced Research Proyects Agency*)
ARPANET	*Advanced Research Projects Agency Network*
AT&T	*American Telephone and Telegraph Company*
ATM	Modo de Transmisión Asincrónica (*Asynchronous Transfer Mode*)
BBN	*Bolt, Beranek and Newman, Inc.*
BBS	*Bulletin Board System*
BITnet	*Because It's Time Network*
BSD	*Berkeley Systems Distribution of Unix*
CAD	*Diseño asistido por computador*
CAM	*Producción asistida por computador*

CERF	*California Education and Research Federation*
CERFnet	*California Education and Research Federation network*
CERN	*Laboratorio de Física de Partículas (Counseil Europeen pour la Recherche Nucleaire*
CERT	*Computer Emergency Response Team*
CGI	*Common Gateway Interface*
CICA	Instituto Canadiense de Contadores Públicos
CORE	*Consejo de Registradores (Council of Registrers)*
CobiT	Objetivos de Control para la información y tecnología relacionada
CoCo	Centro de Control de Criterios
COSO	*Committee Of Sponsoring Organizations of the Treadway Commission*
CREN	Corporación para Investigación y Redes Educacionales (*Corporation for Research and Educational Networking*)
CSA	*Control Self Assessment*
CHAP	*Challenge-Handshake Authentication Protocol.*
CSNET	*Computer Science Network*
DARPA	Agencia de proyectos avanzados de investigación de defensa (*Defense Advanced Research Projects Agency*)
DES	*Data Encryption Standard*
DNS	*Domain Name Server*
DOI	*(Domain of Interpretation)*, Dominio de Interpretación.
DSL	*(Document Security Language),* Documento del Lenguaje de Seguridad.
EAP	*(Extensible Authentication Protoco)*, Protocolo Extendido de Autenticación.
ECP	*(Encription Control Protocol)*, Protocolo de Control de Encriptación.
EARN	Red Europea Académica y de Investigación (*European Academic and Research Network*)
EEUU	Estados Unidos

Email	*Electronic Mail*
FIDOnet	*FIDO Bulletin Board System Network*
FIX	*Federal Internet exchange*
FNC	*Federal Networking Council*
IAB	*Internet Activities Noard*
IAHC	*Internet Ad Hoc Committee*
IBM	*International Business Machines Corporation*
ICCB	*Internet Configuration Control Board*
ICCC	Conferencia Internacional sobre Comunicación por Computadora (*International Conference on Computer Communcatiions)*
ICE	Intercambio de información y contenido, *(Information and Content Exchange).*
IETF	*Internet Engineering Task Force*
IMP	*Interface Message Processor*
INTA	*International Trademark Association*
InterNIC	Centro de Información de Internet (*Internet Network Information*)
INWG	*Internetworking Group*
IKE	*Internet Key Exchange*
IOTP	*Internet Open Trading Protocol.*
IPTO	Oficina para las Tecnologías de Procesamiento de la Información (*Information Processing Technology Office*)
IRC	*Internet Relay Chat*
IRTF	*Internet Research Task Force*
ISACA	Asociación de Auditoria de Sistemas de Información y Control *(Systems Audit And Control Association)*
ISAKMP	*Internet Security Association and Key Management Protocol.*
ISO	Organización Internacional de Normalización (*International Standard Organization*)

ISOC	Sociedad Internet (*Internet Society*)
ITU	*International Telecommunication Union*
JEPI	*Joint Electronic Payments Initiative.*
LDAP	Protocolo de Autenticación (*Light Weight Directory Access Protocol)*
MERIT	*Michigan Education Research Instruction Triade*
MILNET	*Military Network*
MIT	Instituto Tecnológico de Massachusetts (*Massachusetts Institute of Technology*)
MUD	*Multi-User Dungeon*
NCP	Protocolo de control de red (*Network Control Protocol*)
NH	*National Information Infrastructure*
NLP	Laboratorio Físico Nacional en Inglaterra (*National Physical Laboratory*)
NNTP	Protocolo de transferencia de noticias en red (*Network News Transfer Protocol*)
NREN	*National Education and Research Network*
NSF	*National Science Foundation*
NSFnet	*National Science Foundation Network*
NTIA	*National Telecommunications Information Administration*
NWG	*Network Working Group*
OMG	*Object Management Group*
OSI	Interconexión de sistemas abiertos
PAP	Protocolo de Autenticación de Password, *(Password Authentication Protocol).*
PPP	Protocolo Punto-a-Punto. *(Point-to-Point Protocol)*
RDB	Base de Datos Remota, *(Remote Data Base).*
RFC	Solicitud para comentarios (*Request for Comment*)
RIPE	*Reseaux IP Europeens*
SASL	*Simple Authentication and Security Layer.*

SRI	Instituto de Investigación de Standford (*Standford Research Institute*)
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TERENA	*Trans-European Research and Education Network Association*
UCB	*University of California at Berkeley*
UCLA	Universidad de California en Los Angeles (*University of California at Los Angeles*)
UCSB	Universidad de California en Santa Bárbara (*University of California at Santa Barbara*
UUCP	*Unix-to-Unix CoPy*
VAN	*Value-Added Networks*, redes de comunicación privada o también denominadas redes de valor añadido
XML	Lenguaje Extendido de Marcación, *(Extensible Markup Language).*
W3C	*World Wide Web Consortium.*
WIPO	*World Intellectual Property Organization*
WWW	*World Wide Web*

APÉNDICE B

GLOSARIO

Algoritmo criptográfico	Una función matemática que combina texto plano u otra información inteligible con una cadena de dígitos (llamada clave para producir un texto cifrado ininteligible.
Algoritmo de firma digital	Desarrollado por NIST, este sistema se basa en el algoritmo de El Gama El esquema de firma digital utiliza la misma clase de claves que Diffie-Hellman y puede crear firmas más rápido que RSA (conocido también como DSS o Digital Signature Standard).
Algoritmo internacional de encriptación de datos	Creado en 1991, ofrece una encriptación basada en una clave de 128 bits
ARP	Protocolo de resolución de direccionamiento que opera sobre la capa de red.
Autoridad certificante	Una empresa u organización confiable que aceptará su clave pública junto con alguna prueba de su identidad y que sirve como repositorio de certificados digitales. Otros pueden luego requerir verificación de su clave pública a través de la autoridad certificante
Browser Web	Un programa software que permite al usuario conectarse a un servidor de red para acceder a documentos HTLM y sus archivos de medios asociados y seguir enlaces de documento en documento, o página en página.
Cable módem	Un dispositivo que ofrece ancho de banda para transmisión de datos de más de 30 Mbps sobre la línea de cable TV existente.
CEO	Chief Executive Officer
Certificado digital	Documento electrónico, emitido por una autoridad certificante, usado para establecer la identidad de una empresa o persona, por medio de la

verificación de su clave pública.

CGI script (*Common Gateway Interface*) sistema de encriptación diseñado para trabajar con servidores web HTTP. La script, escrita generalmente en lenguaje Perl, se usa a menudo para intercambiar datos entre un servidor Web y Bases de datos.

cifrado Conjunto de reglas que se utilizan para transformar la información original en información codificada.

CIO Chief Information Officer.

Ciptografía asimétrica Un sistema criptográfico donde la encriptación y desencriptación se realiza usando distintas claves.

Clave Un conjunto de dígitos que, usados con un algoritmo de encriptación, produce texto cifrado.

Clave privada Clave usada por el receptor de un mensaje para desencriptar el mismo; puede divulgarse tanto como sea necesario.

Comoditización El proceso a través del cual los productos comienzan a verse parecidos, decrecen sus valores y sus precios bajan. Los productos considerados como commmodities no se ven como algo especial y, a menudo se venden a precios de guerra.

Cracker Persona que ve a Internet y a los sistemas de computación como campos de juego, para perjuicios y beneficios propios.

Criptografía de clave pública (PKI) Método de encriptación que utiliza un par de claves: una pública y una privada. Los mensajes encriptados por cualquiera de ellas pueden decodificarse utilizando la otra. La criptografía de clave pública utiliza un algoritmo asimétrico de encriptación. (*Private Key Infrastructure)*

CTO Chief Technology Officer.

DAP Protocolo de acceso a directorio (*Directory Access Protocol*)

Desintermediación Muchas empresas plantean Internet como un canal de venta directo a los consumidores, reduciendo el papel de los intermediarios tradicionales ya que surgen unos nuevos intermediarios digitales, aunque estos trabajarán con márgenes comerciales más pequeños.

Diffie-Hellman Un sistema creado para permitir que dos personas estén de acuerdo sobre una clave compartida, aún si sólo intercambian mensajes públicamente. El viejo sistema de criptografía de clave pública todavía se usa, pero no soporta encriptación ni firma digital.

Digital cash Reemplazo electrónico de dinero en efectivo.

Dirección IP Una dirección numérica que identifica a una computadora en la red.

DES Algoritmo que asegura la confidencialidad de la información.

DNS	*(Domain Naming Service)*, sistema de nombres de dominios). Este es el sistema de red responsable de convertir las direcciones IP en nombres basados en texto.
DSS	*Digital Signature Standard*
e-cash	Hace referencia a cualquier proceso que permita a una persona pagar productos o servicios transmitiendo un número de un computador a otro. El número es suministrado por un banco y representa una cantidad de dinero. Es un medio de pago anónimo.
EDI	*(Electronic Data Interchange).* Intercambio electrónico de datos, es el intercambio electrónico de documentos comerciales o de negocios (tales como ordenes de compra, remitos, facturas) entre compañías que trabajar con aplicaciones computadorizadas en una forma estandarizada. Los sistemas EDI se usan principalmente por empresas que quieran comunicarse con sus proveedores.
EDI abierto	Una serie de especificaciones diseñadas para que las transacciones EDI sean simples de especificar y setear como así también puedan usarse sobre Internet.
EFT	*(Electronic Fund Transfer)*, transferencia electrónica de fondos. Sistema que optimiza la transferencia de pagos electrónicos, incluyendo información del remitente, sobre redes privadas seguras entre bancos.
Electronic checks	Cheque electrónico. Basado en certificados digitales, se comprueba electrónicamente la validez del mismo.
Electronic wallet	Proceso por el cual se encripta el número de nuestra tarjeta de crédito en nuestro disco duro (por ej.: CyberCash o Verifone). Cuando el consumidor realiza un pedido, el software seguro del vendedor recoge esta información.
Encriptación simétrica	Al usar este método, tanto el remitente como el destinatario, poseen la misma clave, lo que significa que ambas partes pueden encriptar y desencriptar datos con esa clave.
e-tailers	Minoristas electrónicos.
Extranets	Dos o más intranets conectadas a través del protocolo TCP/IP; también llamadas redes compartidas.
FEDI	EDI financiero, usado entre bancos y sus clientes corporativos para permitir a los bancos recibir autorización de pago de los pagadores y hacer los pagos a los receptores. Se usa sólo para transacciones B2B.
Firewalls	Dispositivos que implementan controles de acceso basándose en el contenido de los paquetes de datos que se transmiten entre dos partes o dispositivos de la red. Proporcionan protección contra ataques sobre protocolos o aplicaciones individuales. No proporcionan privacidad ni autenti cación y no pueden proteger a una red contra virus.
Firma digital	Firma especial usada para firmar correspondencia electrónica, se crea

	encriptando el mensaje digest o resumen con la clave privada del remitente.
Firmas ciegas	Sistema, desarrollado por DigiCash que permite a un comprador obtener e-cash de un Banco sin que el Banco deba corroborar el nombre del comprador con el token que él usó.
Front-end processes	Aplicaciones de computadoras que corren en computadoras clientes conectadas a servidores o computadoras mainframe.
Función hash	Fórmula que se usa para para convertir un mensaje de cualquier longitud en una cadena de dígitos llamados un mensaje digest. La longitud de la función determina la longitud del digest y no se requiere ninguna clave.
Gateway	Un programa de software que se usa para conectar dos redes que usan distintos protocolos de manera que puedan transferir datos entre ellas. Antes de la transmisión, el programa convierte los datos en un protocolo compatible.
HTLM	Hyper Text Markup Language, un conjunto de estándard de códigos que se usan para definir documentos Web. El browser de la computadora del usuario mira el código HTML para determinar como se mostrará el texto, gráficos y otros elementos multimedia.
Intranet	Una red TCP/IP interna que se usa para compartir información dentro de una empresa.
IP	(Internet Protocol), este protocolo trabaja en la capa de red para proporcionar un espacio de direcciones para trabajos de Internet y para manejar el ruteo de paquetes a través de un trabajo Internet.
IS	Sociedad Internet *(Internet Society)*
ISP	*(Internet Service Provider)*, empresas que proporcionan a los clientes conexiones con Internet.
IT	Tecnología de la Información *(Information Technology)*
JECF	*(Java Electronic Commerce Framework).* Conjunto de librerías Java, de Sun Microsystems que incluyen wallet y opciones de seguridad para ayudar a los programadores Java a manejar los pagos electrónicos.
JEPI	*(Joint Electronic Payments Initiative).* Esta iniciativa desarrollada por el World Wide Web Consortium y CommerceNet, de standarización de las negociaciones de pago. Del lado del comprador (lado cliente), JEPI sirve como una interfaz que permite a un browser Web y wallets, usar protocolos de pagos variados; del lado del vendedor (lado servidor), actúa entre la red y la capa de transporte para pasar la transacción al protocolo apropiado de transporte y de pago.
Kerberos	Protocolo de control de acceso
Línea digital asimétrica	Protocolo que provee grandes cantidades de datos (6-9Mbs) sobre líneas telefónicas copper existentes.

Marketspace	Mercado donde se lleva a cabo el comercio electrónico. Término que acompaña la transición de un mercado físico a mercados basados en y controlados por la información.
MDS	Algoritmo utilizado para encriptación y que asegura la integridad de la información.
Mensaje resumen	La representación del cuerpo de un mensaje como una cadena simple de dígitos creados usando una función hash unidireccional.
Microcash	Denominación de los token digitales pequeños.
Micromerchants	Aquellos que ofrecen sus objetos en Internet a cambio de e-cash o digital cash.
Micropagos	Pequeñas transacciones entre 25 centavos y 10 U$D, normalmente usada para acceder a juegos, información, fotografías, música en la red.
Microsegmentación	Uso de preferencias detalladas de clientes para delinear grupos chicos de mercados.
Microtransacciones	Transacciones en tiempo real y bajo costo que usan microcash.
Middleware	Software de procesamiento de transacciones que permite a una aplicación cliente acceder datos de múltiple bases de datos.
NAPs	*(Network Acces Points)*. Redes backbone de Internet, de alta vekocidad mantenidas por Sprint, PacBell, MFS y otras.
OV	Organización virtual.
Paquete	Grupo de datos que se transmiten en una red digital. Un paquete consiste en una secuencia de bits que incluye información de control para transmitir los datos y los datos mismos.
PCT	Tecnologías de Comunicación Privada *(Private Communications Technology)*
PDA	*(Personal Digital Assistant)*, pequeña computadora personal portable.
PEM	(Privacy –Enhanced Mail), correo privado extendido. Un estándar Internet para la seguridad del correo que usa clave pública o clave simétrica.
PGP	*(Prety Good Privacy)*, las aplicaciones de seguridad PGP para correo electrónico de Internet usan una gran variedad de estándares de encriptación que están disponibles gratuitamente para la mayoría de los sistemas operativos. Los mensajes se pueden encriptar antes de usar un programa de correo y algunos programas de correo pueden usar módulos especiales PGP para manejar correo encriptado.
POP	*(Post Office Protocol)*, uno de los más importantes protocolo de Inter.-net para correo. POP se usa para manejar la recuperación de mensajes.

Procesos back-end	Aplicaciones de computadora que corren y usan datos almacenados en grandes mainframes u otros computadores o servidores.
Protocolo	Reglas que determinan como trabaja una red.
Protocolo de acceso al correo Internet	Protocolo que se usa para manejar la recuperación de mensajes.
Protocolo de datagrama de usuario	Este protocolo determina el tamaño del paquete a transmitirse.
Protocolo de transferencia de hyper-texto	Este protocolo determina como se transfiere un archivo HTLM desde ur servidor al cliente en la World Wide Web.
Protocolo TCP/IP	Este protocolo define como se dividen los datos en paquetes para la transmisión y como transfieren archivos y envían correo electrónico las aplicaciones.
Protocolos de ambientes distribuidos	Los protocolos DCE *(Distriibuted Computing Environment),* definen como los objetos o módulos software se almacenan y pueden interactuar a través de una red. DCE se usa a menudo para proporcionar una inter-fase común para aplicaciones de red y autenticación a los servicios de red.
RBAC	Control de Acceso basado en roles, *(Role-Based Access Control).*
RC2 – RC4	Algoritmos diseñados por Ron Rivest de RSA Data Security Inc., usan cifrado de clave variable para volúmenes de encriptación rápidos. Un poco menos rápidos que el DES, ambos algoritmos pueden ser más seguros si utilizan un tamaño de clave más grande. RC2 cifra por bloque y puede utilizarse en vez de DES. RC4 cifra por string y es diez veces más rápido que el DES.
Relaciones de mercado	Creación de relaciones de clientes con cada cliente individual.
RSA	Este algoritmo de encriptación de clave pública soporta longitudes variables de clave como así también longitudes variables de bloques del texto a ser encriptado. El bloque de texto a encriptar debe ser de longitud menor que la longitud de la clave. La longitud de la clave es comúnmente de 512 bits. Garantiza la autenticidad y el no repudio de la información.
RST	Software de claves cortas
Server proxy	Un server proxy adopta la forma de guardar información anticipadamente para proteger datos y aplicaciones importantes. Terminan la conexión entrante desde la fuente e inician una segunda conexión hacia el destino, asegurando que el usuario entrante tiene los derechos apropiados para usar los datos solicitados del destino antes de pasárselos.
SET	*(Secure Electronic Transaction)* Transacción Electrónica Segura, desarrollada por MasterCard/Visa es una combinación del protocolo diseñado para ser usado por otras aplicaciones (como por ej. browsers Web) y un standard (un procedimiento recomendado) para manejar operaciones de tarjetas de crédito sobre Internet.

S-HTTP

(Secure Hypertext Transfer Protocol), protocolo seguro de transferencia de hipertexto. Proporciona autenticación para servidores y browsers com así también confidencialidad e integridad de datos para la comunicación entre un servidor Web y un browser.

Smart cards

Tarjeta plástica de crédito con un tipo especial de circuito integrado incorporado a la misma. El circuito contiene información de manera electrónica y controla quien usa esta información y como.

SMTP

(Simple Mail Transfer Protocol), uno de los protocolos más importantes de Internet para el transporte de correo electrónico entre servers.

SNMP

(Simple Network Management Protocol), protocolo que se utiliza para controlar dispositivos de redes tales como routers, bridges y hubs.

SSL

(Secure Sockets Layer). Al igual que el S-HTTP, proporciona autenticación para servidores y browsers y confidencialidad e integridad de datos para comunicaciones entre un servidor Web y un browser pero SSL asegura el canal de comunicación operando a un nivel bajo en la pila de red , entre el nivel de aplicación y el nivel de transporte TCP/IP y los niveles de redes. SSL se puede usar para otras operaciones distintas de la Web, pero no está diseñado para manejar las decisiones de seguridad basadas en el nivel de la autenticación de la aplicación o documento.

SSO

(Single-Sign-On), mecanismo por medio del cual, mediante una única acción de autenticación y autorización, permite el acceso a un usuario a todas las computadoras y sistemas donde dicho usuario tiene permiso, sin necesidad de ingresar múltiples contraseñas.

Standard de datos encriptados

Un algoritmo o bloque cifrado que usa una clave de 56 bits y opera sobre un bloque de 64 bits. Creado por IBM y respaldado por el gobierno de los Estados Unidos en 1977, el estándard de datos encriptados es relativamente rápido y a menudo se usa para encriptar grandes cantidades de datos de una sola vez.

Start ups

Nuevas empresas de Internet

Stock options

Acciones.

SVPNs

Redes Virtuales Privadas Seguras (*Secure Virtual Private Netmorks*)

S/WAN

(Secure Wide-Area Networks), redes seguras de área amplia. Estos protocolos incluyen métodos de autenticación y encriptación de paquetes, como así también, métodos para intercambiar y manejar las claves necesarias para autenticación y encriptación de procesos. Los protocolos S/WAN también ayudan a asegurar la interoperabilidad entre router y firewall.

Telnet

El standard Internet para la emulación de terminales y acceso remoto.

Texto cifrado

La forma codificada de un mensaje.

TIC

Tecnologías de la Información y la Comunicación.

TLS	Seguridad de la Capa de Transporte *(Transport Layer Security)*
Tokens	Cadena de dígitos que representan una cierta cantidad de dinero. El banco correspondiente valida cada token con un sello digital.
TPA	*(Trading Partner Agrreements),* especificaciones que acatan una o más empresas que hacen negocios entre sí y que definen la forma de los datos que se van a intercambiar vía EDI.
URL	(Uniform Resource Locator), la forma de identificar un recurso en Internet. Un URL comienza con el nombre del protocolo necesario para obtener los datos desde el servidor seguido por el nombre, en caracteres, del recurso.
VAN	*(Value Added Networks)*, redes de valor agregado que son mantenidas de manera privada y dedicada a EDI entre compañeros de negocios.
VPN	Redes Privadas Virtuales *(Virtual Private Networks)*
Web server	Un programa software que maneja datos en el sitio Web, controla el acceso a los datos y responde a los requerimientos de los browsers.

APENDICE C

REFERENCIAS BIBLIOGRAFICAS

1. DIRECCIONES EN INTERNET

www.bcg.com
www.cace.com.ar
www.coldewey.com/europlop2000/papers
www.commerceNet.com
www.commercetimes.com/news
www.computerworld.com
www.ecomm.webopedia.com/TERMS/security.htlm
www.ecommerce.gov
www.ecommerce.ncsu.sdu
www.emarketer.com
www.fedex.com
www.forrester.com
www.gartner.com
www.hillside.net/patterns
www.idc.com
www.iesa.edu
www.isworld.org
www.itworks.be/reports
www.marketingycomercio.com
www.nercado.com.ar
www.nielsen.com
www.nipc.gov

www.onnet.es
www.opengroup.org/security
www.reingex.com
www.security-patterns.de
www.spf.gov.ar
www.techrepublic.com
www.verisign.com
www.w3.org/ECommerce
www.zdnet.com

BIBLIOGRAFIA

1. LIBROS

Hassler, Vesna. (2000).
Security Fundamentals for E-commerce.
Boston - London: Artech House Publishers.

Ghosh, Anup K. (2000).
E-Commerce Security: Weak Links, Best Defenses.
España: RA-MA.

Ghosh, Anup K. (2000)
Delivering Security and Privacy for E-Business.
NY, USA: Prentice Hall .PTR

2. ARTICULOS DE DIARIOS Y REVISTAS

Bini, Rafael. (2000,marzo).
Un evangelio para el comercio electrónico.
Nación, (Supl.Informática),17.

Bini, Rafael. (2000, marzo).
La fiebre del comercio electrónico.
Nación, (Sección 5), 16.

Blanco, Javier. (2000, abril).
Los cajeros: nuevos socios del e-commerce.
Nación, (Sección 2), 9.

Boragni, Claudia. (2000, abril).
Integrando redes.
Clarín, (Supl.Económico), 7.

Campanario, Sebastián. (2000, julio).
Como se arman los pronosticos virtuales.
Clarín, (Supl.Económico), 2-3.

Castrillón, Manuel H. (2000, enero).
Las reglas para una compra segura.
Nación, (Supl.Informático), 8-10.

EE.UU. pide más comercio electrónico. (2000).
Nación, (Sección 2 p.12).

El e-commerce transforma las organizaciones. (2000, junio).
Nación. (Sección 1), 8.

Ferrarese, Laura. (2000, abril).
Adiós a miles de sitios.
Nación, (Sección 2), 7.

Giglio, Josefina. (2000).
El futuro de los portales está en el
Comercio Electrónico.
Nación, (Sección 2), 4.

Grojsman, Lorena. (2000, julio).
El e-commerce estratégico.
Revista Mercado, 40-50.

Lejos del primer mundo. (2000).
Nación, (Sección 2), 4.

Levi Yeyati, Eduardo. (2000, abril).
Encandilados por la red.
Clarín, (Supl.Económico), 44.
Los medios electrónicos en la actividad financiera.
Nación, (Sección 2, Tecnologías y empresas), 3.

Luz verde a la firma digital.
Nación, (Sección 2, p.3).

Maas, Pablo. (2000, abril).
E-commerce: como ganar la gran carrera de Internet.
Clarín, (Supl.Económico), 4-6.

Mangalindan, Mylene. (2000, octubre).
¿Qué dicen los profetas de la Red?
Nación, (Sección 2), 8.

Pellegrinelli, Victoria. (2000, marzo).
Internet: Hacia donde va la Red en Argentina.
Revista Negocios, 52-56.

Ravier, C. Y Heller, D. (2000).
Yo vendo en Internet ¿y Usted?
Nación, (Sección 2), 4.

Rouillon, Jorge. (2000, noviembre).
Internet plantea retos al derecho.
Nación, (Sección 1), 10.

Sametband, Ricardo. (2000, noviembre).
La firma digital llega a la Argentina.
Nación, (Supl.Informática), 8-9.

Silva Pintos, F. Y Pellegrinelli, V. (2000).
E-commerce: Todas las fichas al B2B.
Revista Negocios. 72-74.

White, Joseph. (2000, octubre).
Que funciona y que no en el comercio en línea.
Nación, (Sección 2), 8.

Wolf, R., Tait, N. & Bowe, Ch. (2000,junio).
Fantasmas del cybermercado.
Clarín, (Supl.Económico), 17.

INDICE ALFABETICO

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

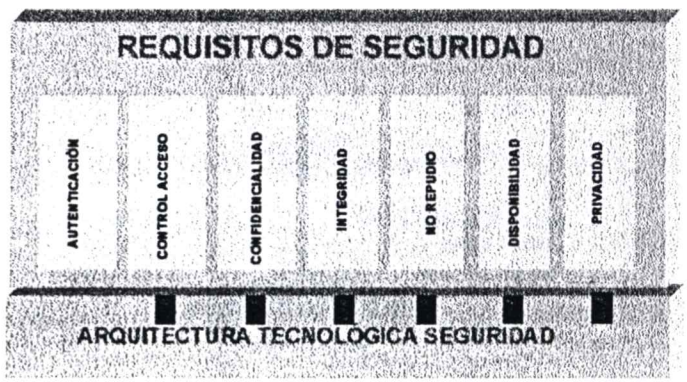
W

Seguridad e-commerce:

Lic.Susana Vaquer

svaquer@arnet.com.ar

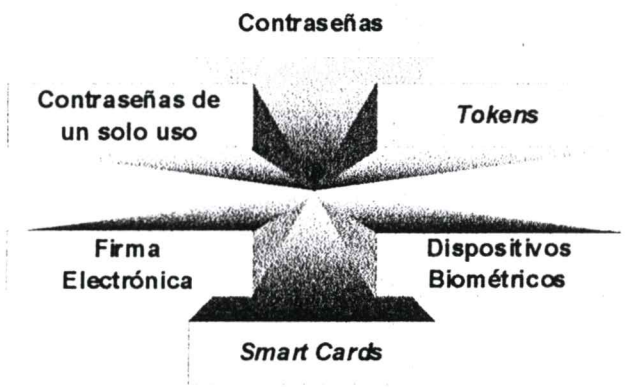
Requerimientos de seguridad



AUTENTICACION - DEFINICION

- Identificación de los participantes en las transacciones por medio de la verificación de sus identidades
- Garantiza que el usuario que accede a áreas de un sistema es quien dice ser

AUTENTICACIÓN



AUTENTICACION – METODOS

- **Contraseñas:** secuencia secreta de caracteres que se teclean y se requieren para utilizar un sistema o servicio
- **Contraseña de un solo uso:** una única acción de autenticación y autorización permite a un usuario acceder a todas las computadoras y servicios a los cuales tiene permiso de acceso

AUTENTICACIÓN - METODOS

- **Tokens:** dispositivo de autenticación del tamaño de una tarjeta de crédito que posee un usuario remoto
- Posee una serie de números que cambian a través del tiempo
- Los números están sincronizados con un servidor de autenticación de la red

AUTENTICACION - METODOS

- **Firma electrónica:** firma especial usada para firmar correspondencia electrónica
- Se crea encriptando el mensaje resumen con la clave privada del remitente
- Permite al receptor de los datos comprobar su fuente y la integridad de lo recibido.

AUTENTICACION - METODOS

- **Dispositivos biométricos**
- Se utilizan para:

  - controlar los acceso a sistemas informáticos
  - garantizar la seguridad en transacciones bancarias
  - acceder a nuestro dinero

AUTENTICACION DISP.BIOMETRICOS

- Identifican automáticamente a un individuo por sus características:

  - biológicas
  - psicológicas
  - de conducta

AUTENTICACION DISP.BIOMETRICOS

- Verificación de identidad a través de:

  - el modelo de huellas digitales
  - de vasos sanguíneos en la mano o retina
  - el modelo del rostro
  - el olor

AUTENTICACION DISP.BIOMETRICOS

- **Componentes:**

  - **Hardware:** captura la característica concreta del individuo

  - **Software:** interpreta la información y determina su aceptabilidad o rechazo según datos previamente almacenados

AUTENTICACION DISP.BIOMETRICOS

- **EJEMPLOS:**

  - Sensor de huellas dactilares
  - Videocámara para identificación de iris/retina
  - Videocámara para identificación de rostro, mano completa, etc.

AUTENTICACION SMART CARDS

- Tiene el tamaño de una tarjeta de crédito
- Puede almacenar muchos datos y contiene un microprocesador que ejecuta procesos, por ej. encriptación
- Un lector de smart cards lee los datos y los envía a través de la red
- Pueden protegerse a través de una password

AUTENTICACION SMART CARDS

- **APLICACIONES EN LA WEB:**

  - Almacenamiento de claves encriptadas
  - Dinero electrónico
  - Perfil portátil del usuario

CONTROL DE ACCESO ELEMENTOS BASICOS

- Manejo de la capacidad o derecho de una parte para entrar o acceder a una zona o servicio
- **Incluye:**
  - **un objeto** (sistema, programa, BD, etc.)
  - **un sujeto** (entidades externas que acceden a los objetos)
  - **derechos de acceso** (forma que los sujetos acceden a los objetos)

CONTROL DE ACCESO ORGANIZACION

- **Se organizan casi siempre en forma de:**

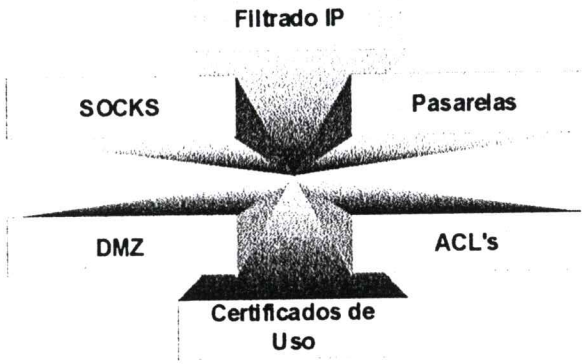
  - Matrices de acceso
  - Listas de Control
  - Listas de Capacidades

CONTROL DE ACCESO PROTOCOLOS UTILIZADOS

- **LDAP**
- Proporciona acceso seguro a contraseñas en un directorio/repositorio
- No ofrece la flexibilidad y rendimiento necesario para las aplicaciones de comercio electrónico

- **Kerberos**
- Extiende el modelo LDAP brindando privilegios de control de acceso a aplicaciones de cliente/servidor
- Ofrece uno de los más altos niveles de control de acceso de usuario y sistema disponible hoy en día
- Proporciona el sistema SSO

CONTROL DE ACCESO



CONTROL DE ACCESO
FILTRADO IP

- Utiliza un firewall o router
- Los mismos permiten o prohiben la entrada o salida de los paquetes de una red
- Para ello se basan en las direcciones IP y en los puertos de origen y destino

CONTROL DE ACCESO SOCKS - FUNCIONES

- Protocolo de una red proxy
- Autentica y autoriza requerimientos
- Establece una conexión proxy
- Transmite datos entre los hosts

PASARELAS DE PAGO

- **Ventajas para el comprador:**
  - El pago se realiza directamente en los servidores del banco
  - El número de la tarjeta viaja encriptado y sólo hacia el servidor del banco (uso de SSL)
  - El vendedor debe tener una cuenta en el banco con sus datos auténticos
  - El cliente puede elegir entre varias tarjetas de crédito dependiendo del banco que esté empleando

PASARELAS DE PAGO

- **Ventajas para el vendedor:**

  - Seguridad total para sus clientes
  - El banco correspondiente verifica que la tarjeta de crédito es real y tiene fondos suficientes
  - El cobro se ingresa al instante
  - El sistema permite cobrar a clientes de cualquier lugar del mundo

PASARELAS DE PAGO

- **Desventajas:**

  - Comisiones muy altas debido al elevado número de reclamaciones existentes

  - Posibilidad de reclamos a una entidad emisora por parte de compradores insatisfechos o maliciosos

CONTROL DE ACCESO ZONA DMZ

- **Se divide en tres zonas:**

  - **zona roja**, la más riesgosa; estaría en el dominio público donde se ubica un router de la empresa
  - **zona amarilla**, aloja los servicios tales como la Web de la empresa y los sitios FTP
  - **zona verde**, sería la intranet de la empresa controlada más firmemente

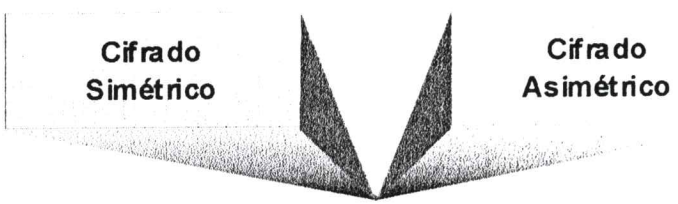
CONTROL DE ACCESO CERTIFICADOS DE USO

- Documentos electrónicos emitidos por una autoridad certificante
- Se utilizan para establecer la identidad de una empresa o persona por medio de la verificación de su clave pública
- **Autoridad Certificante:** organización confiable que aceptará su clave pública con alguna prueba de identidad; repositorio de certificados digitales

CONFIDENCIALIDAD

- Protección de la información personal y sensible
- Se logra por medio de la **criptografía**: proceso que transforma un texto legible en uno cifrado y viceversa
- Los algoritmos de encriptación se clasifican en:
  - Simétricos o de clave privada
  - Asimétricos o de clave pública

CONFIDENCIALIDAD



CONFIDENCIALIDAD CLAVE PRIVADA

- Utiliza la misma clave para encriptar y desencriptar un mensaje
- Su seguridad se basa en el secreto de dicha clave
- Utiliza dos funciones:
  - Una para realizar la encriptación
  - Otra para realizar la desencriptación

CONFIDENCIALIDAD CLAVE PRIVADA: DESVENTAJAS

- El emisor y el receptor comparten la clave
- **Ejemplos:**
  - DES (Data Encryption Standard)
    longitud de clave: 56 bits
  - AES (Advances Encription Standard)
    longitud de clave: mínimo 128 bits

CONFIDENCIALIDAD CLAVE PUBLICA

- Mayor confidencialidad a costa de mayor carga computacional
- Cada usuario tiene dos claves: una pública y una privada
- Dos forma de usar los algoritmos según la clave pública se emplee como clave de encriptación o de desencriptación

CLAVE PUBLICA COMO CLAVE DE ENCRIPTACION

- **A** utiliza la clave pública de **B** para encriptar la información que tiene que enviarle
- **C** utiliza la clave pública de **B** para encriptar la información que tiene que enviarle
- **B** utiliza su clave privada para obtener el texto legible a partir de la información encriptada
- Sólo **B** puede descifrar los mensajes enviados por **A** y **C**

CLAVE PUBLICA COMO CLAVE DE DESENCRIPTACION

- **B** encripta la información utilizando su clave privada
- Cualquiera que conozca la clave pública de **B** podría descifrar la información transmitida

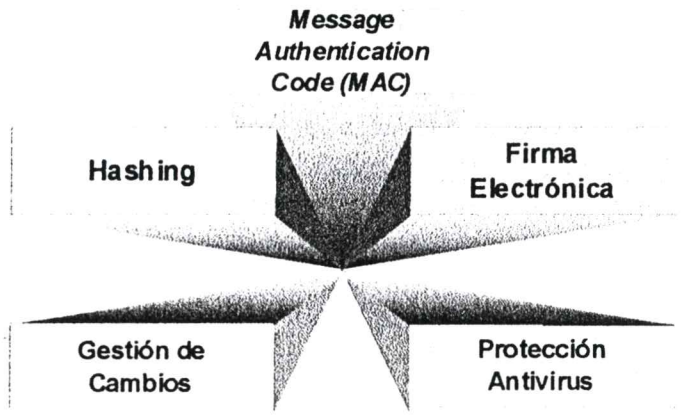
- **Ejemplos:**
  - RSA (inventado por Rivest, Shamir y Adleman en el MIT)
  - El Gamal
  - Diffie - Hellman

INTEGRIDAD

- Asegura que la información entregada no ha sido manipulada

- Toda modificación debe contar con el acuerdo de las partes según un estándard

INTEGRIDAD



INTEGRIDAD
MAC

- Programas de cómputo, llamados agentes electrónicos, que autentifican mensajes sin intervención humana
- Se utilizan con mayor frecuencia en las transacciones B2B

INTEGRIDAD
HASHING

- Uso de una función hash:
  - Convierte un mensaje, de cualquier longitud en una cadena de dígitos llamados mensaje digest o resumen
  - La longitud de la función determina la longitud del digest
  - No se requiere ninguna clave

INTEGRIDAD
FIRMA ELECTRONICA

- Firma especial utilizada para firmar correspondencia electrónica (ej.:firma digital)
- Se crea encriptando un mensaje digest o resumen con la clave privada del remitente
- Garantiza la autoría e integridad de un documento electrónico
- En Argentina, la ley de Firma Digital fue aprobada el 14 de noviembre del 2001

INTEGRIDAD
GESTION DE CAMBIOS

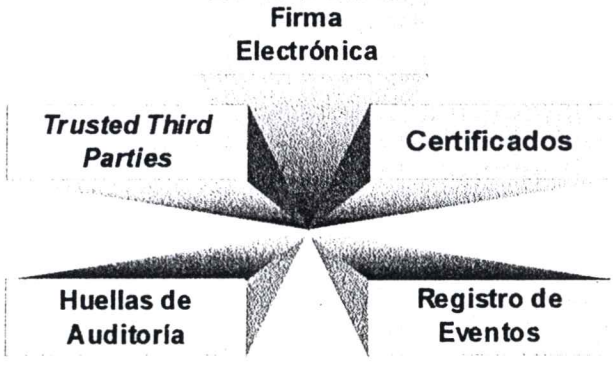
- Reacción frente a posibles ataques en el comercio electrónico

Ataques		**Medidas preventivas**
Modif.de la información	→	Firmas digitales
Enmascaramiento y espionaje	→	Autenticación Encriptación
Penetración	→	Autenticación Encriptación

NO REPUDIO

- Propiedad que se consigue por medios criptográficos (se usa la criptografía asimétrica con la autenticación y el uso de clave privada para certificar)
- Impide a una persona o entidad negar haber realizado una acción en particular relativa a datos
- Evita el desconocimiento de envío y recepción de un mensaje

NO REPUDIO



NO REPUDIO TERCERAS PARTES CONFIABLES

- Una empresa u organización confiable que aceptará su clave pública junto con alguna prueba de su identidad
- Sirve como repositorio de certificados digitales
- Otros pueden requerir verificación de su clave pública a través de estas empresas

NO REPUDIO CERTIFICADOS

- Pueden ser de usuario y de servidor seguro
- Son emitidos por terceras partes confiables *Certificado de servidor:* autentifica al servidor frente al usuario que está accediendo al mismo, pero no autentifica al puesto cliente
- *Certificado de usuario:* autentifica al cliente que se está conectando al servidor, con las funciones de firma y cifrado de los mensajes que envíe

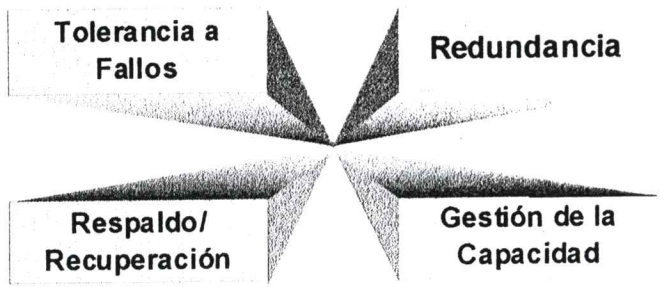
NO REPUDIO HUELLAS DE AUDITORIA

- Registros de Auditorias de Seguridad
- Actividades muy utilizadas por las empresas, especialmente las auditorias externas
- Permiten conocer el nivel de seguridad de la empresa y las acciones a emprender para corregir posibles fallos

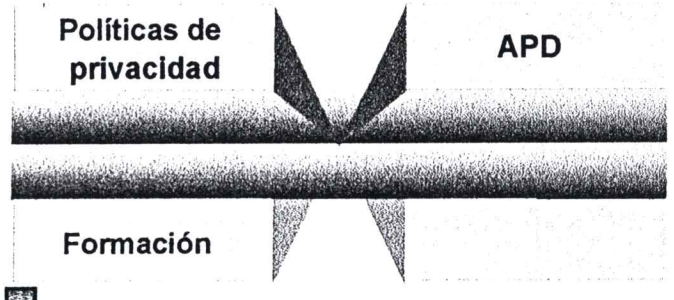
DISPONIBILIDAD

- Asegura que los recursos del sistema y la información estarán disponibles a los usuarios autorizados siempre que éstos los necesiten

DISPONIBILIDAD



PRIVACIDAD



MEDIDAS DE SEGURIDAD EJEMPLO