“Seguridad en las transacciones on line de comercio electrónico”

Tesis de Grado – Licenciatura en Sistemas de Información

Convenio UTN – ISIPER

Autor: Lic Gonzalo Ernesto Domingo

Director de Tesis: Lic Bernardo Fernández

Asesora Metodológica: Lic Graciela Mingo de Bevilacqua

Datos Personales:

Nombre: Gonzalo Ernesto Domingo

Lugar de residencia: Neuquén Capital

e-mail: gedosilvi-sol@yahoo.com

Todos los imperios del futuro van a ser imperios del conocimiento, y solamente serán exitosos los pueblos que entiendan cómo generar conocimientos y cómo protegerlos; cómo buscar a los jóvenes que tengan la capacidad para hacerlo y asegurarse que se queden en el país.

Albert Einstein

Índice

Introducción

Al iniciar este trabajo de tesis, me preguntaba: ¿cuán seguro era introducir el número de mi tarjeta de crédito en una página Web y qué probabilidades habría de ser estafado si lo hacía?

Era un usuario más, con algunos conocimientos más que algunos pocos, sobre el tema. Las siguientes eran algunas de las preguntas que me planteaba:

- ¿Qué conceptos involucra la seguridad en las transacciones on-line del comercio electrónico?
- ¿Por qué es necesario garantizar la seguridad de las transacciones de datos y su inviolabilidad?
- ¿Cuáles son las arquitecturas disponibles para garantizar la seguridad?
- ¿Cómo se puede reconocer un "sitio seguro"?
- ¿Cuáles son las diferencias entre los distintos medios de transacciones y cuáles son sus implicaciones de seguridad?
- ¿Cómo un sitio de comercio electrónico le transmite seguridad al cliente?
- ¿Qué relación hay entre la seguridad y el éxito comercial de la transacción?
- ¿Qué posibilidades tiene el usuario para determinar la seguridad de un sitio Web antes de relacionarse comercialmente con él?

Todas fueron disparadores del trabajo presente y motivaron a la investigación y estudio de los conceptos teóricos relacionados con el comercio electrónico y la seguridad. La idea fue establecer un punto de partida para posibles soluciones, luego se observaron en empresas del medio la aplicación de los conceptos desarrollados. Con esto se arribó a algunos descubrimientos y nuevos interrogantes. Las visión del trabajo surge de un mundo en recesión con el capitalismo atravesando su mayor crisis. Es necesario generar formas de co-mercio y expansión de mercados. En Internet transitan día a día millones de posibles clientes. Es un deber proveer soluciones técnicas al esfuerzo que el personal de marketing y diseño realiza para atraer la atención de los clientes. No podemos permitir que una vez captada la atención de los mismos, en un artículo determinado, la compra no se realice por falta de confianza en la seguridad del vendedor. En marketing existe un precepto que reza: **"La venta siem-**

siempre se cierra; si no la cierra el vendedor (con la concreción), la cierra el cliente (con el rechazo)"

Problemáticas de las transacciones de comercio electrónico

En 1969 el departamento de defensa de los Estados Unidos creó la Agencia para Proyectos Avanzados de Investigación (ARPA, Advanced Research Project Agency). El departamento de defensa aspiraba crear una red de comunicación de tal manera que si una parte de la misma sufría un colapso total, los mensajes pudieran encontrar el camino hasta su destino de cualquier manera, motivados por la sensación de un inminente conflicto mundial nuclear. Es quizá paradójico pero muchos de los avances de la humanidad se han logrado teniendo la idea de sacar ventajas en conflictos armados. El resultado fue ARPAnet.

En 1983, mas que nada debido a razones pragmáticas, ARPAnet se dividió en dos sistemas diferentes llamados ARPAnet y MILENET. La primera fue puesta a disposición de los ciudadanos para usos civiles, y MILENET fue reservada para uso militar. Las redes se conectaron de tal manera que los usuarios pudieran intercambiar información; esto acabó por conocerse como Internet.

Uno de los avances más importantes de Internet tuvo lugar en 1986, cuando la Fundación Nacional de la Ciencia (NFS, National Foundation of Science) de los Estados Unidos creó NSFNET con el propósito de conectar varias supercomputadoras de gran velocidad a lo largo del país, principalmente con fines de investigación. ARPAnet fue desmantelada y NSFNET se convirtió en el principal conducto de Internet.

En sus primeros días, Internet era un lugar tranquilo donde no se hacia mucho más que mandar mails o intercambiar archivos. Era utilizada para diseminar información pública de universidades y organizaciones. Los navegadores[1] y la Web[2], como los conocemos hoy, no existían. El servicio WWW de Internet, el responsable de su gran expansión global y popularidad gracias a las facilidades multimediales, no hizo su aparición hasta 1992. El world wide Web fue inventado por Tim Berners-Lee, el mismo fue concebido como un medio para publicar documentos relacionados con la física sin tener que descargar los archivos e imprimirlos. El www no alcanzó gran popularidad hasta que en la

[1] En Inglés Browser. Es un software que sirve para visualizar páginas de Internet.

[2] Forma abreviada de World Wide Web, servicio de Internet, también llamado www.

Universidad de Illinois se desarrolló un navegador Mosaic, programa luego conocido como Netscape Navigator. [L-1] [L-2] [L-9] [W-8]

La información en la Web se despliega como un conjunto de páginas escritas en Lenguaje de Marcación de Hiper Texto (HTML, Hyper Text Mark Up Language), almacenadas en servidores Web, término utilizado tanto para describir las computadoras que alojan las páginas Web como a los programas que reciben peticiones de la red y responden en forma de archivos HTML. Estas páginas se solicitan y reciben mediante mensajes definidos por el Protocolo de Transporte de Hiper Texto (HTTP, Hyper Text Transport Protocol). Además de transmitir un archivo un servidor Web puede ejecutar un programa como respuesta a una petición esto se puede realizar a través del lenguaje Interfaz de Compuerta Común (CGI, Common Gateway Interface). Esta interfaz simplifica al servidor algunas operaciones complejas pero no es eficiente, ya que requiere la ejecución de programas independientes por cada llamada; una técnica mejor en la que el mismo servidor realiza la operación externa es la de Interfaz de Programación de Aplicaciones (API, Application Programming Interfaces). [L-1]

La Web agrupó todos los servicios de Internet que antes estaban separados y les da un entorno capaz de combinar imágenes, texto y sonido.

"Una de las leyes fundamentales de la seguridad informática dice que el grado de seguridad de un sistema es inversamente proporcional a la operatividad del mismo". [W-21]

Internet es una red de grandes servidores en configuración de cliente - servidor[3] conceptualmente insegura, ya que fue diseñada con un alto nivel de operatividad. No está mal que sea insegura, ni se trata de un error de diseño, sino que para cumplir con la función para la cual se la creó debía tener el más alto grado de operatividad, lo que trae como consecuencia un alto nivel de inseguridad.

Podemos decir que la seguridad e Internet son conceptualmente opuestas. A lo que se le puede dar un grado de seguridad mediante un determinado mecanismo, es a una transacción específica, y este mecanismo se debe repetir cada vez que se lleve a cabo una operación similar.

No ha de creerse que por implantar determinados mecanismos de seguridad automáticos, Internet se vuelve segura. Esto se afirma en

"Una cadena es tan fuerte como su eslabón más débil"

Por lo que cuando se conectan dos sistemas, uno seguro y otro inseguro, el grado de seguridad no se promedia, sino que pasa a ser el del más inseguro para todo el sistema.

Definición del problema

Mientras Internet, crece rápidamente, aumenta el intercambio de datos. Muchas empresas realizan transacciones financieras con sus clientes en Internet y necesitan asegurarse que sus transacciones sean privadas y de confianza.

Hacia fines del 2002, asistimos al auge y caída de los negocios en Internet. La gran mayoría de las empresas dedicadas al comercio electrónico fracasaron y se vaticinó la muerte de las punto com.

Sólo los que hicieron un buen plan de negocios siguen en marcha y los que han fracasado fueron megaproyectos que apostaban a imponer sus marcas y rentabilizar su inversión mediante anuncios publicitarios.

Lo más utilizado actualmente en el comercio electrónico es el e-mail, como herramienta para oferta segmentada a un costo bajísimo.

Según la consultora Carrier y Asociados [W-20], en su publicación Internet en Argentina: Cuantificación y Perfil de usuario, "el mercado argentino de usuarios de Internet mostró un crecimiento del 15%, con lo que, a diciembre de 2002, llegó a alrededor de los 4 millones de usuarios." Lo que es equivalente a 2 veces la audiencia de AM, 39 puntos de rating o 2 veces la cantidad de lectores de diarios. Por su parte la consultora D´Alessio IROL [W-25] publicó en su sitio web que "contrariamente a lo que se piensa, Internet no es un ámbito principalmente formado por adolescentes, ya que el 82% tiene más de 24 años" y "los segmentos de mayor nivel socioeconómico son los que ocupan el lugar más importante dentro del perfil de usuarios, aunque los niveles medios están equiparándolos en su peso numérico" del total de usuarios de Internet, el 46% ocupa cargos de jefaturas, gerencias o dirección. Esto abre más que nunca una oportunidad de negocios on line. El mercado potencial es enorme y sigue creciendo. Aunque es imposible precisar la cantidad, la Asociación para la Investigación de Medios de Comunicación de España (AIMC) aventura que en

[3] Arquitectura en la que cada equipo de computo que participa, sirve recursos o los aprovecha. A las primeras se les denomina servidores. A las otras computadoras se las llama clientes y son quienes consumen el contenido o la información ofrecida por los servidores.

todo el mundo somos unos 160 millones de usuarios. Todos los días se incorporan miles de nuevos navegantes que no quieren saber nada de caídas de Nasdaq, ellos desean una Internet que cubra todas sus expectativas y la problemática es que queden satisfechos y que consuman. Pero esto no se produce. La consultora D´Alessio IROL [W-25] asegura que del total de usuarios de Internet que **NO** compran online, el 52% prefiere no hacerlo por desconfianza a los medios electrónicos de pago. Pese a que a la hora de buscar información sobre un producto, el 82% de los usuarios considera a Internet el medio más confiable; de forma que el 75% de los usuarios de Internet han efectuado consultas a servicios y/o productos online pero solo el 15% efectuó alguna transacción. El cliente, frente al comercio electrónico, se siente solo, sin ayuda a la hora de hacer consultas, con una gran desconfianza hacia la tecnología y pensando que toda la población de maliciosos hackers está esperando que él ingrese sus datos para hacer todo tipo de estragos. Temeroso, apaga su PC, hace una lista de compras manual y sale hacia la tienda a hacer las compras personalmente.

Definiciones de Comercio Electrónico

- **"Es la aplicación de la tecnología de información avanzada para incrementar la eficacia de las relaciones empresariales entre socios comerciales"** [W-23]

- **"La disponibilidad de una visión empresarial apoyada por la tecnología de información avanzada para mejorar la eficiencia y la eficacia dentro del proceso comercial."** [W-24]

Combinando estas definiciones podemos decir que el comercio electrónico es una metodología moderna para hacer negocios que se apoya en la tecnología informática.

Su éxito radica en que está en sintonía con la necesidad de las empresas, comerciantes y consumidores de reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los mismos.

¿Es seguro el comercio electrónico?

Pregunta que muchos usuarios se hacen antes de ingresar en un medio que les parece al menos impersonal, y al que deben entregar datos tan privados como los de su tarjeta de crédito.

Es importante tener en cuenta que no existe sólo una forma de comercio en la Red. Hay miles y miles de páginas Web que ofrecen artículos o servicios a través de Internet y también son cientos de miles las transacciones de datos

que se realizan, pero se ha difundido un gran miedo sobre la inseguridad que ofrecen las transacciones por Internet y en particular las que se llevan a cabo mediante tarjetas de crédito. Es apreciable que se corre tanto riesgo en el mundo "real", como en Internet. Por ejemplo en un restaurante: cuando el mozo se lleva nuestra tarjeta, él mismo puede copiar sus datos y luego utilizarla en Internet o en otro comercio. Otro ejemplo es en las compras telefónicas donde transmitimos vía oral los datos de la tarjeta que pueden ser fácilmente interceptados o incluso malversados por la empresa en que confiamos, aunque indiscutiblemente la interacción con una voz humana nos da una tranquilidad que será difícil reemplazar.

En Internet hay sitios de transacción con facilidades criptográficas en los cuales la información que enviamos se transmite de tal manera que si alguien la intercepta solo verá ceros y unos entreverados porque la información ha sido cifrada para que resulte ilegible a un interceptor (a este proceso se le llama encriptación). Esta condición es indicada en los navegadores por un símbolo gráfico para poder detectar si un sitio ofrece estas facilidades. Otra forma de hacer una transacción con tarjeta de crédito es enviar los datos de la misma por fax, este método se usa generalmente para evitar que la información viaje por Internet y tiene la ventaja que la persona que envía los datos se queda con una copia firmada de la transacción. Esta última es de uso difundido en países donde no puede haber una transacción comercial sin una firma de la persona que adquiere el bien o servicio.

Existen, por supuesto, otras formas de pago ya que la idea de hacer transacciones sólo a través de tarjetas de crédito está ampliamente difundida en los Estados Unidos (allí este medio es casi tan común como el documento de identificación) pero excluye a muchos potenciales clientes del resto del mundo; estos son los giros postales o bancarios que ofrecen total seguridad en cuanto al envío y recepción de dinero.

Empresas como Western Union y DHL con sucursales en más de 100 países son una solución práctica y cercana (hay sucursales hasta en farmacias) a la hora de realizar transferencias de montos pequeños.

Para transacciones de montos mayores se justifica el ya legendario y engorroso giro bancario.

Otro punto importante a la hora de realizar una transacción, sea del tipo que sea, es verificar la seriedad de la empresa, ya sea solicitando referencias de sus clientes u observando su evolución y presencia en Internet.

Por lo antes expresado, vemos al comercio electrónico como una realidad que puede tener distintas formas y que seguramente tendrá un crecimiento enorme en el futuro de la Informática.

Las inquietudes a develar con el trabajo de tesis son numerosas y serán tomadas como puntos de partida de la investigación.

Hoy, el gran tema en la informática, pasa por la seguridad ya que con el crecimiento desmesurado que ha tenido, también se expandieron los agujeros de seguridad y la tendencia al caos. Intentamos brindar un humilde aporte al tema y lograr una referencia a la hora de solucionar un problema concreto que existe en el mundo de la Informática.

Una de las principales dificultades al escribir sobre la seguridad en la Web es que esta área es increíblemente dinámica. Por esta razón en lugar de proporcionar información técnica detallada acerca de la instalación y configuración de programas específicos, los cuales serán obsoletos terminada la lectura de este trabajo de tesis, se ha incluido información sobre los conceptos y técnicas que son y serán aplicables en los años venideros.

La estructura de la presente tesis es la siguiente

La parte 1, a continuación, está dedicada a introducir los conceptos del comercio en la Web.

Se abordan los temas relacionados con la privacía de los datos en la era tecnológica actual, su tratamiento, legislación vigente y particularmente el delito informático. Se realiza un acercamiento a los conceptos de seguridad Web. Se presentan los motivos que llevan a atender esta problemática y qué tecnologías se utilizan en defensa de los servidores Web. Adicionalmente se tratan los medios de pago que soportan al comercio electrónico.

En la parte 2 se describen las tecnologías de protección de datos y la privacidad del cliente.

Se detallan las políticas de seguridad que debieran ser parte de la ética que un sitio Web de comercio electrónico mantiene hacia sus clientes. Se realiza un acercamiento a los conceptos involucrados en las técnicas de identificación digital y firma electrónica. También se muestra el uso de los certificados digitales, cómo medio de lograr que los clientes sientan la confianza necesaria para realizar transacciones que impliquen el intercambio de datos sensibles.

Se explican los conceptos involucrados en la criptografía, cómo pieza importante de la seguridad en la Web.

Trataremos la problemática de proteger un sitio Web, qué soluciones arquitectónicas se pueden implementar y cuales son sus diferentes implicancias.

Por último, en la parte 3, abordamos la problemática de llevar a la práctica los conceptos vistos y cómo trazar una hoja de ruta para recorrer en la construcción de un sitio Web de comercio electrónico. También realizamos una encuesta entre un grupo de profesionales de la informática y analizamos sus resultados, comparando los mismos con algunos trabajos sobre el mercado informático y el comercio electrónico.

Finalmente se exponen las conclusiones del presente trabajo.

Parte 1
Introducción al Comercio en la Web

En el presente capítulo se introducen los temas relacionados con el comercio en la Web. La privacía de los datos, su tratamiento y legislación vigente; y particularmente el delito informático. Se realiza un acercamiento a los conceptos de seguridad Web. Se analizan los motivos que llevan a atender esta problemática y qué tecnologías se utilizan en defensa de los servidores Web. Adicionalmente se tratan los medios de pago que soportan al comercio electrónico.

Comercio en la Web

En marzo de 1997 surgió una nueva clase de amenaza en la Web, Paul Greene [L-9] descubre que una página Web con ciertas instrucciones especiales podía engañar al navegador Internet Explorer[4], de Microsoft, y hacer que ejecutara cualquier programa con cualquier entrada en la computadora del usuario. Este error podría ser utilizado para destruir la computadora de la víctima, infectarla con un virus o capturar información confidencial del disco duro. El error le otorgaba al Webmaster[5] el control total sobre cualquier computadora que visitara un sitio con Internet Explorer. A las 48 horas de haber sido detectado este error, Microsoft publicó una corrección al mismo, demostrando tanto la habilidad de la compañía para responder y la efectividad de la Web para distribuir correcciones de errores. A pesar de esto, a los pocos días se descubre otro error en Internet Explorer con el mismo efecto destructivo. Estos errores no son solamente de Microsoft, paralelamente se descubrían errores en el ambiente de Java, de Sun Microsystems, incluido en Navigator de Netscape.

Por otro lado, el gobierno de Massachusetts había anunciado que los conductores podían pagar sus infracciones mediante la Web. Debían dirigirse al sitio Web del Registro de Vehículos Automotores, hacer clic en un botón determinado y pagar la infracción con el número de su tarjeta de crédito. Evitando de esta forma tener que perder tiempo haciendo cola para el pago.

Para que el trámite con tarjetas de crédito sea seguro en Internet, el gobierno aseguraba utilizar un servidor Web “seguro”. Pero con “seguro” se refería a la conexión entre el servidor Web y el navegador, es decir, que el primero utiliza protocolos criptográficos de manera tal que al enviar un número de tarjeta de crédito por Internet, se codifica de modo que no pueda ser interceptado en su recorrido. Pero solo por utilizar criptografía para enviar números de tarjetas de crédito por Internet no significa que sea inviolable. En el caso de que alguien logre acceder a la computadora con fines delictivos, podría instalar programas en el servidor y así obtener los números de tarjeta de crédito una vez decodificados. Obteniendo estos números, podría utilizados para cometer fraudes. Esto podría llevar meses para que las compañías emisoras de las tarjetas

[4] Aunque existe una gran diversidad de navegadores de Internet, en este trabajo citaremos siempre al Internet Explorer ya que es el más usado. El mismo viene con el sistema operativo Windows a partir de su versión 95 IE. Aunque en ocasiones se harán comparaciones con el Navigator de Netscape que tiene similares características y similares falencias de seguridad.

[5] Forma en que se suele llamar al líder de proyecto de un sitio Web.

localicen la fuente del robo de los números, al tiempo que los maleantes habrían cambiando de víctima. [L-9]

La seguridad en la Web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios de la Web contra el comportamiento inesperado.

Las empresas y los gobiernos utilizan cada vez mas el World Wide Web para distribuir información importante y hacer transacciones comerciales. Al violar servidores Web se pueden dañar reputaciones y perder dinero. A pesar que la Web es fácil de utilizar, los servidores y navegadores Web son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales. Muchas veces se han incorporado funciones sin prestar mucha atención a su impacto en la seguridad. Aunque el software esté bien instalado puede ser una amenaza de seguridad. Al violar los navegadores y servidores Web, los atacantes pueden utilizarlos como base para otros ataques. También existen muchos usuarios principiantes de los servicios basados en el WWW. La generación actual de software les exige tomar decisiones de seguridad relevantes a diario, sin proporcionarles información suficiente.

Por lo expresado es que atendemos el tema de seguridad en la Web, con la seguridad de que es más costosa la recuperación de un incidente de seguridad que tomar medidas preventivas. [E-1]

La información en la Web

La vida privada[6] y las nuevas tecnologías nunca se han llevado bien, ya que siempre se han ideado formas de espiar a nuestros semejantes. Las autopistas de la comunicación han supuesto una revolución en nuestro concepto de intimidad, debido a que a lo largo de nuestra vida dejamos cientos de datos, registros y firmas que se van acumulando. Si alguien pudiera tener acceso a ellos, podría reconstruir fielmente nuestro perfil vital.

En cada etapa de nuestra historia, vamos dejando huellas en nuestros actos cotidianos. Por ejemplo, la toma de huellas y datos en el Registro Civil, datos sobre sucesivas vacunaciones y enfermedades, inscripción en el colegio, datos de participación en concursos y en ofertas comerciales, ingreso a la universidad, ingreso en el padrón electoral, conexión a Internet, registro de casa-

[6] Se incluye en el concepto privacidad dos supuestos: el derecho de cada persona a no ser perturbado en su soledad y el derecho a que no se divulguen datos que puedan perjudicarla.

miento y divorcio, carnet de conducir, créditos hipotecarios, datos bancarios, compras con tarjetas de crédito, registros judiciales y policiales, etcétera.

El vivir rodeados de rastros, nos genera algunos deberes como el que obliga, según la Ley 17.671 en la República Argentina, a comunicar el cambio de domicilio dentro de los treinta días de haberse producido. Entre los derechos, aquel que establece la propia Constitución Nacional, denominado Habeas Data, que declara que " todos los habitantes de la Nación Argentina tienen derecho a conocer los datos que las autoridades poseen respecto de su persona".

En el artículo 43 de dicha constitución [W-22], se establece la acción de amparo, siempre que no exista otro medio judicial más idóneo, para ser interpuesta por cualquier persona para tomar conocimiento de los datos referidos a ella y su finalidad, sea que éstos consten en registros públicos o privados. La acción es igualmente válida para exigir la supresión, rectificación, confidencialidad o actualización de los datos, cuando éstos sean falsos o discriminatorios.

Cuando la revelación incompleta de datos es engañosa y no coincidente con la realidad, el interesado tiene el derecho constitucional de exigir la rectificación o actualización de los antecedentes que sobre su persona se brindan a terceros.

El derecho de poder controlar a quienes difunden información personal, es un derecho fundamental porque de no existir la posibilidad de lograr judicialmente la rectificación de los datos falaces acerca de una persona, se afectan directamente derechos constitucionales, tales como el derecho a la privacidad, al honor, a la identidad personal y a la propiedad, con todos los perjuicios económicos y morales que ello puede acarrear para la persona involucrada.

La ley 25.326 de hábeas data reglamenta el derecho de todo ciudadano argentino a exigir se le haga saber que tipo de información se tienen sobre él en cualquier base de datos pública o privada.

Tratamiento de los datos

Si bien no existen disposiciones específicas sobre el resguardo de datos en la Web, esto no significa que quede excluida su protección.

Es importante tener en cuenta que la información acerca de un individuo se compone de diferentes tipos de datos que se muestran en la figura A y se detallan a continuación. [W-24]

a) **Datos sensibles**: Son los que pueden afectar la intimidad del individuo como son el de raza, ideología, estado de salud, creencias, religión.

b) **Datos secretos**: como son el secreto profesional, secreto comercial, secreto bancario, secreto de confesión, etc.

c) **Datos reservados**: siendo aquellos que el titular no está obligado a proporcionar para que sean conocidos por terceros, como son : filiación (hijo matrimonial, extramatrimonial, adoptado), delitos contra el honor (difamación, calumnia, injuria), libertad sexual (violación), adulterio, aborto, etc.

d) **Datos privados**: los que el titular debe proporcionar periódicamente a la autoridad para fines específicamente señalados, como por ejemplo los datos contenidos en una declaración jurada del impuesto a las ganancias, sólo deben ser utilizados para los fines que específicamente fueron dados, no para fines distintos.

e) **Datos públicos**: Son aquellos cuya publicación no afecta al individuo, como el sexo, número de documento, nombre y apellido. Los datos que figuran en los padrones electorales o en la guía telefónica.

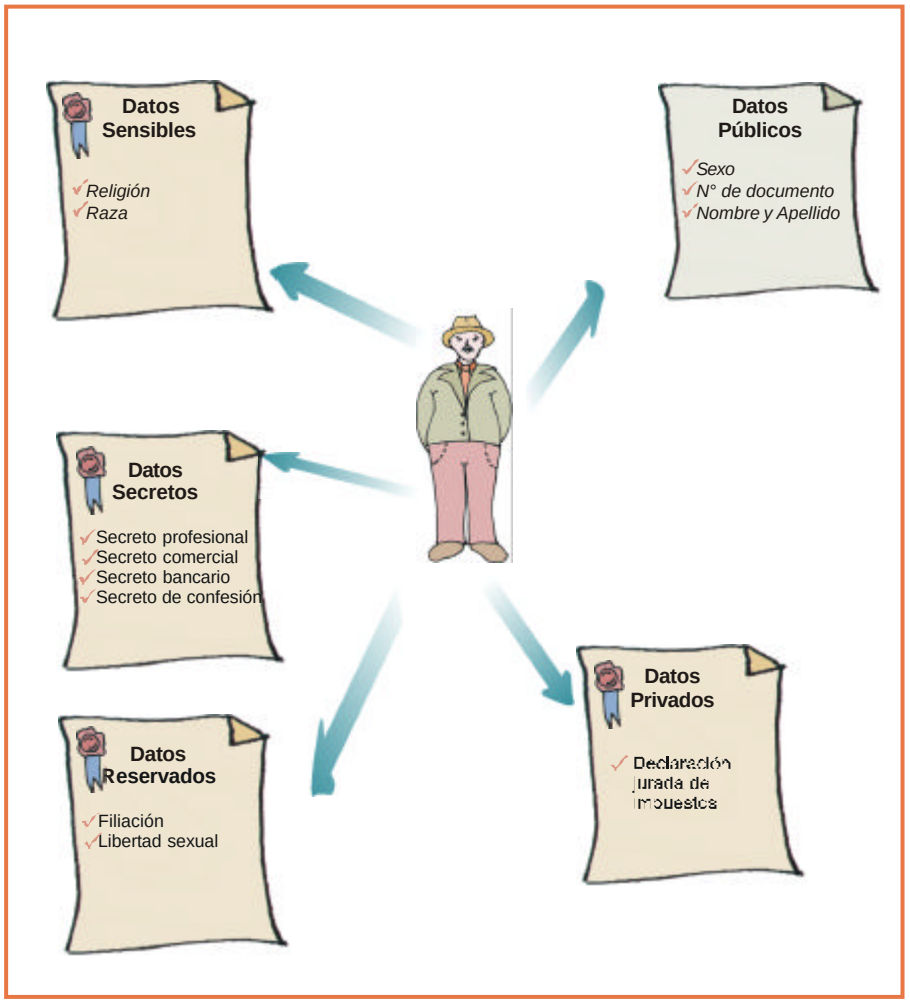


Figura A.: Tipos de datos.

Estos tipos de datos determinan que la información pueda o no ser tratada como confidencial, también debe tenerse en cuenta los límites territoriales de aplicación de la ley argentina, que puede no emplearse si el usuario local brinda información sensible a sitios extranjeros que la divulgan. No hay una pauta única para determinar cuándo una información debe considerarse confidencial; depende de las circunstancias. Datos como nombre, domicilio, dirección de e-mail o número de teléfono no necesariamente constituyen información sensible ya que su divulgación no vulnera el derecho a la intimidad. Pero si esos mismos datos son tomados en conjunto o procesados para inferir características, tendencias o perfiles de sus titulares, bien podrían constituir información confidencial y sensible. Además, pocos dudarían que los números de tarjeta de crédito, ingreso patrimonial, antecedentes penales y de evaluación crediticia, tendencias sexuales y creencias políticas y religiosas, no sean datos cuyo uso pueda afectar al individuo en su intimidad.

Las empresas que operan en Internet están en una situación privilegiada para obtener información personal de los usuarios, y ninguna ley les impide recopilar sus datos y utilizarlos para fines propios de marketing u otros. Este uso sería contrario a la lealtad contractual y, aunque no es sancionado por la ley, habilita a los afectados a reclamar la indemnización de los daños ocasionados. Es recomendable, entonces, que el usuario se interese por la política de confidencialidad de los sitios y, a su vez, que éstos soliciten el consentimiento del usuario antes de divulgar sus datos personales.

En los últimos años un creciente tráfico de archivos, con datos sensibles sobre los usuarios, se ha hecho moneda corriente en Argentina. Pero no había ningún instrumento legal creado para castigar este tipo de delitos.

Entre las principales características de la ley, se cuenta la creación de un organismo estatal que controlará este tipo de delitos en empresas y organismos públicos. Tendrá a su cargo un censo, que habilitará a las empresas inscriptas con un permiso habilitante para guardar datos sobre sus clientes, siempre y cuando no violen su privacidad. Si alguien hace una denuncia porque considera que se han utilizado datos sensibles sobre su persona sin su consentimiento, la oficina investigaría y podría multar a la compañía. Además, se prevé penas de prisión por 3 años como máximo para aquellos que introduzcan información falsa a propósito en una base de datos.

Uno de los puntos conflictivos en estos años han sido la gran cantidad de personas que han denunciado errores en los bancos de datos comerciales. Este problema las inhabilitaba para recibir créditos, aún cuando no tenían ni-

guna morosidad. Por ello, la ley establece que las entidades financieras deberán blanquear todos esos errores.

Los archivos de los medios de comunicación quedaron explícitamente fuera del alcance de la ley, para proteger el derecho de los periodistas a reservar sus fuentes de información.

En la iniciativa legal se explicita que los datos sensibles no pueden ser almacenados de ninguna forma y que toda persona debe ser notificada cuando sea incluida en una base de datos.

La protección de datos personales no es un problema nuevo, pero la Red potencia el riesgo implícito al facilitar la comunicación y el almacenamiento.

El código civil impone el deber de reparar el daño causado por intromisión en la intimidad ajena. En materia comercial, la ley de confidencialidad prohíbe la divulgación, adquisición o utilización indebidas de información de valor comercial, en atención a su carácter secreto. La ley de habeas data aún espera su reglamentación. Toda persona, tiene el derecho de conocer cuáles de sus datos se incluyeron en registros y bancos de datos públicos o en registros privados y de pedir su supresión, rectificación, confidencialidad o actualización.

Uno de los frenos más grandes para el comercio electrónico es la desconfianza generalizada a la hora de dar los datos de la tarjeta de crédito, por temor a que se agreguen a la cuenta cosas que no se compraron o que el producto no llegue a destino final. Los consumidores están desconfiando de la tecnología y del sistema de medios de pago. Y no nos referimos a la desconfianza comercial acerca de quién es el que vende y qué es lo que vende. Esto se sostiene con los relevamientos y con las comprobaciones prácticas que se hacen en la Argentina. Es evidente la necesidad de una seguridad jurídica por parte de los inversores y de las empresas. Si el marco económico no es seguro, la gente no realiza emprendimientos.

Dejamos en claro que los registros que administran antecedentes personales tienen obligaciones ineludibles como obtener los datos por vías legales, conservarlos en secreto, tener información cierta, completa, actualizada y proporcionarla sólo cuando media la orden de una autoridad competente o cuando la persona involucrada ha autorizado su revelación para el caso concreto.

El incumplimiento de las obligaciones referidas convierte a la administración de datos en manipulación, siendo esta última, ilegal. Se afirma que el espí-

ritu de las garantías constitucionales que involucran la cuestión analizada, es que los actos privados de los hombres permanezcan preservados, que haya una esfera de intimidad o privacidad y que la información que se difunde no perjudique injustamente el goce de derechos. Pero más allá de los problemas legales, nos motiva la seguridad del negocio. Aún no se ha denunciado un caso de estafa comercial importante, pero si llegara a pasar los daños en la credibilidad del sistema de comercio electrónico podrían ser irreversibles. Acabarían comercialmente, de hecho, con la empresa afectada y dañarían a todo el mercado.

"En algunas empresas es necesario que las cosas ocurran al menos una vez para que se planifiquen acciones a seguir". [E-1]

Servidor Web Seguro

La definición de servidor Web seguro depende de quién sea el receptor:

?? Para los proveedores de software es un programa que instrumenta protocolos criptográficos, de forma que la información transferida entre un servidor y un navegador no pueda ser interceptada.

?? Para los usuarios es el que resguarda la información personal que se reciba, asegurando la privacía sin instalar en su computadora programas hostiles.

?? Para las compañías que lo administran es el que resiste ataques internos y externos.

Un servidor Web seguro es todo esto y más. Es un servidor confiable, con respaldo, que en caso de fallar puede restablecerse con rapidez. Es expandible de forma que pueda dar servicio a grandes cantidades de tráfico.

Aunque la criptografía es ampliamente reconocida como prerrequisito para el comercio en Internet no es ni estrictamente necesaria para la seguridad en la Web, ni suficiente para garantizarla. Por ello, en este trabajo de Tesis se utilizará el término Web con facilidades criptográficas para denominar a un servidor Web que instrumenta protocolos criptográficos, ya que como veremos la seguridad en la Web es mucho mas que la protección contra la intercepción.

¿Por qué atacar un servidor Web?

A continuación se analizan algunas de las razones que llevan a los atacantes a querer introducirse en un servidor Web.

?? **Publicidad:** Un sitio Web es la cara visible de una empresa al mundo, y el violar la seguridad de un espacio visitado por cientos de miles de personas en pocas horas, es atractivo para atacantes ideológicos.

?? **Comercio:** Muchos servidores Web están relacionados con el comercio y con dinero. Por esta razón los protocolos criptográficos integrados a Navigator de Netscape y otros navegadores fueron originalmente incluidos para permitir a los usuarios enviar números de tarjetas de crédito por Internet sin preocuparse de que fueran interceptados. Así los servidores Web se han convertido en repositorios de información financiera confidencial, blanco interesante para los atacantes. Además los servicios comerciales que prestan también los tornan interesantes.

?? **Extensibilidad de los servidores:** Debido a su naturaleza, los servidores Web están diseñados para ser extensibles, lo cual hace posible conectarlos con bases de datos, sistemas heredados y otros programas que se ejecutan en la red de una organización. Si no se implementan de modo adecuado, los módulos que se agregan a un servidor Web pueden comprometer la seguridad de todo el sistema.

?? **Extensibilidad de los navegadores:** Además de poder extender los servidores Web, también los clientes Web pueden serlo. Las aplicaciones auxiliares pueden enriquecer la experiencia de la Web con diversas características nuevas que no son posibles utilizando solo el lenguaje HTML. Por desgracia, estas tecnologías también pueden revertirse y ponerse en contra del usuario del navegador, muchas veces sin su conocimiento.

?? **Soporte complicado:** Los navegadores necesitan servicios externos como Servicio de Nombres de Dominio (DNS, Domain Name Service) y el enrutamiento del Protocolo de Internet (IP, Internet Protocol) [7] para funcionar bien. La solidez y confiabilidad de tales servicios pueden ser desconocidas y vulnerables a errores de programación, accidentes y subversión. La subversión de un servicio de más bajo nivel puede causar problemas también a los navegadores.

?? **Ritmo de desarrollo:** El crecimiento explosivo del comercio electrónico y del WWW ha sido empujado (y a su vez empuja) por un ritmo frenético de innovación y desarrollo. Los proveedores liberan nuevas características y plataformas de software, muchas veces prestando mínima (o nula) atención a

[7] Computadoras especiales llamadas enrutadoras, usan un protocolo de Internet para mover bits de información a través de Internet. Cada paquete de información cuenta con la dirección IP tanto de la computadora que lo envió como de la que recibe el paquete. Una dirección IP es un número de identificación único de la computadora tal como es reconocida por las demás computadoras en Internet.

la verificación[8], diseño y seguridad adecuados. El mercado presiona al usuario a adoptar las nuevas versiones a fin de permanecer competitivos. Sin embargo, estos programas pueden no ser compatibles con las prestaciones anteriores o contener vulnerabilidades desconocidas para el público en general.

La solución a estos problemas no es desdeñar la tecnología de la Web sino, por una parte, comprender sus limitaciones y, por la otra, adoptar medidas de seguridad adecuadas.

Componentes de la seguridad en la Web

Los tres siguientes elementos componen la problemática de proteger sitio Web: [E-1]

?? **Asegurar el servidor y los datos que contiene:** el servidor debe poder continuar operando y la información que en él reside debe ser modificada sólo por quienes poseen la autorización y ser distribuida sólo a quienes se desee distribuir. Para asegurar la computadora en sí, se deben utilizar técnicas tradicionales de seguridad computacional garantizando a los usuarios, autorizados del sistema, las capacidades necesarias para hacer su trabajo y sólo esas capacidades.

?? **Asegurar la información que viaja entre el servidor Web y el usuario:** esta información no puede ser leída, modificada ni destruida por terceros. Asegurar físicamente la red de forma que la intercepción sea imposible sería utópico debido a su costo, las soluciones pasan por ocultar la información que se desea asegurar dentro de la información que parece no tener importancia. Esto es encriptar la información de forma que no pueda ser decodificada por nadie que no posea la llave correcta.

?? **Asegurar la computadora del usuario:** garantizar que la información, datos o programas descargados no causarán daños a los usuarios. Las fallas de seguridad en los navegadores puede permitir que los usuarios descarguen programas hostiles que pueden permanecer inactivos hasta que se teclee, por ejemplo el número de una tarjeta de crédito, capturar la misma y enviar esta información a través de Internet.

Es también un reto de seguridad verificar la identidad del usuario al servidor, verificar la identidad del servidor al usuario, asegurar que los mensajes

[8] La revisión del diseño es una tarea fundamental ya que los diseños, como el buen vino, debe estacionarse, decantarse y fermentarse antes de ser consumible. Muchas veces somos renuentes a revisar nuestros diseños y replantearnos los problemas, pero ¿subiríamos a un avión donde el ingeniero aeronáutico tuvo pereza de revisar sus diseños? El rediseño y replanteamiento debe formar parte del cronograma de cualquier proyecto informático.

enviados entre cliente y servidor sean oportunos, confiables y sin repeticiones, llevar bitácoras y auditar información sobre las transacciones, equilibrar la carga sobre los servidores.

Tarjetas de crédito viajando por la Web

La tarjeta de crédito es un método de pago que permite transferir valor sin transmisión de objetos físicos. No es una idea nueva, el crédito es mencionado en escritos que datan del año 1750 a.c., la noción moderna de crédito al consumidor es de principio del siglo XIX y aparece junto con el liberalismo económico de Adam Smith. En Estados Unidos, país donde el crédito se ha convertido en uno de los instrumentos de pago más utilizados, se empezó a popularizar después de la Guerra Civil, cuando las compañías manufactureras de máquinas de coser comenzaron a vender en pago a plazos.

La tarjeta de crédito moderna no existió hasta 1949, cuando Alfred Bloomingdale, Frank McNamara y Ralph Snyder concibieron la idea de establecer una posibilidad de crédito que sirviera para viajar ya que si bien el retirar productos de lugares donde uno era conocido se había popularizado en los Estados Unidos, era imposible comprar sin dinero o cheques en lugares donde uno no era conocido y esto era un problema a la hora de hacer viajes de negocios donde una persona debía pagar restaurantes y hoteles. Surgió así la tarjeta Diner's Club (Club de los Comensales).

Hoy en día existen miles de tarjetas de pago, algunas emitidas por una sola institución financiera, otras funcionan como grandes organizaciones de membresía en donde en realidad la tarjeta es otorgada por un banco miembro. Los bancos imponen tasas de interés sobre el crédito otorgado y contratan a una empresa procesadora de tarjetas bancarias para que mantenga la cuenta de clientes y comerciantes. El servicio que otorga la organización de membresía (Visa o MasterCard) es el establecimiento de políticas y la operación interbancaria.

Las tarjetas de crédito son la forma más popular para pagar servicios u objetos en la Web en la actualidad, como lo demuestran estudios realizados sobre el comercio en la red por Global Concepts [W-13] por ello en lugar de intentar buscar un sistema que la sustituya, la mayoría de los sistemas de compra en Internet, utilizan las tarjetas de crédito.

La protección del número en tarjetas de crédito para transacción en línea es un ejemplo típico de la necesidad de la seguridad de la Web. La Figura B,

muestra un ejemplo de una transacción con tarjeta de crédito en la Web para observar los riesgos.

Un sujeto **A** utiliza su computadora para conectarse con un almacén de música en la Web, navega por el catálogo de discos, encuentra uno que desea comprar y crea la orden de pedido. Ingresa su nombre, dirección, número de tarjeta de crédito, fecha de vencimiento de la misma y presiona un botón para enviar el pedido.

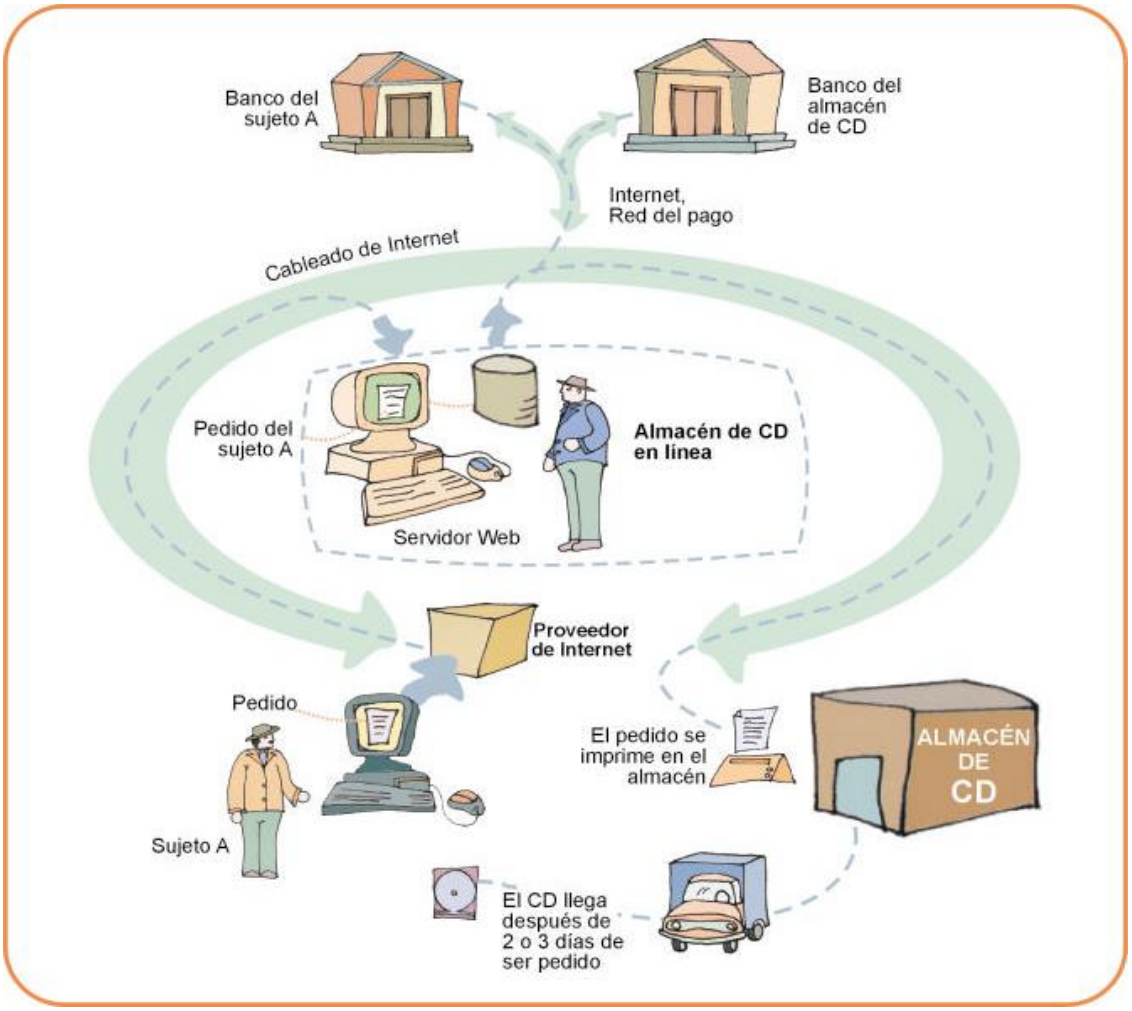


Figura B.: Compra de un CD con tarjeta de crédito a través de Internet.

Tanto el tarjeta habiente como el comerciante enfrentan riesgos en esta transacción, para el tarjeta habiente son dos riesgos obvios:

?? El número de su tarjeta de crédito puede ser interceptado y utilizado para hacer fraudes, de lo cual el sujeto no se percataría hasta que reciba su estado de cuenta o hasta que su tarjeta quede sobregirada.

?? Podría hacerse el cargo a la tarjeta de crédito pero nunca llegar el pedido, cuando el sujeto **A** investiga la página Web ya no existe y no puede localizar a la compañía que le realizó el cobro.

Luego veremos métodos diseñados para combatir estos dos riesgos utilizando una técnica matemática para revolver la información conocida como encriptación y soportando un complejo sistema de identificación digital. El sujeto **A** tiene la certeza de que detrás de la página Web del almacén de música están las personas que son quienes dicen ser, como se muestra en la Figura C.

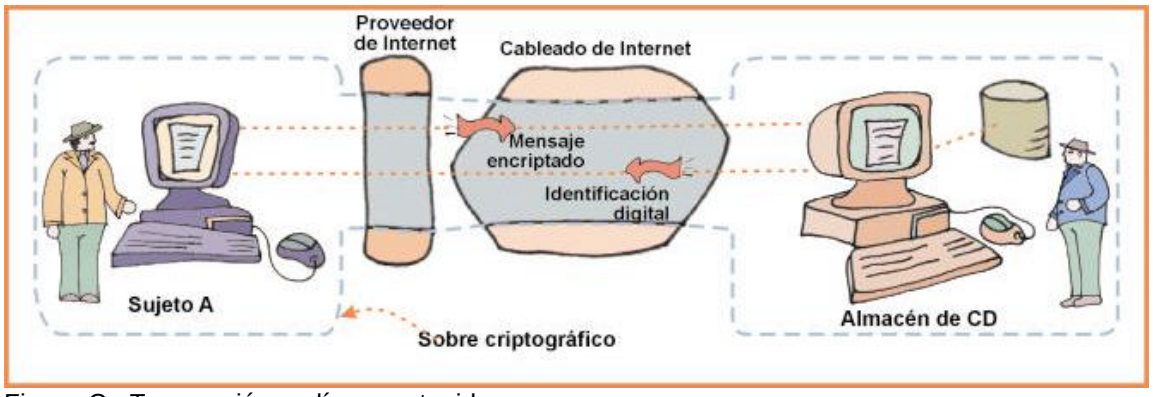


Figura C.: Transacción en línea protegida.

En realidad el consumidor está protegido en el caso que le interceptaran su número de tarjeta de crédito y no es necesario verificar la identidad de los comerciantes ya que éstos no podrían cobrar una compra hecha con tarjeta de crédito a menos que el banco le provea una línea de crédito, lo cual implica un largo procedimiento de solicitud (mucho más arduo que el que podríamos realizar como consumidores), una verificación de fondos y hasta en la mayoría de los casos una visita física.

La idea de asegurar las transacciones con tarjetas de crédito es importante a la hora de tranquilizar al consumidor, más que a la hora de protegerlo. Esta tecnología en realidad protege a los bancos y comerciantes ya que si el número de tarjeta es robado debido a negligencia del comerciante éste es responsable ante el banco de cualquier fraude cometido con ese número, a partir de esto las compañías emisoras de tarjetas de créditos exigen que las transacciones en línea se realicen con servidores Web con características criptográficas.

Transacciones de pagos interbancarios de tarjetas

Una transacción común de tarjeta de crédito involucra a cinco partes:

- El cliente.
- El comerciante.
- El banco del cliente.
- El banco del comerciante (banco adquiriente).
- La red interbancaria.

Y consta de diez pasos que se grafican en la Figura D:

1. El cliente entrega su tarjeta de crédito al comerciante.
2. El comerciante pide autorización al banco adquiriente.
3. La red interbancaria envía un mensaje del banco adquiriente al banco del consumidor pidiendo autorización.
4. El banco del cliente envía una respuesta al banco adquiriente mediante la red interbancaria.
5. El banco adquiriente notifica al comerciante que el cargo ha sido aprobado o rechazado.
6. En caso de haber sido aprobado el comerciante realiza la orden de compra.
7. Luego el comerciante presentará cargos al banco adquiriente.
8. El banco adquiriente envía la solicitud de pago al banco del cliente mediante la red interbancaria.
9. El banco del cliente acredita el dinero en una cuenta de pagos interbancarios deduciendo algún cargo en concepto del servicio dependiendo del convenio. Este dinero será debitado de la cuenta del cliente de acuerdo a las fechas de cierre y pago pactadas entre el cliente y el banco del cliente.
10. El banco adquiriente acredita en la cuenta del comerciante debitando algún cargo en concepto del servicio dependiendo del convenio entre él y el comerciante.

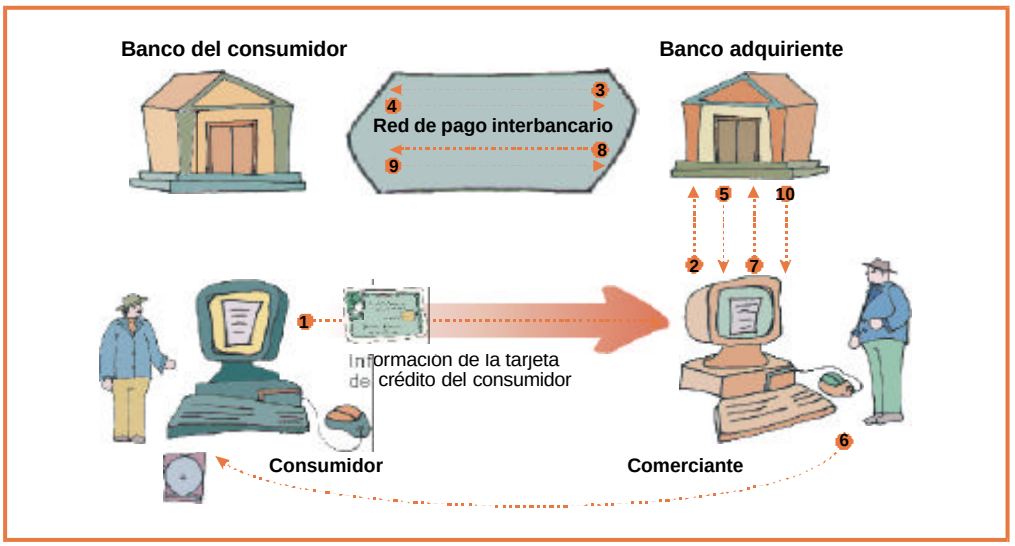


Figura D.: Participantes de una transacción típica con tarjeta de crédito.

El registro de la transacción de la tarjeta de crédito, durante más de treinta años se han llevado en papel hasta que en los ochenta, American Express comenzó a digitalizarlos entregando a los clientes impresiones digitales del mismo. Con el tiempo la información que contiene el comprobante se ha ido incrementando. En la actualidad, aunque varía, de tarjeta en tarjeta es común encontrar los siguientes datos:

- Nombre del cliente.
- Número de la tarjeta de crédito.
- Dirección del cliente.
- Fecha de transacción.
- Monto de la transacción
- Descripción de la mercadería o servicio.
- Código de autorización.
- Nombre del comerciante.
- Firma del cliente.

La información contenida en el comprobante es útil para consumar transacciones y combatir el fraude.

Los bancos cobran una comisión por las prestaciones con tarjeta de crédito. Esta comisión varía de acuerdo a convenios entre el banco y el comercio, entre el 1 y el 7%. Este porcentaje lo paga el comerciante de modo que si una persona compra $100 en productos en un comercio X, verá en su estado de cuenta un cargo de $100 pero al comerciante se le depositarán $97 quedándose el banco adquiriente con la diferencia. Algunos bancos además cobran a los comerciantes una cuota fija por transacción y autorización, además de una inscripción anual y del alquiler de la terminal de tarjeta de crédito.

Los bancos emisores obtienen ganancias de las cuotas impuestas al consumidor y de los intereses resultantes, además del costo de mantenimiento.

La mayoría de los comerciantes deberían preferir recibir pagos con tarjeta de crédito en lugar de cheque o efectivo pese al porcentaje que se le debita, ya que este sistema brinda una confianza instantánea de que se ha hecho el pago y el dinero se depositará en la cuenta del comerciante a diferencia de los cheques que pueden no tener fondos o el efectivo que puede ser falso y aún siendo cheques o dinero efectivo bueno, son objetos físicos que se pueden perder, robar, destruir, etc.

En algunas ocasiones es necesario cancelar el cargo hecho a la tarjeta ya sea por devolución de mercadería o cancelación del servicio. Los bancos emisores de tarjetas están preparados para transferir cargos en ambos sentidos sea por un débito o por un crédito. De la misma forma se puede cancelar un débito que se prueba fraudulento.

Los primeros sistemas de pagos basados en Internet tomaron la infraestructura de transacciones con tarjetas de crédito de forma natural, ya que, muchos comerciantes y clientes estaban habituados a este sistema.

El número de tarjeta de crédito es una clave de acceso utilizada para realizar cargos en la cuenta del consumidor. Es considerado un dato sumamente sensible y la responsabilidad legal por el robo de un número de tarjeta de crédito a causa de una transacción es para el comerciante, ya que se considera una negligencia de seguridad.

Uso de las tarjetas de crédito en Internet

Existen tres formas de realizar una transacción con un número de tarjeta de crédito en la Web:

?? ***Fuera de línea*:** en este método el cliente realiza la orden de compra utilizando la Web. Luego el comerciante llama por teléfono al cliente y verifica la orden de compra y le solicita los datos de la tarjeta de crédito. Los riesgos de este método son equivalentes a enviar el número de tarjeta de crédito sin encriptar ya que la línea de teléfono podría estar intervenida, pero sin embargo existe porque en el imaginario de los consumidores es aterradora la idea de mandar el número de tarjeta de crédito a través de Internet. Además las personas parecen comprender las leyes básicas de fraude con tarjeta de crédito e intervención telefónica mejor que estas mismas leyes aplicadas a la intervención de transacción electrónica de datos. Es intención del autor promover en el lector la idea de la importancia de cambiar este punto de vista del mercado, ya que en rigor este método es el más inseguro. Debemos, con la correcta promoción de las políticas de seguridad aplicadas a la empresa, generar confianza en el cliente.

?? ***En línea con encriptación*:** el consumidor envía el número de tarjeta al comerciante a través de Internet mediante una transacción encriptada. Este método es el único recomendable.

?? ***En línea sin encriptación*:** el consumidor envía el número de tarjeta, ya sea utilizando correo electrónico o un comando POST o GET de HTTP. Esta técnica es vulnerable a la intercepción.

Métodos alternativos a la tarjeta de crédito para compras en Internet

Desde que existe el comercio electrónico se han buscado distintos métodos alternativos de pago intentando reducir el costo de transacción; proporcionar anonimato, ya que con los sistemas de tarjeta de crédito se le debe dar al comerciante varios datos que algunos consumidores son reacios a proporcionar; buscar mayor mercado, muchos potenciales clientes del mercado electrónico no tienen posibilidad de acceder a una tarjeta de crédito por no cumplir con los requisitos exigidos, los nuevos sistemas al no basarse en crédito podrían ser menos restringidos permitiendo entrar al mercado electrónico a muchos potenciales consumidores.

Algunas compañías han incurrido en sistemas prepagos donde el adquiriente abona por adelantado una suma de dinero en efectivo y obtiene una tarjeta con el monto pagado. Este método no tubo gran difusión.

Otra forma de pago utilizada por empresas es el registrar personalmente en una sucursal los datos del cliente y de su tarjeta de crédito. El cliente recibe un identificador de usuario y clave para realizar compras en una cuenta corriente virtual para luego recibir el cargo en su tarjeta. De esta forma el número de la tarjeta no viaja por Internet y el usuario siente que la atención personalizada de la sucursal le transmite seguridad.

Las tarjetas de débito con marcas de tarjetas de crédito como Visa o MasterCard permiten realizar una compra y el cargo se debita de inmediato de la cuenta del cliente procesándose en la misma red interbancaria de las tarjetas de crédito. Las tarjetas de débito están reguladas por leyes distintas a las de crédito, lo que impacta en varios aspectos de su uso, por ejemplo el consumidor no está protegido en forma automática si la tarjeta es robada, éstas y otras diferencias deben leerse con sumo cuidado en el acuerdo con el banco emisor.

Estos medios alternativos de pago en Internet no se han popularizado, siendo la tarjeta de crédito la opción más viable.

Cómo evaluar un sistema de pago mediante tarjetas de crédito

Las siguientes preguntas se deben hacer a la hora de evaluar un sistema de pagos.

- ¿Está la información de los números de tarjetas de crédito, y el resto de la información sensible y privada almacenada, encriptada?
- ¿Los números de tarjetas de crédito de transacciones no recurrentes son eliminados una vez terminada la transacción?
- ¿Comprueba el sistema el dígito verificador del número de tarjeta de crédito proporcionado al introducirlo?
- ¿Realiza el sistema autorizaciones en tiempo real?
- ¿Está el sistema preparado para manejar cancelaciones de cargos?

De las respuestas a estas preguntas dependerá el nivel de seguridad en el manejo de datos de tarjetas de crédito de un sitio Web.

Consideraciones legales

El autor mexicano Julio Tellez Valdez [W-8] señala que los delitos informáticos son "actitudes ilícitas en que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Los ejemplos de delitos informáticos son muchos y con las posibilidades tecnológicas, aumentan en cantidad. Algunos de ellos son: Falsificación de documentos vía computarizada, variación de la situación contable, planeamiento y simulación de delitos convencionales, sustracción o copiado de información confidencial, modificación de datos, uso no autorizado de programas de computo, alteración en el funcionamiento de los sistemas, propagación intencional de virus informáticos, acceso a áreas informatizadas en forma no autorizada, intervención en las líneas de comunicación de datos o teleproceso, programación de instrucciones que producen un bloqueo total al sistema, destrucción de software o hardware por cualquier método, secuestro de soportes computarizados con fines de chantaje, uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario, uso no autorizado de información almacenada en una base de datos, lectura de un mensaje electrónico ajeno, estafas y engaños en transacciones electrónicas, mensajes que remitan consignas, información y planes de actuación de

consignas, información y planes de actuación de cualquier delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Estos delitos afectan de distinta forma a las víctimas. Siendo algunas más preocupantes que otras. En este trabajo veremos como elaborar estrategias que nos protejan de varios de estos ataques. Centrándonos en aquellos que afectan la transacción de datos en el comercio electrónico.

Los puntos a continuación detallan algunas consideraciones a tener en cuenta para no incurrir en un delito informático relacionado al comercio electrónico:

?? Si se está consciente de una actividad criminal y no se informa, legalmente se es responsable como cómplice.

?? Si una computadora se utiliza para actividades ilegales y su dueño no toma acciones definitivas puede ser acusado con una demanda civil que busque compensación de los daños ocasionados.

?? Si un ejecutivo de una empresa es consciente de una actividad ilegal dentro de la misma y decide no investigar y perseguir dicha actividad, los accionistas pueden hacerle una demanda.

Si cree se que el sistema está en riesgo o ha sido utilizado para actos ilegales o inapropiados, se debe considerar levantar un acta penal y buscar asesoría legal teniendo en cuenta que se pueden ver involucrados códigos civiles y penales de varios países ya que Internet se caracteriza por su nivel alto de globalización.

A continuación describimos políticas a seguir para resguardarse de problemas legales:

?? Utilizar el derecho de autor registrando el código fuente e indicando en los mismos que son propiedad privada, aumentando la posibilidad de persecución a gente que robe su código.

?? Asegurarse de que los usuarios sepan que pueden y que no pueden hacer.

?? Poner sobre aviso a los usuarios de que se los está monitoreando por su propia seguridad, ya que de lo contrario, el monitoreo podría ser considerado una violación a la privacía.

?? Tener buenas políticas de back up, para que las mismas puedan ser utilizadas como evidencia legal de como estaba el sistema antes de un ataque y para recuperarse del mismo.

?? Las bitácoras pueden ser valiosas durante una investigación o proceso judicial, deben tener fecha, hora y descripción del evento que se ha producido.

?? Tener por escrito políticas de seguridad y asegurarse de que cada persona sea empleado o usuario del sistema esté en conocimiento de las mismas.

?? Cuando ocurre algún hecho en el que deba intervenir alguna agencia judicial no se debe permitir al personal de la empresa conducir su propia investigación.

?? Los empleados que traten información sensible deben firmar un convenio de confidencialidad.

Se deben tener planes de contingencia con abogados y aseguradoras que contengan acciones a emprender en caso de ser víctima de una irrupción o delito informático.

Administración de riesgos

La seguridad en la Web es difícilmente absoluta, mientras más medidas de seguridad se utilicen, menor es el riesgo que se corre. Se debe reducir el riesgo tanto como sea posible y planear las medidas para recuperarse rápidamente de un incidente de seguridad.

La seguridad Web no es fácil ni barata pero la inseguridad puede ser aún más costosa.

La seguridad no es un producto que pueda comprarse, es parte integral de una organización y de la mentalidad de sus componentes. [E-1]

Parte 2
Tecnologías de protección

En este capítulo se analiza la necesidad de proteger los datos y la privacidad del cliente, brindándole seguridad. Las políticas de seguridad que debieran ser parte de la ética, que un sitio Web de comercio electrónico mantiene hacia sus clientes. Se realiza un acercamiento a los conceptos involucrados en las técnicas de identificación digital y firma electrónica. También se muestra el uso de los certificados digitales, como medio de lograr que los clientes sientan la confianza necesaria para realizar transacciones que impliquen el intercambio de datos sensibles.

Se explican los conceptos involucrados en la criptografía, cómo pieza importante de la seguridad en la Web.

En particular nos concentramos en la problemática de proteger un sitio Web, qué soluciones arquitectónicas se pueden implementar y cuales son sus diferentes implicancias.

Protección de la privacía

Es importante prestar atención a la protección de la privacía personal en la Web ya que esta es una razón por la que muchos potenciales usuarios del comercio electrónico permanecen renuentes a serlo. Además de tener presente la defensa que otorga la legislación a los usuarios.

Cada vez que un navegador muestra una página Web, se crea un registro en el servidor. El mismo contiene el nombre y dirección IP de la computadora que hizo la conexión, la fecha y hora de la petición, el URL solicitado, el tiempo que tomó descargar el archivo. Si se ha usado autenticación mediante HTTP se registra el nombre de usuario, cualquier error que haya ocurrido, la página anteriormente descargada y el tipo de navegador utilizado.

Una de las violaciones a la privacidad del usuario más frecuentemente usada es registrar la página descargada anteriormente, de esta manera las empresas además de evaluar la efectividad de su publicidad en otras páginas pueden hacer un estudio de la forma en que un usuario navega a través de un sitio, sus preferencias e intereses. A tal efecto se utilizan archivos, llamados **cookies**, que se graban en la computadora del usuario al ejecutarse algún evento. Para ciertos tipos de aplicaciones basados en Web, como por ejemplo los carritos de compras de los sitios de e-commerce, son necesarias. Si bien las cookies pueden emplearse para mejorar la seguridad, también para eliminarla. Por desgracia esto no es elección del usuario. Los navegadores deberían dar la posibilidad de controlar las cookies presentando las siguientes opciones:

?? Posibilidad de habilitar o deshabilitar el envío y almacenamiento de cookies.

?? Indicación de si se está utilizando una cookie.

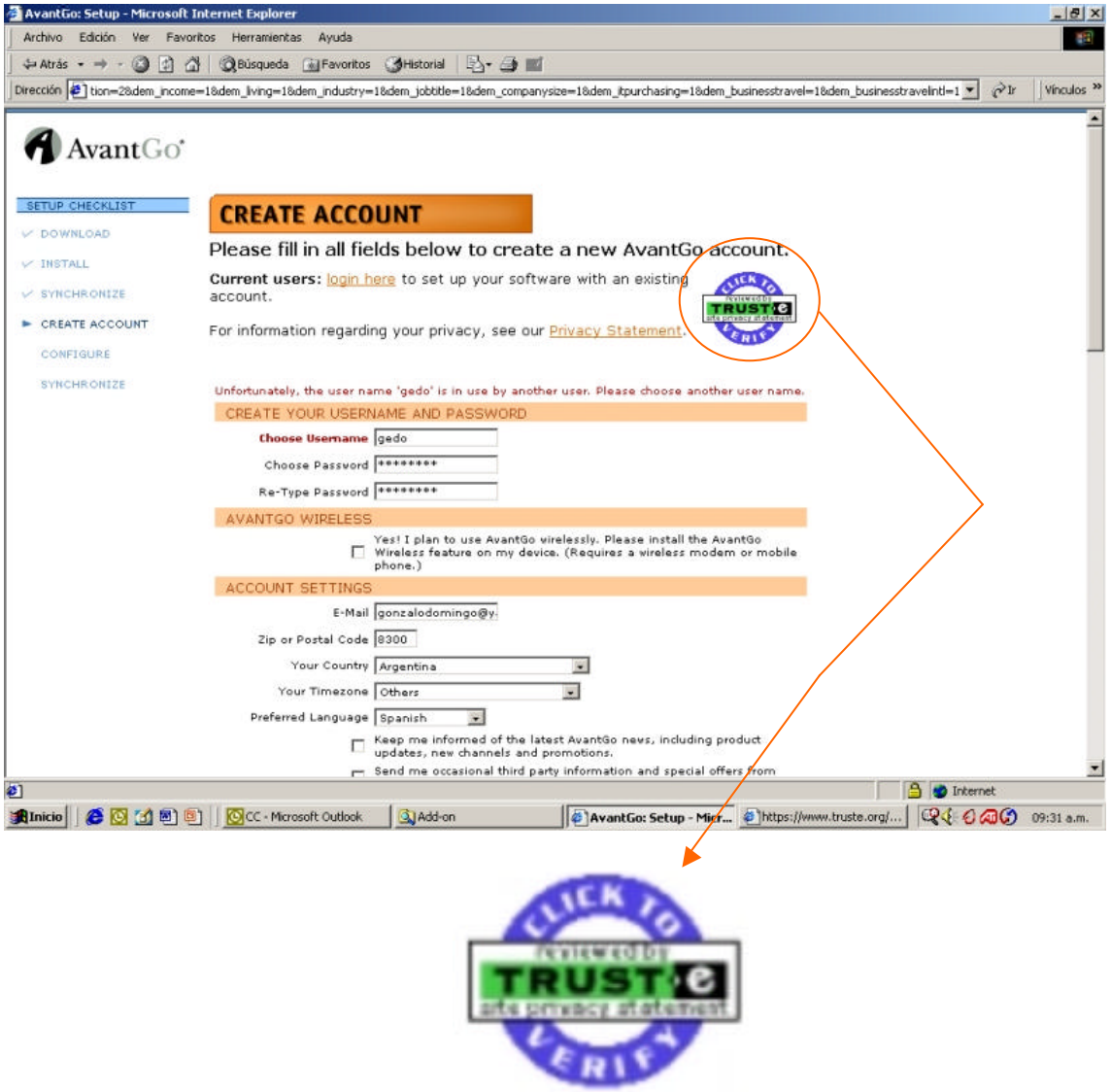
?? Capacidad de especificar un conjunto de dominios para los que se pueden almacenar cookies, permitiendo que si el usuario tiene confianza en un sitio en particular pueda utilizar la aplicación sólo para ese sitio.

Los navegadores más comunes notifican al usuario cuando se recibe una cookie, si éste especifica esa opción, pero no permiten deshabilitar el envío de cookies que ya se han aceptado, rehusar las cookies de algunos sitios pero no de otros o rehusarlas de manera categórica sin ser molestado. El hecho de que no exista un método fácil para deshabilitar el mecanismo de cookies no significa que no pueda hacerse. Algunos trucos son:

?? En sistemas Unix, reemplazar el archivo de cookies con un link a /dev/null.

?? En Windows reemplazar el archivo de cookies por uno de longitud cero con permisos que nieguen la lectura y la escritura.

?? Aceptar las cookies que se desee y luego cambiar los permisos del archivo a sólo lectura, evitando el almacenamiento de más cookies.

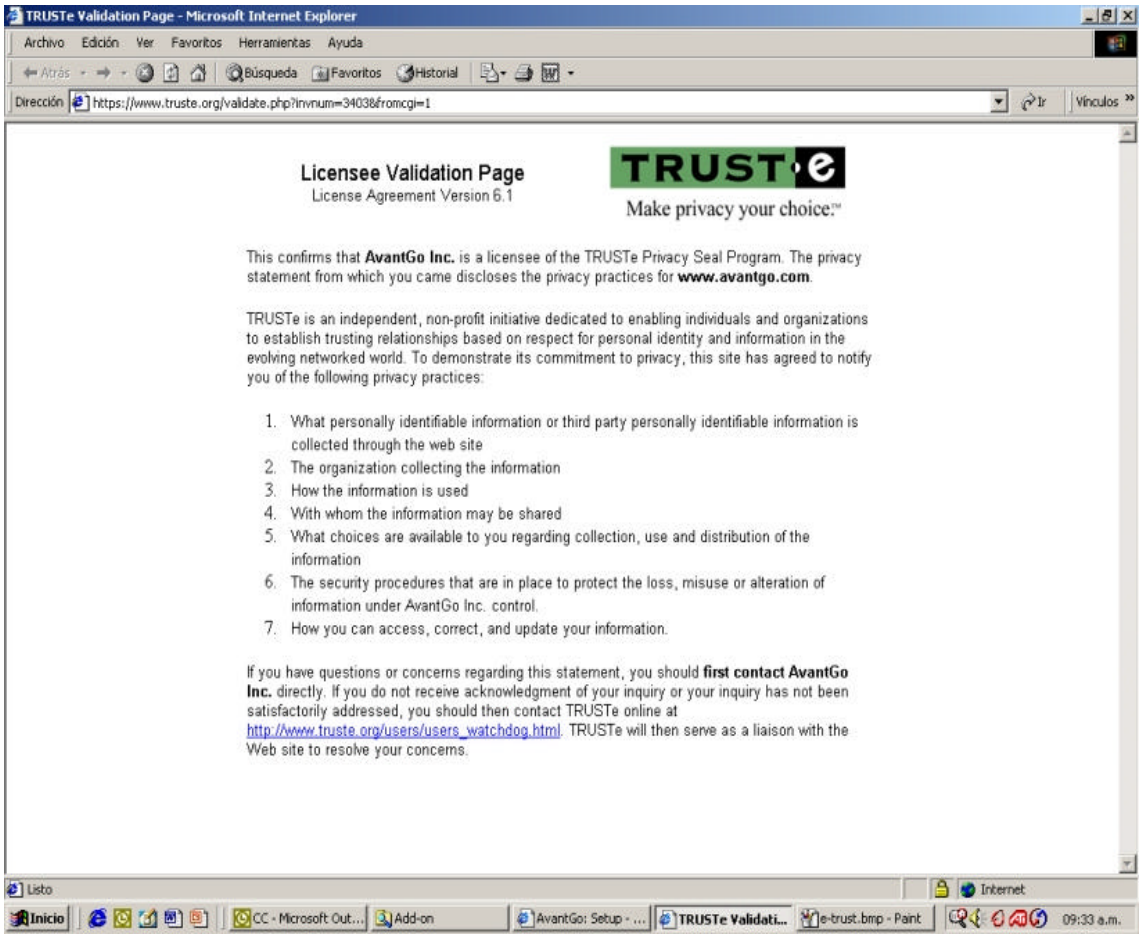


FiguraE.: El sitio está certificado por e-trust y lo promociona.

Los negocios en línea saben mucho acerca de sus clientes, como en cualquier negocio, conocen los nombres, dirección, teléfono y nro de tarjeta de crédito. Pero también pueden registrar con quién intercambian correo electrónico, intereses de mercado, etc. La Fundación de la Frontera Electrónica ha desarrollado un proyecto llamado **e-trust** (confianza electrónica) que consiste en someter a auditorías periódicas a las empresas de comercio electrónico. Las

que cumplan con un estándar, que especifica lo que se puede hacer con los datos sensibles de los usuarios, podrían certificarse como sitio e-trust. La Figura E muestra un sitio que promociona su certificado e-trust como forma de generar confianza en el cliente.

Al hacer clic en el vinculo del logo aparece un certificado con el detalle de la certificación, como vemos en la Figura F.



FiguraF.: Pagina de validación del certificado e-trust del sitio.

En Estados Unidos está en vigencia desde 1997 el Acta de Protección de la Privacía de los Consumidores de Internet que prohíbe a los servicios en línea divulgar cualquier información personalmente identificable sobre sus clientes, a menos que con anterioridad, el cliente hubiese dado su expresa autorización por escrito. Por esto es que en Internet se ha hecho común que algunos servicios se ofrezcan de forma gratuita a cambio de que uno ingrese ciertos datos como la dirección de correo electrónico y su consentimiento para recibir publicidad. Los datos son vendidos a distintas consultoras de mercadeo que los utilizan para los más diversos fines.

A continuación se presenta una lista de políticas empleadas por los sitios que respetan la privacía de los datos sensibles.

?? No exigir a los usuarios que se registren para utilizar su sitio.

?? Permitir a los usuarios registrar su dirección de correo electrónico sólo si desean recibir boletines.

?? No compartir con otra compañía los datos de un usuario sin la autorización explícita de este, para cada una de las compañías con las que se desea compartir esas direcciones.

?? Siempre que se envíe un mensaje de correo electrónico a los usuarios, explicarles como se obtuvo su dirección y como puede hacer para borrarse de la lista de distribución si así lo desea[9].

?? No permitir el acceso a las bitácoras.

?? Eliminar las bitácoras cuando ya no sean necesarias.

?? Eliminar de las bitácoras toda la información personalmente identificable de los usuarios que no sea necesaria para la misma.

?? Encriptar las bitácoras.

?? No dar ninguna información personal de los usuarios.

?? Aplicar políticas internas de privacía con los empleados, una organización es la suma de sus componentes.

?? Informar a los usuarios acerca de las políticas en la página principal y permitir que la compañía sea auditada por terceros si surgen preguntas sobre su política.

[9] Esto es obligatorio para no violar la legislación sobre SPAM (correo electrónico no deseado) que especifica que un mail no podrá ser considerado SPAM mientras el usuario posea un modo explícito de ser removido de la lista de distribución.

Técnicas de identificación digital

La identificación es parte indispensable de la vida actual. Es cosa de todos los días identificarnos mediante documentación: al cobrar un cheque, al abrir una cuenta en un negocio, al abonar con tarjeta de crédito o débito, al solicitar empleo, al ingresar en un edificio, al adquirir propiedades, ante los representantes de alguna fuerza de orden y justicia y en todos los casos en que necesitemos probar de forma confiable quienes somos. Los símbolos físicos como el DNI, cédula u otra tarjeta de identificación permiten a las empresas extendernos crédito y confianza. Estos medios de identificación no crean por si mismos un ambiente de negocios estable, trabajan a la par del sistema legal. Si una persona firma un cheque sin fondos o no cumple con un contrato la parte perjudicada puede esperar una reparación satisfactoria mediante el orden legal, asegurándose previamente de verificar que la persona que le ocasionó el daño es quien dice ser.

Para los clientes también es importante verificar que las empresas son quien dicen ser, para esto se puede utilizar la ubicación física de la misma, ya que en el Registro Público de la Propiedad consta quién es el dueño de una propiedad y se puede recurrir a la justicia para exigir una reparación en caso de ser damnificado por una empresa ubicable.

En el mundo digital, en cambio, las cosas pueden no ser como parecen a simple vista y ambas partes, cliente y empresa podrían no ser quien dicen ser.

Identificación computarizada

Tradicionalmente las computadoras personales no identificaban a sus usuarios sino que le daban acceso total a quién se sentara frente al teclado. Hoy en día con los sistemas operativos con módulos avanzados de seguridad y tendientes a operar en red, las cosas han cambiado. Sin embargo la preocupación de estos sistemas de identificación no son que la persona sea legalmente quien dice ser, sino que el usuario esté autorizado para acceder a sus recursos. Se pueden identificar cuatro tipos de sistemas de identificación que se detallan a continuación.

a) Sistemas basados en clave de acceso: algo que se sabe

Este fue el primer sistema de identificación digital, donde cada usuario del sistema tiene un nombre de usuario y una clave de acceso que se corresponden para probar la identidad del mismo. La premisa es: si el usuario ingresa

un nombre de acceso valido y una clave que se corresponde con la que está almacenada para ese nombre de usuario, simplemente debe ser quien dice ser.

Existen varios inconvenientes con este tipo de identificación:

?? El sistema debe tener archivado el nombre de usuario y su correspondiente clave antes de comprobar la identidad.

?? La clave puede ser interceptada y quien lo haga puede hacerse pasar por el usuario.

?? El usuario puede olvidar su clave de acceso.

?? Una persona que conozca al usuario puede inferir su clave si este no aplica una buena política al elegir la clave.

?? El usuario puede compartir su clave con otras personas de forma voluntaria.

b) Sistemas basados en prendas físicas: algo que se tiene

Otra forma de probar la identidad de un usuario es mediante una prenda física, como las tarjetas de acceso. Cada tarjeta tiene un número único y el sistema tiene una lista con tarjetas autorizadas y los privilegios de cada una. Pero al igual que los sistemas basados en claves de acceso, hay algunos inconvenientes con este sistema.

?? La prenda no prueba quien es la persona. Cualquiera que la tenga accederá a los privilegios asociados a la misma.

?? Si un usuario pierde su prenda, no podrá acceder al sistema aunque tenga todos los derechos.

?? Algunas prendas pueden ser copiadas o falsificadas.

?? Este sistema en realidad no autoriza al individuo sino a la prenda.

c) Sistemas basados en biométrica: algo que se es

Esta técnica realiza mediciones físicas al usuario y lo compara con registros almacenados con anterioridad. La biométrica se puede realizar a través de huellas digitales, forma de la mano, patrón de vasos sanguíneos de la retina, patrones de ADN, registro de voz, caligrafía, forma de teclear, si bien es una forma bastante confiable de determinar la identidad de un usuario, tiene algunos problemas.

?? La firma biométrica de una persona debe estar almacenada en un banco de datos de una computadora antes de ser identificada.

?? Requiere de equipamiento caro y de propósito específico.

?? El equipo de medición es vulnerable al sabotaje y fraude.

d) Sistemas basados en ubicación: Algún lugar en el que se está

Este sistema utiliza el Sistema de Ubicación Global (GPS, Global Positioning System) para autenticar al usuario sobre la base del lugar en el que está. Como sus predecesores, no es ajeno a inconvenientes:

?? La ubicación de una persona debe estar almacenada en un banco de datos de una computadora antes de ser identificada.

?? Requiere de equipamiento caro y de propósito específico.

?? El sistema asegura que hay alguien que posee el GPS en donde se supone que lo debe tener pero nada más.

Firmas digitales

Los sistemas de identificación antes descriptos son mejorados al combinarse con firmas digitales [L-9]. La firma digital es una tecnología que consta de:

?? **Una llave privada:** utilizada para firmar un bloque de datos.

?? **Una llave pública:** utilizada para verificar la firma.

Supongamos que un sujeto **A,** como el de la Figura G, distribuye una llave pública a prueba de alteración. Como esta llave sólo sirve para comprobar si la llave privada que el sujeto **A** conserva es realmente la llave privada del sujeto **A**, sí alguien intercepta la llave pública no le serviría de nada, por lo tanto el sujeto **A** podría distribuir la llave pública por cualquier medio.

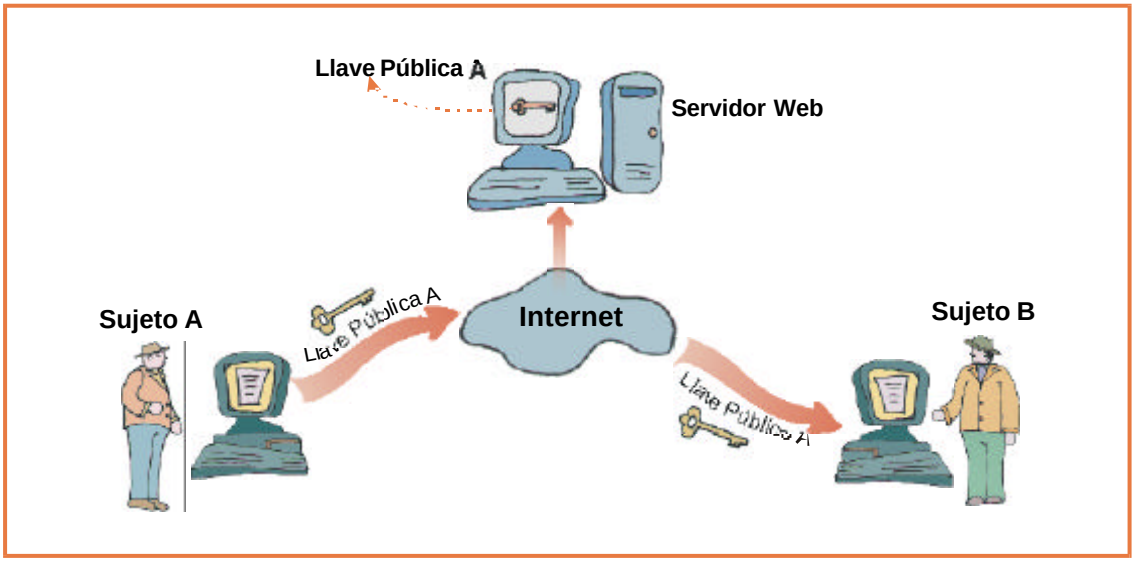


Figura G.: Distribución de una llave pública.

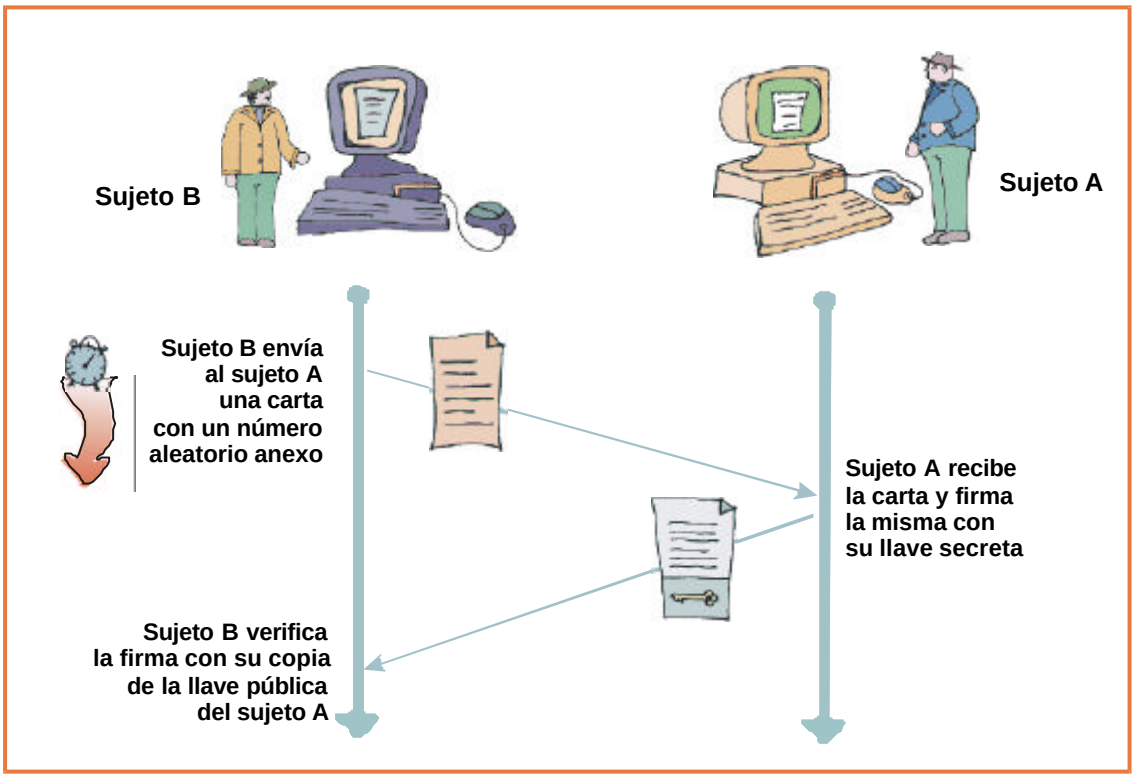


Figura H.: Uso de la firma digital para comprobar la identidad.

Supongamos ahora que un sujeto **B**, como el de la Figura H, necesita corroborar que el sujeto **A** ha leído un documento **X**, para esto envía el documento **X** por mail al sujeto **A**, el sujeto **A** recibe el documento **X** lo lee y anexa su firma generada con la llave secreta. El sujeto **A** reenvía el documento firmado al sujeto **B** que mediante la llave pública corrobora la legitimidad de la firma.

Los siguientes son los medios físicos en los que soportan la tecnología de llave digital para realizar firmas.

?? **Llave encriptada almacenadas en disco duro:** esta es la forma más sencilla de almacenar la llave, aunque vulnerable a usuarios de la computadora y a programas hostiles.

?? **Llave encriptada en medio removible:** es un poco más seguro guardar la llave privada en un disquete, disco compacto u otro medio removible. Pero para utilizar la llave privada la computadora debe desencriptarla y copiar la memoria, por lo que aún sigue siendo vulnerable a programas hostiles.

?? **Llave almacenada en un dispositivo inteligente:** estos dispositivos son una tarjeta con un microprocesador que almacena la llave privada transfiriéndola directamente sin cargarla en memoria por lo que es inmune a un programa hostil que intente capturarlo. La desventaja de este tipo de dispositivo es su fragilidad y la posibilidad de ser robadas o extraviadas.

Desventajas

A continuación mencionaremos algunas desventajas que presenta utilizar una infraestructura de llaves públicas.

?? La mayor parte de las transacciones de comercio en Internet se basan en las tarjetas de crédito, sin utilizar la tecnología de firmas digitales.

?? Las firmas digitales facilitan la prueba de identidad pero no la aseguran, todo lo que comprueban es que una persona tiene acceso a una llave privada específica que complemente a una llave pública específica que está firmada por una autoridad certificadora específica.

?? Al no existir estándares que regulen a las autoridades certificadoras no es posible evaluar la confiabilidad de las mismas, no es posible saber si la autoridad certificadora quebranta sus propias reglas emitiendo documentos fraudulentos. También es difícil comparar una autoridad certificadora con otra y más difícil aún hacerlo de forma automática.

?? El certificado no posee los datos suficientes como para identificar de forma legal a su poseedor.

?? La tecnología de firma digital no permite la divulgación selectiva de datos.

Certificados digitales

Existen organizaciones, llamadas autoridades certificadoras, que se encargan de comprobar si una llave pública específica es propiedad de un individuo u organización en particular. Como resultado de esta comprobación emiten un “Cerificado de llave pública” que contiene el nombre de la persona, la llave pública, número de serie, la fecha de creación del certificado y la fecha de vencimiento. El certificado comprueba que una llave pública específica es propiedad de un individuo u organización en particular. Los navegadores de Internet reconocen a muchas de estas autoridades certificadoras automáticamente y permiten agregar manualmente a las que no reconocen.

Si la llave privada del tenedor ha sido violada, si la persona ha dado datos incorrectos o si hay copias falsas de ésa llave, el certificado puede ser revocado. Las llaves revocadas que aún no están vencidas son colocadas en una Lista de Revocación de Certificados (CRL, Certificate Revocation List), estas listas tienden a crecer con rapidez pero su actualización es lenta.

La Figura I, muestra un certificado emitido por VeriSign, una de las autoridades certificadoras más fuertemente reconocidas. El certificado fue tomado de la página www.cti.com.ar que utiliza el comercio electrónico para hacer el

pago de la factura de los clientes por medios electrónicos de pago. El acceso al certificado se logra haciendo doble clic sobre el candadito[10] que aparece en el Internet Explorer al entrar a esta página o accediendo al menú *Archivo,* en la opción *Propiedades* del Internet Explorer.

En la Figura J se observa un sitio que promociona su seguridad de forma explícita, poniendo en su página principal un vinculo a su certificado digital.

Direcciones falsas

Es muy simple redirigir a un usuario a una página que parezca otra, por ejemplo, si yo doy la dirección www.microsoft.com@3358557665 aunque parezca absurdo va a datafull. ¿Por qué? Porque el número que figura detrás de la @ es el número de IP de datafull en formato longbyte y la @ es la encargada de indicarle los parámetros a la página. De este modo es sencillo engañar a alguien que quiere hacer una compra, dándole una dirección con estas características, el usuario, entra al sitio, parece que está todo en orden, ingresa los datos de tu tarjeta y del otro lado le realizan los cargos sin enviarle nada. Principalmente, estas técnicas toman ventaja del formato estándar de direcciones.

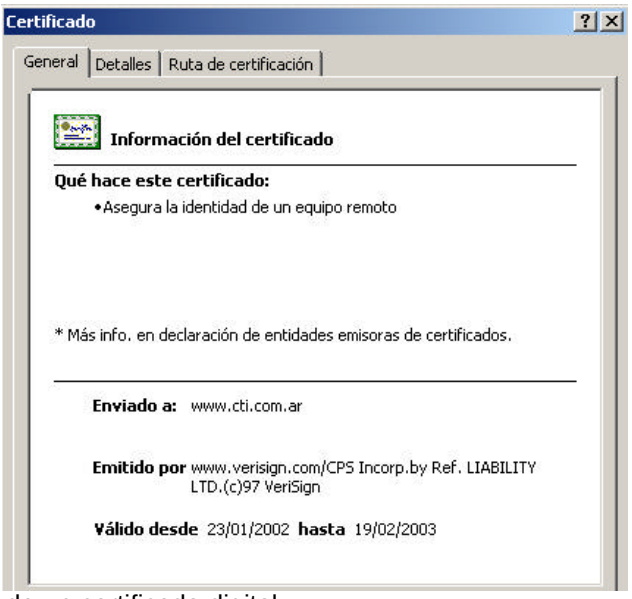


Figura I.: Descripción de un certificado digital.

[10] Este candado indica que la página utiliza facilidades criptográficas. Como se ve más adelante en la figura X.

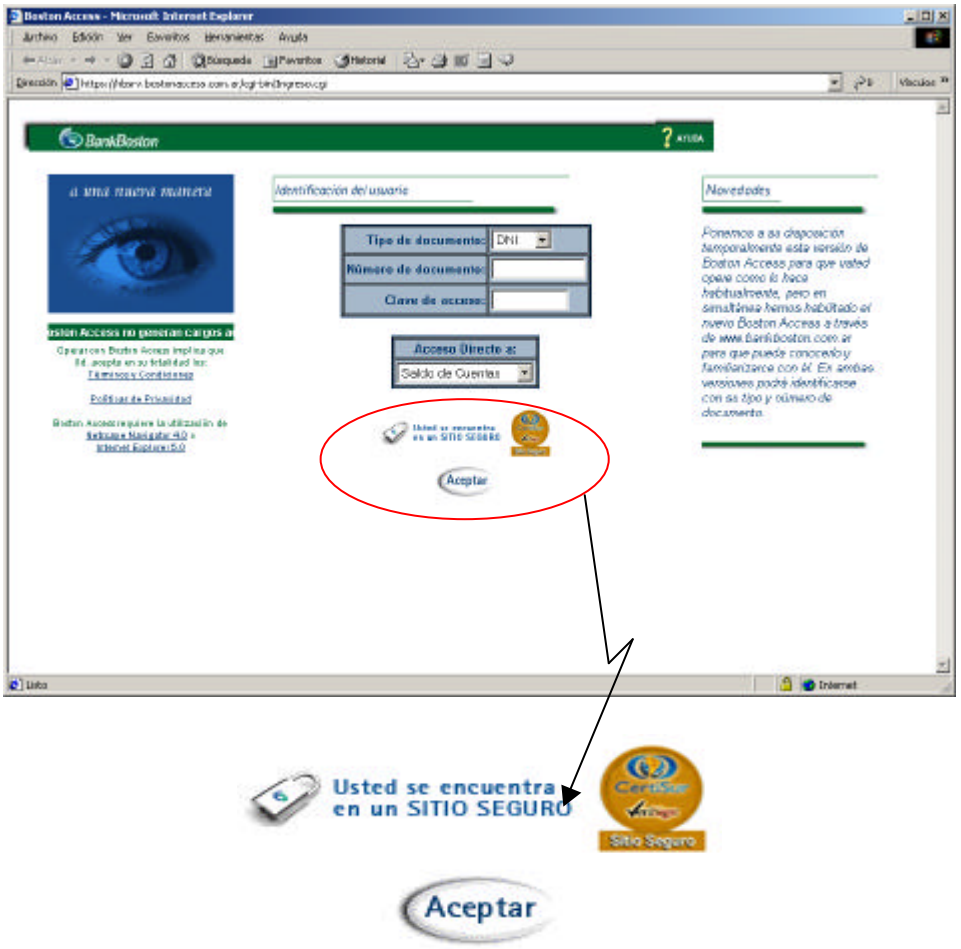


Figura J.: Promoción de la seguridad de un sitio.

El formato completo de una dirección HTTP es, por ejemplo: http://usuario:password@host.com, entonces, si logramos esconder, el nombre del host (esto se logra reemplazando host.com por el número IP), podemos poner adelante de la arroba lo que queramos. Existen páginas como http://people.freenet.de/bxxxxj/ que divulgan esta información y convierten un URL a su equivalente en formato longbyte para ayudar a los que pretendan realizar engaños.

Por lo tanto no debemos confiar en sitios que no certifiquen su nombre ya que podríamos creer estar en un lado y estar en otro y si el sitio falso usa facilidades criptográficas aún veríamos el candadito y estaríamos confiados...

Pero no es malo que esto se sepa, ni peligroso; al contrario, mientras más sepamos de los peligros que nos rodean más abiertos tendremos los ojos para defendernos.

VeriSign™
The Sign of Trust on the Net

HBSRV.BOSTONACCESS.COM.AR es un Sitio Seguro CertiSur

CertiSur

La **Seguridad** sigue siendo una de los principales preocupaciones para los consumidores on-line. El **Programa de Sitio Seguro de CertiSur** le permite a Ud. obtener más información sobre los sitios seguros que visita antes de enviarles información que considere confidencial. Por favor, verifique que la información que aparece en esta página coincide con la información del sitio que Ud. está visitando.

Nombre	HBSRV.BOSTONACCESS.COM.AR
Estado	**Valido**
Período de Validez	10-JAN-02 - 10-JAN-03
Información de la Empresa	Country = AR State = Buenos Aires Locality = Capital Federal Organization = BankBoston National Association Organizational Unit = Sistemas Organizational Unit = Terms of use at www.certisur.com/rpa (c) 00 Organizational Unit = Authenticated by CertiSur S.A. Organizational Unit = Member, VeriSign Trust Network Common Name = hbsrv.bostonaccess.com.ar

Si la información es correcta, Ud puede enviar información sensible, (ej. número de tarjeta de crédito) con la seguridad que:

- Este sitio tiene un Server ID emitido por CertiSur S.A.
- CertiSur S.A. ha verificado el nombre de la Organización y que BANKBOSTON NATIONAL ASSOCIATION ha entregado documentación que demuestra el derecho a su uso.
- El sitio legítimamente opera bajo el auspicio de BANKBOSTON NATIONAL ASSOCIATION.
- Toda la información enviada a este sitio, si se encuentra bajo una conexión SSL, será encriptada, protegiendo su divulgación hacia terceras partes.

Para asegurar que este es un **Sitio Seguro CertiSur** legítimo, debe verificar:

1. El URL del sitio que Ud está visitando viene de HBSRV.BOSTONACCESS.COM.AR.
2. El URL de esta página es **https://digitalid.certisur.com/**.
3. El Estado del Server ID es **Válido**.

Figura K.: Descripción extensa de un certificado digital.

Robo y falsificación de certificados digitales

¿Qué sucede si el certificado que ofrece el servidor como prueba es un certificado falsificado o robado de otro servidor?.

Este problema existe con algunas versiones de Microsoft Internet Explorer y pone a los usuarios en una situación de inseguridad para la compra a través de Internet. A continuación se detalla el problema y se demuestra con ejemplo práctico.

Para corroborar la autenticidad de los sitios y los usuarios que acceden a ellos, se utilizan certificados que deben ser instalados en nuestra computadora. Por ejemplo, si manejamos una cuenta bancaria vía Web, en algún momento la institución bancaria debe habernos remitió un certificado que nos permite actuar en nuestra cuenta. La tarea fundamental de esta certificación, es demostrar que quienes se conectan, cliente y servidor, son quienes dicen ser, y además se implementa una codificación única entre ambos. Sin embargo, si se logra falsificar dichos certificados se podría tomar el control de la cuenta. Existe un método, llamado "hombre en el camino", en el que el atacante intercepta la comunicación entre dos partes haciéndoles creer a cada una de ellas que se comunica con la otra, cómo observamos en la Figura L. Este tipo de ataque puede permitir "secuestrar" una conexión para remitir el certificado falso sin el conocimiento de la víctima. También logra engañar al cliente para que este crea ver el certificado que está esperando, y que además suponga que proviene del verdadero servidor seguro.

Documento de práctica de certificación

Las autoridades certificadoras publican un documento de práctica de certificación donde describen qué políticas y procedimientos se siguen para emitir y revocar certificados digitales ya que no existen estándares a seguir respecto a condiciones para emitir certificados. Esto impide su procesamiento automático.

Las autoridades certificadoras van tendiendo a adoptar el certificado X.509 v3 como un modelo para certificar llaves públicas. Muchos protocolos criptográficos lo utilizan. La Figura M muestra la estructura esquemática del certificado X.509 v3. Cuando nos fijamos en las propiedades de una página con transferencia de datos encriptados, nos muestra un mensaje como el de la Figura N.

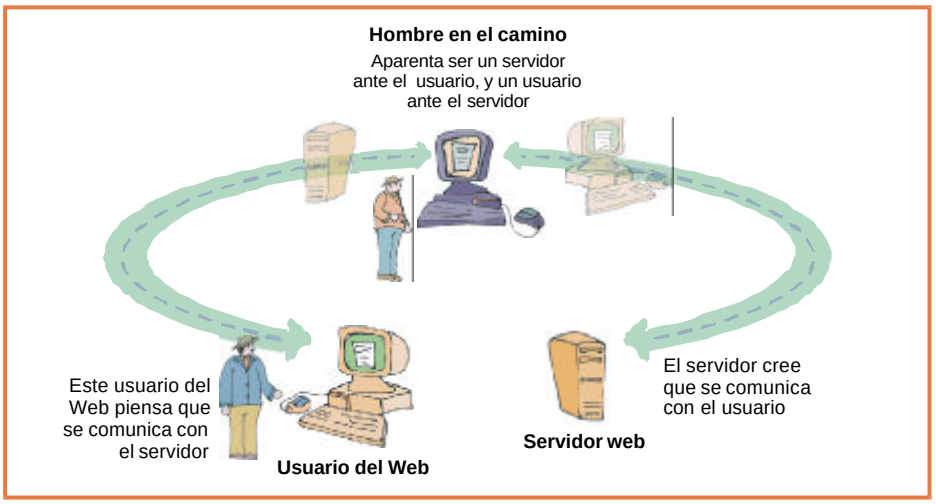


Figura L.: Ataque de hombre en el camino.

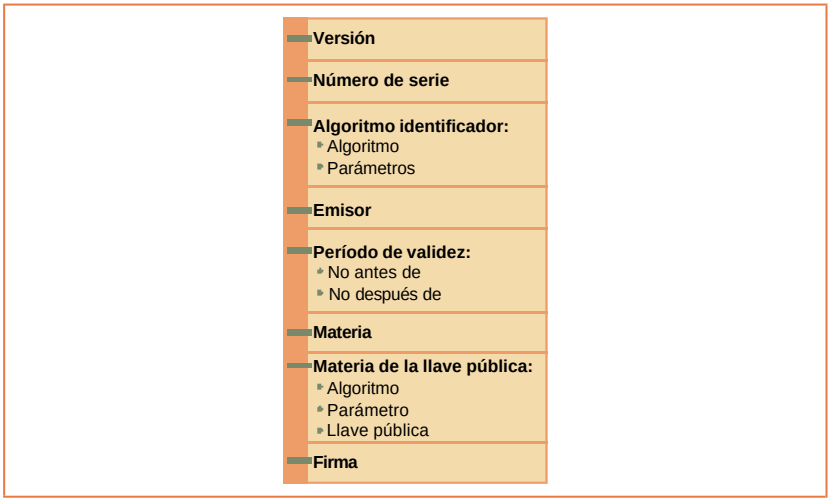


Figura M.: Estructura esquemática de un certificado X.509 típico.

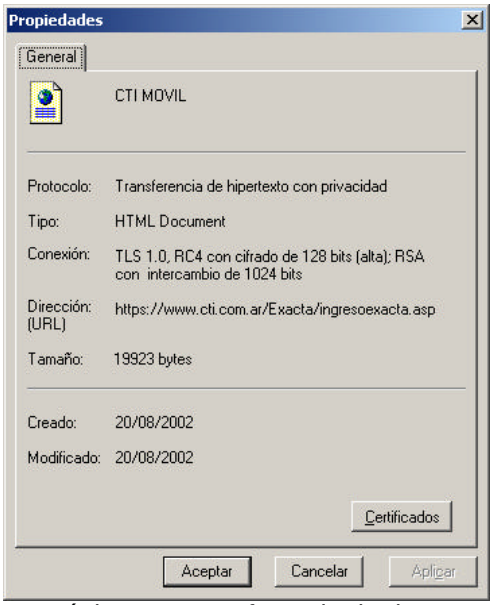


Figura N.: Propiedades de una página con transferencia de datos encriptados.

Ventajas de los certificados

a) desde el punto de vista del consumidor

?? Proveen una forma sencilla de verificar la autenticidad de una organización antes de darle información digital.

?? Da la tranquilidad de tener una dirección física y un nombre legal de la organización para poder emprender acciones legales en caso de ser necesario.

b) desde el punto de vista del comerciante

?? Proveen una forma sencilla de verificar la dirección de correo electrónico del cliente.

?? Elimina la necesidad de utilizar nombre de usuario y clave de acceso; lo cual ahorra costos de administración y evita que más de un usuario compartan el mismo nombre y clave. Aunque es posible compartir una llave secreta el riesgo que esto presenta para el usuario puede ser mayor que los beneficios obtenidos al hacerlo.

Tipos de certificados

A continuación veremos los distintos tipos de certificados disponibles hoy en día:

a) Certificados de autoridades certificadoras

Se utilizan para certificar otro tipo de certificados. Contienen el nombre y la llave pública de la autoridad certificadora, pueden ser auto firmados o firmados por otra organización. Por lo general se incluyen directamente en los navegadores.

b) Certificados de servidores

Contienen la llave pública de un servidor, el nombre de la organización que lo administra, el nombre de anfitrión en Internet y la llave pública del servidor. Cada servidor que utilice facilidades criptográficas debe tener un certificado de servidor. Cuando el navegador se conecta a un servidor Web mediante el protocolo criptográfico, el servidor le envía su llave pública dentro de un certificado X.509 v3 el cual autentica la identidad del servidor y distribuye la llave pública que el cliente utilizará para encriptar la información que enviará al servidor. Un certificado contiene los siguientes campos:

?? Longitud de llave de la firma.

?? Número de serie del certificado, que es único dentro de cada autoridad certificadora.

?? Nombre distintivo.

?? Especificación del algoritmo utilizado para la firma.

?? Nombre del servidor de dominio.

Para obtener un certificado para un servidor es necesario seguir los siguientes pasos:

?? Generar un par de llaves pública / privada de RSA[11] mediante un programa proporcionado por el proveedor del servidor.

?? Enviar la llave pública, el nombre distintivo y el nombre del servidor de dominio a la autoridad certificadora que va a proporcionar el certificado.

?? Seguir el procedimiento que la autoridad certificadora requiera.

?? Si la solicitud es aprobada se recibe el certificado el cual se instala con algún programa proporcionado por el proveedor del servidor.

Los certificados expiran generalmente un año después de su emisión, cuando esto sucede se debe obtener un nuevo certificado. La razón por la que expiran es para disminuir la probabilidad de que la llave privada sea violada y aumentar la confianza en las llaves públicas. Si el navegador se conecta a un servidor Web con facilidades criptográficas y el contenido de un campo del certificado no corresponde con lo esperado, el navegador alerta al usuario o no permite la conexión dependiendo de la configuración de seguridad del mismo. Mostrando un mensaje como el de la Figura O.

c) Certificados personales

Contienen el nombre y la llave pública de un individuo, también pueden tener información como su correo electrónico, dirección postal, o cualquier otro atributo de la persona. Los siguientes son algunos de sus usos:

?? Elimina la necesidad de nombre de usuario y clave de acceso.

?? Se pueden utilizar para enviar correo encriptado.

?? Si el certificado contiene datos sobre la persona puede utilizarse para discriminar la información que recibirá.

d) Certificados de editor de software

Se utilizan para firmar software que va a distribuirse. Mejora la confiabilidad del software distribuido por Internet reduciendo la posibilidad de descargar programas hostiles como virus y caballos de Troya[12].

[11] RSA: Sistema de llave pública creado por **R**ivest, **S**hamir y **A**dleman en 1978 y que ha ganado gran aceptación, por la seguridad que ofrece al basarse en un problema matemático difícil de resolver que había dejado de tener interés en la comunidad mundial, como lo es el problema de la factorización entera y a causa del sistema RSA se ha retomado e incrementado su investigación. Por otra parte, aunque implementar RSA requiere de mucho cuidado en detalles que son necesarios, la idea de su funcionamiento es muy simple de entender, lo que lo hace muy popular principalmente en sectores donde no hay abundancia de matemáticas. [W-16]

Hoy en día existen varias propuestas para la firma de código: Authenticode de Microsoft, JAR un formato de archivo Java desarrollado por JavaSoft y Netscape el cual es un archivo ZIP firmado digitalmente y otras.

Recordamos que la tecnología de Firma Digital no hace que el software sea más seguro sino que permite a las autoridades certificadoras revocar certificados de editor de software a aquellos que distribuyan programas dañinos; es decir que proveen una solución una vez que el daño está hecho.

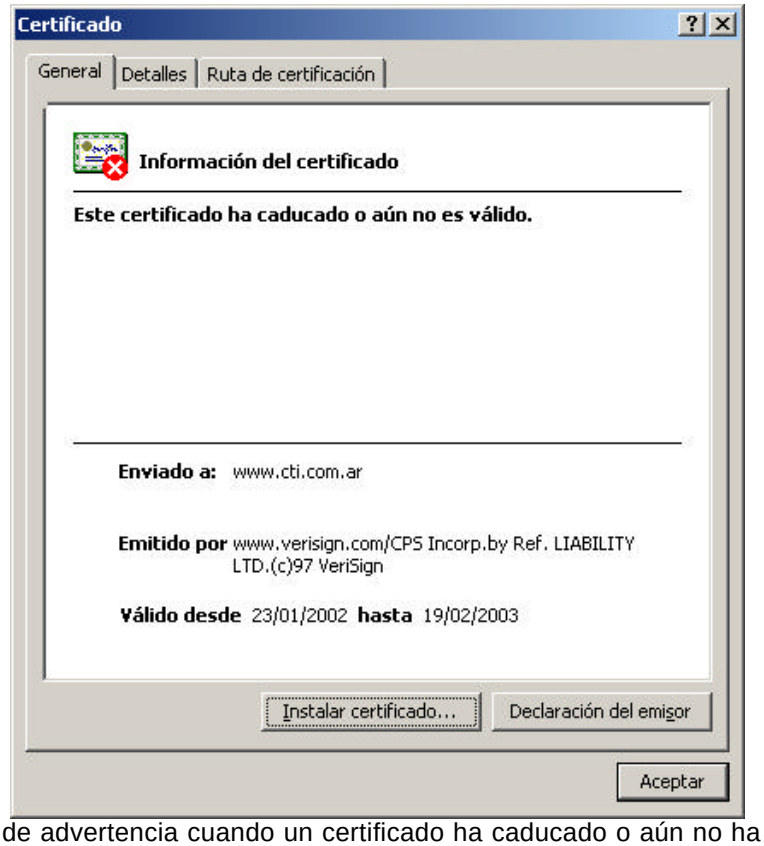


Figura O.: Mensaje de advertencia cuando un certificado ha caducado o aún no ha entrado en vigencia.

[12] Programas que aparentan tener una función específica pero en realidad poseen una función hostil oculta.

Criptografía, la piedra fundamental de la seguridad

Hasta aquí se ha nombrado a la criptografía y a las facilidades criptográficas como una herramienta básica para proveer de seguridad a una transacción en línea a través de Internet. En este capítulo entraremos en detalle a la definición de la criptografía y su aplicación en la arquitectura de seguridad de un sitio Web. [L-4] [L-9] [W-6] [W-14] [W-15]

La criptografía

Es un conjunto de técnicas empleadas para conservar la información de forma segura. Está basada en la transformación de los datos de forma tal que sean incomprensibles para los receptores no autorizados, en cambio para aquellos receptores que posean la autorización correspondiente, los datos que conforman dicha información resultarán perfectamente comprensibles.

En la transformación se pueden identificar 2 procesos bien definidos (Figura P):

?? **Encriptación:** Proceso mediante el cual un conjunto de datos se transforman en un conjunto cifrado de datos mediante una función de transformación y una llave de codificación.

?? **Desencriptación:** Proceso inverso a la encriptación, en el cual el conjunto cifrado de datos se convierte en el texto original mediante una segunda función de transformación y una llave de desencriptación. La llave puede ser la misma para ambos procesos o distinta.

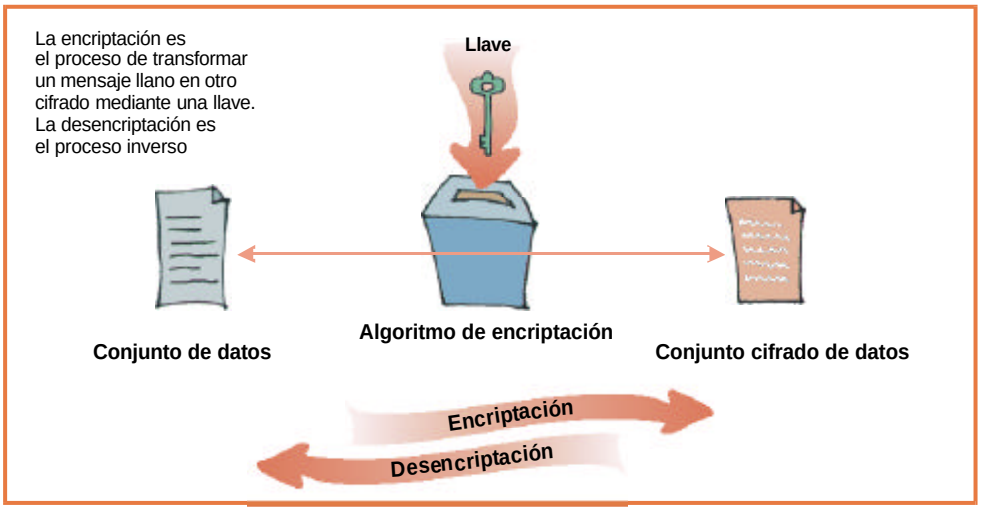


Figura P.: Ejemplo sencillo de encriptación y desencriptación.

En la Figura Q, se presenta un par de algoritmos de encriptación y desencriptación que tiene dos inconvenientes:

1. Es tan fácil encriptar como desencriptar. El éxito de la encriptación radica en que sea relativamente sencillo, barato y con poco tiempo de procesamiento, el realizar el encriptado. Mientras que el desencriptado debe ser más complejo ya que eso asegurará que a un receptor que no posea autorización para leer el mensaje y por lo tanto el algoritmo desencriptador, le resulte más costoso deducir el algoritmo de desencriptación que la información que el mensaje encriptado contiene.
2. El mensaje: “LOS PATOS SON 2” se encriptaría de la siguiente manera: “L4S P1T4S S4N 2” y sería desencriptado de la siguiente manera: “LOS PATOS SON E”. Es decir este algoritmo pierde información si el mensaje original contiene números.

Pero aun así sirve a modo de ejemplo.

Algoritmos y funciones criptográficas

La criptografía tiene miles de años de antigüedad, los primeros usos de esta técnica se remontan a las Guerras Helénicas en que los comandantes utilizaban el método de sustitución y transposición para enviar mensajes a los soldados en el campo de batalla, asegurándose así que la posible intercepción del mensajero no signifique que el enemigo supiera el contenido del mensaje interceptado.

La sustitución es un método que consiste en reemplazar una letra del mensaje por otro símbolo equivalente, como en el ejemplo antes citado. Esté método se llama también Método César ya que Julio Cesar lo utilizaba en sus campañas.

Mensaje: **“ESTE ES UN MENSAJE”**

Mensaje encriptado: **“2ST2 2S 5N M2NS1J1”**

Algoritmo de encriptación:

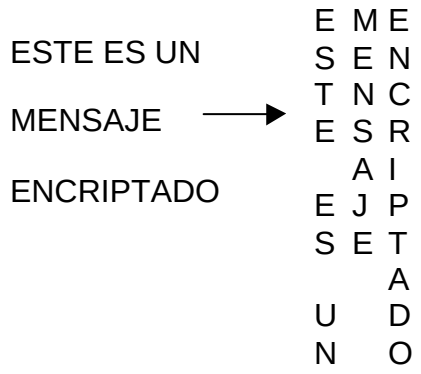
```
Tomar una letra
Repetir
  Según letra
      “A” : letra = “1”
      “E” : letra = “2”
      “I” : letra = “3”
      “O” : letra = “4”
      “U” : letra = “5”
  Fin Según
  Tomar siguiente letra
Hasta (fin de mensaje)
```

Algoritmo de desencriptación:

```
Tomar una letra
Repetir
  Según letra
      “1” : letra = “A”
      “2” : letra = “E”
      “3” : letra = “I”
      “4” : letra = “O”
      “5” : letra = “U”
  Fin Según
  Tomar siguiente letra
Hasta (fin de mensaje)
```

Figura Q.: Ejemplo de algoritmos de encriptación y desencriptación.

La transposición, en cambio se basa en intercambiar el orden de los caracteres para evitar que el mensaje sea legible. Un método es el matricial donde el mensaje es escrito en una matriz y luego la misma se transpone. Ej:



Los algoritmos de encriptación actuales, utilizan los métodos de sustitución y transposición combinados y transformaciones mediante funciones matemáticas. A continuación detallamos los más utilizados.

a) Algoritmos de llaves simétricas

Son llamados así los algoritmos que usan la misma llave para encriptar y para desencriptar. Son más rápidos que los de llave pública y más sencillos de implementar. Un problema es que para poder intercambiar mensajes de forma segura, ambas partes deben primero intercambiarse la llave de forma segura ya que si un receptor no autorizado posee la llave podrá desencriptar los mensajes.

Este tipo de algoritmo es aun muy utilizado debido a su rapidez.

La fortaleza[13] de los algoritmos de llaves simétricas depende de los siguientes factores:

- ?? Confidencialidad de la llave.
- ?? Dificultad de adivinar la llave.
- ?? Dificultad de forzar el algoritmo de encriptación.
- ?? Ausencia de puertas traseras, es decir huecos de seguridad que permitan desencriptar el mensaje sin tener la llave.
- ?? La posibilidad de desencriptar un mensaje si se conoce una parte de él (ataque de piedra roseta).

[13] Capacidad del algoritmo de proteger a la información contra un ataque.

Lamentablemente es muy difícil probar la fortaleza criptográfica. Generalmente se prueba la debilidad de un algoritmo que a veces ya se encontraba difundido como seguro. La verdadera seguridad criptográfica está en publicar el algoritmo y esperar a que no se le encuentren errores

Los ataques más comunes que reciben este tipo de sistemas son algunos de los siguientes:

?? **Ataque de búsqueda de llaves (fuerza bruta):** Si el violador de códigos tiene la capacidad de reconocer el resultado de utilizar la llave correcta, entonces el método más simple de violar la encriptación es probar todas las llaves posibles. Casi todas fallarán pero al final alguna tendrá éxito, cómo se grafica en la Figura R. La forma de protegernos contra este tipo de ataques es que el universo de llaves posibles sea suficientemente grande para evitar que se prueben todas. Por ejemplo. En Internet se utilizan, generalmente llaves de 128 bits. Esto permite 2^{128} (3.4×10^{38}) llaves posibles, un número suficientemente grande como para evitar que alguien se ponga probar de a una. Hasta con ayuda de procesadores que intenten violar el código se tomaría varios miles de años hasta descifrar el código.

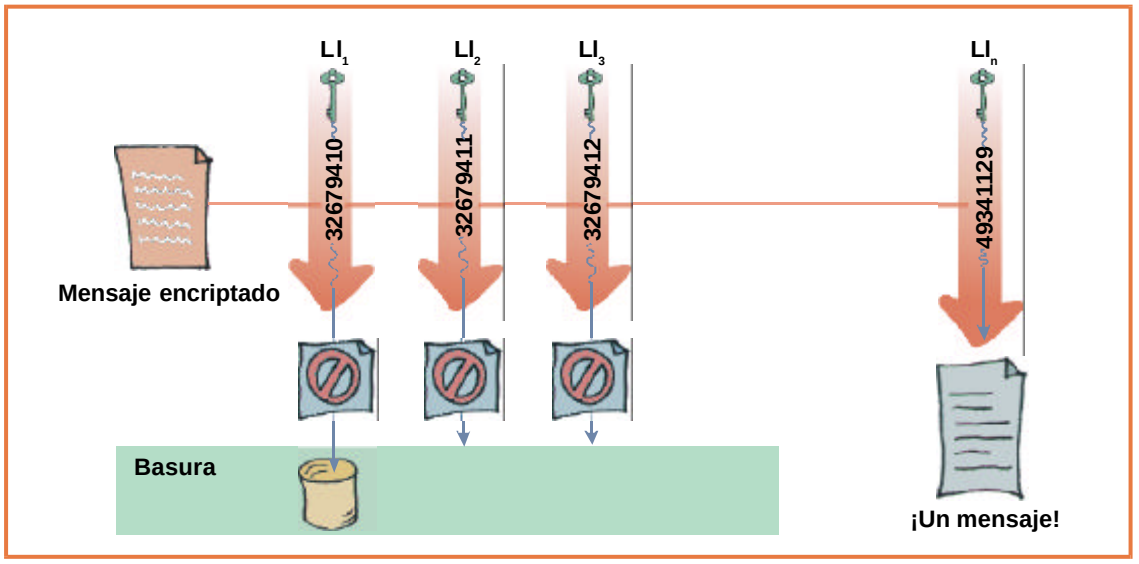


Figura R.: Ataque de fuerza bruta.

?? **Criptoanálisis:** La mayoría de los algoritmos de encriptación pueden ser vencidos mediante la combinación de matemáticas y poder de cómputo. Por lo que casi nunca es necesario, para violar un código, el intentar el método de la fuerza bruta. Un criptoanalista (persona que rompe códigos) puede descifrar el texto encriptado sin necesidad de tener la llave y sin saber el código de encriptación. Un tipo de criptoanálisis es el ataque de piedra roseta en el que el violador tiene parte del mensaje desencriptado y la misma parte

encriptada; con este tipo de ataque el violador obtendrá primero el algoritmo de encriptación, el que luego puede utilizar para intentar inferir el algoritmo de desencriptación para así descifrar el mensaje.

?? **Ataques basados en el sistema:** Esta forma de ataque se basa en buscar debilidades en el sistema que utiliza el algoritmo criptográfico sin atacar al algoritmo en sí. Un ejemplo es el caso de una violación en la seguridad de Netscape que utiliza una llave aleatoria[14]. Pero el generador de números aleatorios de Netscape no era un buen generador por lo que se podía alterar la semilla del generador y predecir el número aleatorio generado, pudiendo así adivinar la llave.

b) Algoritmos de llave pública

En este tipo de algoritmos se utiliza una llave para encriptar y otra para desencriptar. De esta forma los sujetos que desean intercambiar mensajes pueden intercambiarse la llave pública encriptadora de forma no segura y conservar la llave desencriptadora. Este principio es el mismo que se usa en las firmas digitales. El problema más grave de este sistema es que es muy lento, entre diez y cien veces más que el sistema de llaves simétricas.

Ha habido mucho menos desarrollo de algoritmos de llave pública que de llave simétrica ya que para crear un algoritmo de llave simétrica sólo hace falta idear una forma de hacer la revoltura de datos, de forma confiable y suficientemente intrincada como para que no sea fácil deducir el algoritmo de desencriptación. En cambio, los algoritmos de llave pública se basan en la teoría numérica por lo que el desarrollo de un algoritmo nuevo implica encontrar un paradigma matemático de características especiales.

Los ataques más comunes que reciben este tipo de sistemas son los siguientes:

?? **Ataques de factorización:** Intentan derivar la llave secreta a partir de la llave pública, de la que el atacante tiene una copia. Este ataque necesi-

[14] En gran parte de los sistemas criptográficos usados actualmente se hace necesario generar números aleatorios, sin embargo, es conocido que es una tarea difícil de llevar a cabo, por lo que se opta por generar números pseudoaleatorios, es decir, números que están cerca de ser aleatorios. Se dice que un dispositivo o algoritmo genera números pseudoaleatorios si contiene un proceso determinístico, el cual toma como entrada un número que se supone aleatorio, llamado semilla y tiene como salida una sucesión de números "casi" aleatoria.
Para poder considerar que un número es aleatorio, el conjunto de donde es tomado debe de cumplir los requisitos de espacio equiprobable, es decir, que todo elemento tenga la misma probabilidad de ser elegido y que la elección de uno no dependa de la elección del otro. [W-14]

ta resolver problemas matemáticos de alta dificultad como la factorización de números grandes.

?? **Ataques algorítmicos:** Este tipo de ataque consiste en encontrar una falla o debilidad fundamental en el algoritmo en que se basa el problema matemático.

El problema con este tipo de algoritmos es que un defecto en los mismos no necesariamente tiene que ser publicado, lo cual no significa que no exista o no se conozca.

c) Criptosistemas híbridos público / privado

Este sistema se basa en una llave de sesión, que es una llave pública aleatoria que se utiliza para crear un sistema de llaves simétricas. Cada vez que se inicie un intercambio de datos, la llave aleatoria habrá cambiado y se generará una nueva llave simétrica. Este sistema es uno de los más utilizados ya que combina las ventajas de ambos sistemas.

d) Funciones de compendio de mensaje

Este tipo de encriptación genera un patrón de bits único para cada entrada específica. Son como huellas digitales para archivos. Se ilustra en la Figura S.

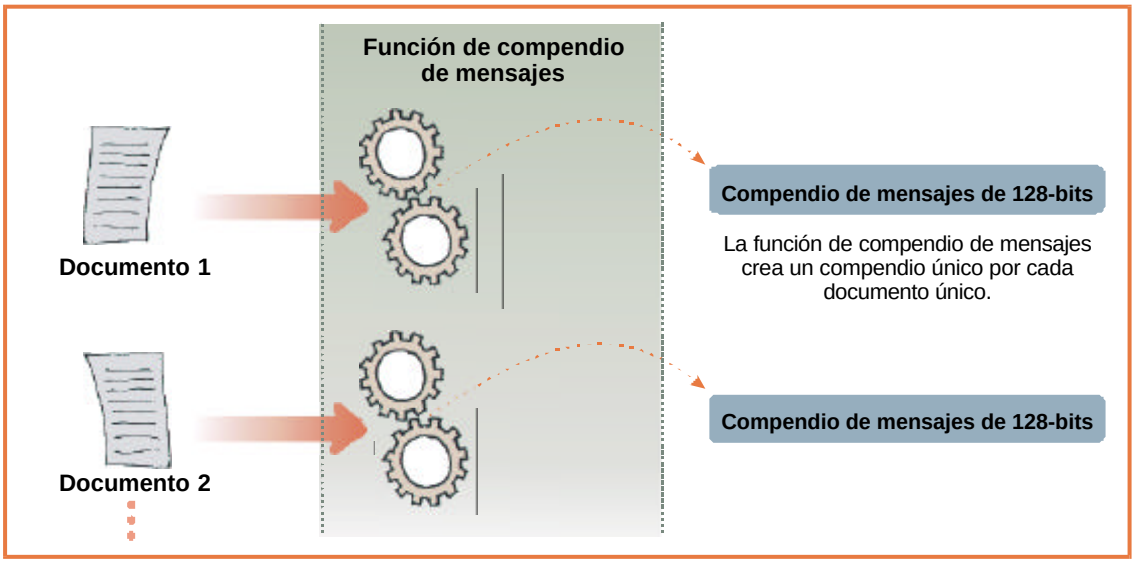


Figura S.: Función de compendio de mensajes.

Este tipo de algoritmo, no se utiliza para encriptar y desencriptar sino para crear firmas digitales, códigos de autorización de mensajes y llaves de encriptación a partir de frases de acceso.

Estas funciones son más rápidas que las funciones criptográficas de llaves simétricas, conservando sus mismas propiedades criptográficas y no tienen restricciones de patente.

La criptografía en la Web

La encriptación es la única tecnología viable para proteger la transacción de datos mientras son transportados de una computadora a otra a través de la red pública.

Las funciones de la encriptación permiten brindar seguridad a un sitio Web mediante los siguientes conceptos:

?? **Confidencialidad:** la encriptación se usa para ocultar información enviada a través de Internet y almacenarla de forma que si alguien intercepta la comunicación no puede acceder al contenido de los datos ya que los mismos le resultan incomprensibles.

?? **Autenticación:** la encriptación es utilizada para realizar firmas digitales, para identificar al autor de un mensaje, comprobando su identidad.

?? **Integridad:** la criptografía sirve también para verificar que un mensaje no ha sido modificado mientras se encontraba en tránsito, ya sea por una voluntad de modificarlo o por un ruido accidental en la línea de comunicación.

?? **No repudiación:** mediante la encriptación se crean remitos de forma que un autor de un mensaje no pueda negar su autoría.

Aunque hay algoritmos de encriptación que cumplen más de una de estas funciones, en la mayoría de los casos se considera mejor utilizar métodos diseñados específicamente para cada función que se quiera lograr en vez de confiar en los beneficios colaterales de otros algoritmos.

Limitaciones de la criptografía

La criptografía en la Web es tan necesaria que muchos usuarios y lo que es peor hasta administradores de sistemas confunden criptografía con seguridad. En realidad, si bien es un elemento importante de la seguridad en la Web, la criptografía sólo nos protege de la intercepción de datos mientras están siendo comunicados entre computadoras,.

La criptografía no es la solución adecuada para muchos problemas, incluyendo los siguientes:

?? **La criptografía no puede proteger los documentos no encriptados**: si el servidor Web está configurado para enviar documentos encriptándolos, pero los documentos originales residen en él. Se podría tener acceso a la información, violando el acceso al servidor.

?? **La criptografía no puede proteger contra el robo de llaves de encriptación**: el sentido de la encriptación reside en que quienes poseen la llave criptográfica puedan desencriptar los archivos o mensajes. Con esto cualquiera que pueda robar, comprar o poseer de algún modo la llave para desencriptar logrará acceder a la información.

?? **La criptografía no puede proteger contra ataques de negación de servicio**[15]: por definición la criptografía intenta proteger la información de interceptores no autorizados. Si un atacante tiene un propósito por el cual no le sea de interés acceder al contenido de la información, la criptografía no será una defensa apropiada.

?? **La criptografía no puede proteger contra el registro de un mensaje ni contra el hecho de que el mensaje haya sido enviado**: en el criptoanálisis el estudio de esta información se conoce como análisis de tráfico y significa que si bien se está ocultando el contenido de los mensajes no se está ocultando el rastro de los mismos y al hacer una auditoría se puede saber que un sujeto **A** ha estado intercambiándose mensajes con otro sujeto **B**.

?? **La criptografía no puede proteger contra un programa de encriptación con trampas**: es posible modificar los algoritmos de encriptación para hacerlos inútiles, esta posibilidad no se puede eliminar, aunque se reduce el riesgo, obteniendo los programas criptográficos de canales confiables y tomar políticas de seguridad para evitar que los mismos sean modificados.

?? **La criptografía no puede proteger contra un traidor o contra un error**: las personas son el eslabón más débil de cualquier sistema. Si una persona dentro de la organización altera o divulga la información protegida criptográficamente, el sistema no tiene manera de proteger la información.

Riesgos de una transacción en línea con encriptación

A continuación se enumeran aquellos riesgos que se corren al transmitir un mensaje en la Web contra los que la encriptación no nos protege. [L-9] [E-1]

?? Riesgo de que la información proporcionada para la transacción sea utilizada en un futuro para fines no deseados, ejemplo correo no deseado.

?? Riesgo de que el comerciante pueda obtener control del navegador del sujeto **A**.

?? Riesgo de que un tercero se infiltre en la comunicación y controle el navegador del sujeto **A**.

?? El sujeto **A** podría proporcionar al comerciante datos falsos y realizar una compra fraudulenta.

?? Un tercero podría violar la computadora del comerciante robando el número de tarjeta de crédito de los clientes y hacer transacciones fraudulentas.

?? Un tercero podría entrar en la computadora del comerciante e introducir datos fraudulentos directamente en su base de datos de pedidos haciéndole creer de esta manera al sistema que ha realizado compras.

?? Un tercero podría alterar la base de datos del comerciante o su página Web o cualquier otro perjuicio imaginable para el comerciante.

Es por todo lo antedicho que la encriptación no es suficiente para asegurar una transacción en línea.

La criptografía en el comercio electrónico

A continuación se describen los protocolos criptográficos más utilizados para la protección de datos en las transacciones de comercio electrónico. Nos detendremos en detalle en el SSL y SET por considerarlos de mayor importancia para los objetivos de este trabajo.

Protocolo de Nivel de conexiones seguro (SSL, Secure Sockets Layer)

Es un protocolo de criptografía que asegura la comunicación bidireccional. Este protocolo se utiliza juntamente con TCP/IP [16]. Ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario; integridad, mediante funciones hash[17] criptográficas especificadas por el usuario, y no re-

[15] Ataque en el que el usuario consume un recurso compartido de forma tal que no deja nada para otros usuarios. Estos ataque son muy difíciles de controlar y de determinar su origen.

[16] TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet, Transfer Control Protocol / Internet Protocol): Define la manera en que la información será separada en paquetes y enviada a través de Internet. También revisa los paquetes recibidos para localizar errores de transmisión.

[17] Las funciones HASH sirven para garantizar la integridad de los textos: Se basan en el código ASCII. Trabajan asignándole un número a cada letra o signo de puntuación. Luego se aplica una función matemática sobre el valor numérico de cada carácter. Cualquier modificación en el texto provoca un cambio en el valor de la función HASH. Al enviar un mensaje electrónicamente se envía también su valor HASH el cual al recibirse se recalcula. Si el valor recibido y el recalculado coinciden se puede saber que el mensaje no ha sido deformado. Recordemos que los textos enviados electrónicamente pueden deformarse, por la intervención de terceras personas, o bien por errores en la transmisión. [W-9]

pudiación, mediante firma digital. La conexión SSL la inicia el cliente por medio de un prefijo especial en el URL; por ejemplo “https:” significa que se iniciará una conexión HTTP encriptada con SSL, mientras que “snews:” significa que se iniciará una conexión TNNP encriptada con SSL. [W-3] [W-9]

El rasgo que distingue a SSL de otros protocolos para comunicaciones seguras, es que se ubica en la pila OSI, entre los niveles de transporte (TCP/IP) y de aplicación (donde se encuentran los conocidos protocolos HTTP para Web, FTP para transferencia de ficheros, SMTP para correo electrónico, Telnet para conexión a máquinas remotas, etc.) como puede observarse en la Figura T. Gracias a esta característica, SSL resulta muy flexible, ya que puede servir para asegurar potencialmente otros servicios además de HTTP para Web, sin más que hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte de datos TCP.

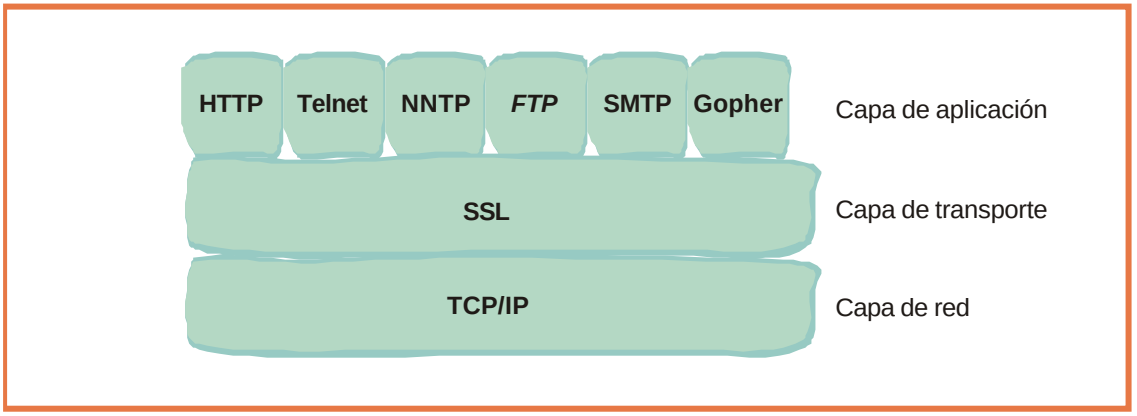


Figura T.:Ubicación de SSL en la capa de transporte.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente y cifrando la clave mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea rota por un atacante en una transacción dada, no sirva para descifrar futuras transacciones.

SSL ganó popularidad en principio porque se necesitaba servidores Web con facilidades criptográficas y un cliente gratuito que implemente los mismos protocolos. Si bien la iniciativa fue de Netscape fue incorporado rápidamente por otros servidores y navegadores Web convirtiéndose en el protocolo criptográfico más popular de Internet.

SSL en el comercio electrónico

El propósito y el éxito de SSL es su transparencia para usuarios y desarrolladores. Suponiendo que el servidor Web tenga facilidades criptográficas que soporten SSL y que el cliente esté accediendo con un navegador que reconozca SSL (cualquiera de los navegadores popularmente difundidos), bastará reemplazar el "http" del URL por "https" de esta forma el cliente obtendrá de forma segura el contenido de la página y lo más importante, realizando este reemplazo al enviar información al servidor Web, se hará también de forma segura. Por ejemplo en un formulario CGI en lugar de poner :

<form metod=POST action="http://www.nombre.com/cgi-bin/formulario">

el programador deberá poner

<form metod=POST action="https://www.nombre.com/cgi-bin/formulario">

La elección de algoritmos y longitudes de llaves la determinará el servidor SSL limitado por el cliente de acuerdo al intercambio de notas electrónicas antedichas.

Los navegadores muestran un pequeño icono cuando una página es descargada con SSL. En el Internet Explorer este icono es un candado que está cerrado si la página fue descargada con SSL y abierto de lo contrario o no aparece el candado, dependiendo de la versión. Lo graficamos en la Figura U.

Características de SSL

- La encriptación y desencriptación no se repite para cada comunicación entre el cliente y el servidor, permitiendo que las nuevas conexiones SSL se inicien de inmediato aportando eficiencia al proceso.
- Permite la autenticación tanto del cliente como del servidor mediante certificados digitales.
- Aunque SSL fue diseñado para correr sobre TCP/IP, puede hacerlo sobre cualquier protocolo confiable orientado a conexiones como X.25[18] u OSI[19].

[18] El protocolo X.25 fue diseñado para evitar que las redes procedentes de diferentes países lleguen a desarrollar interfases mutuamente incompatibles en 1974.

[19] El modelo OSI (Sistema de Interconexión Abierta, Open Systems Interconection) de telecomunicaciones esta basado en una propuesta desarrollada por la organización de estándares internacional (ISO, International Standards Organization), por lo que también se le conoce como modelo ISO - OSI. Su función es la de definir la forma en que se comunican los sistemas abiertos de telecomunicaciones, es decir, los sistemas que se comunican con otros sistemas.

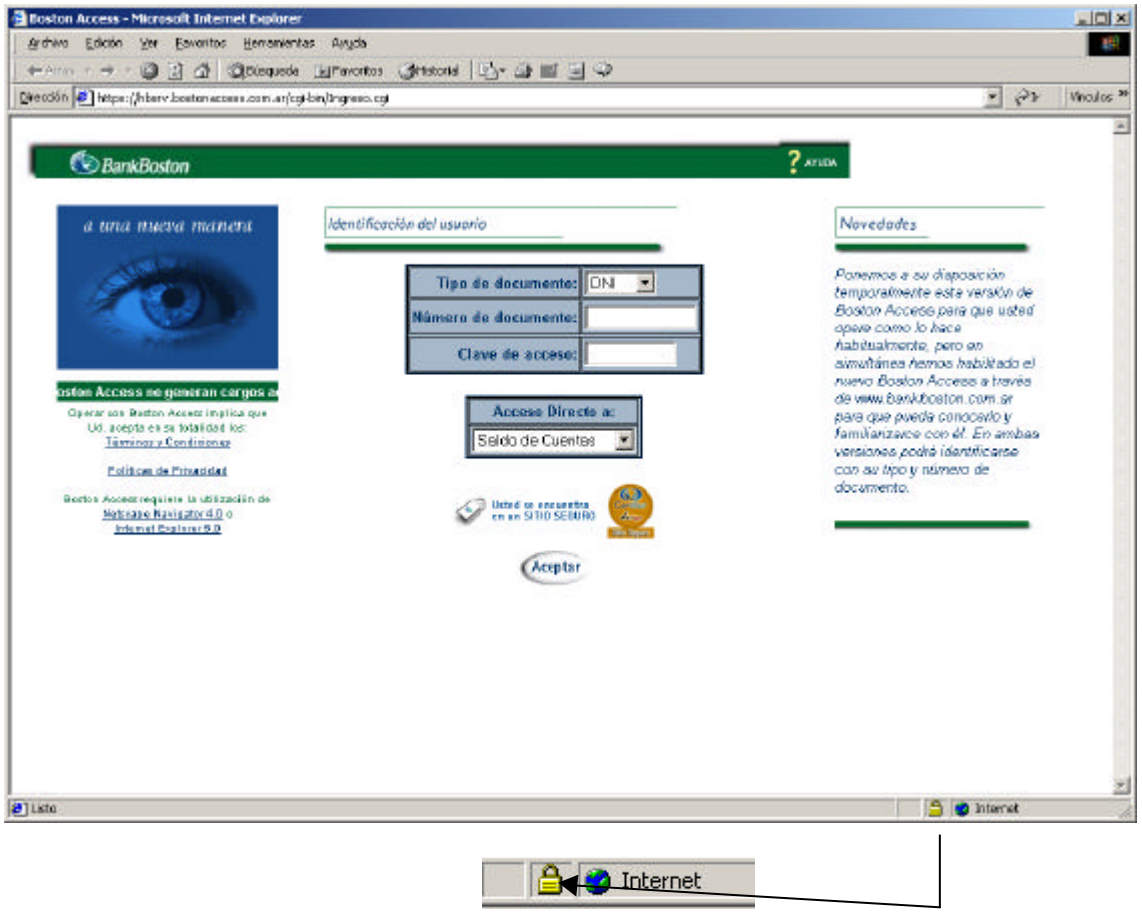


Figura U.: Icono indicador de que la página usa un protocolo de encriptación para transferencia de datos.

?? Protege contra ataques conocidos como “hombre en el camino”, explicado con anterioridad. Esto lo hace mediante certificados digitales para permitir al usuario de la Web conocer el nombre validado del sitio con el que se está conectando.

?? Disminuye notablemente la velocidad de transmisión de información. El desempeño se degrada, mayormente, en el inicio de la primera conexión ya que es cuando se produce la encriptación / desencriptación de la llave pública. Debido a esto, muchas organizaciones tienden a encriptar sólo información sensible, dejando la mayoría de la transacción vulnerable a un ataque. Por ejemplo, al obrar de esta manera, un HTML no encriptado podría ser modificado por un programa de filtrado e inyección de paquetes que cambien el código del formulario HTML y en lugar de enviar el nro de tarjeta de crédito al servidor legal, lo haga a otro servidor en cualquier lado del mundo. Suponiendo que el pirata obtenga una identificación digital para su servidor SSL, sería muy difícil que un usuario engañado detecte la maniobra.

?? Es una capa entre el protocolo TCP/IP y la aplicación, que agrega autenticación y no repudiación del servidor y autenticación, del cliente mediante firmas digitales.

?? Confidencialidad de los datos mediante encriptación.

?? Integridad de los datos mediante códigos de autenticación de mensajes.

?? Es extensible y adaptativo, condición necesaria ya que la criptografía es un campo que se transforma con gran rapidez y los protocolos no funcionan a menos que ambas partes de la comunicación utilicen los mismos algoritmos. Cuando un programa intenta comunicarse con otro utilizando SSL se intercambian notas electrónicas para determinar el protocolo criptográfico más fuerte que tienen en común.

Implementación del protocolo

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Como mostramos en la Figura V.

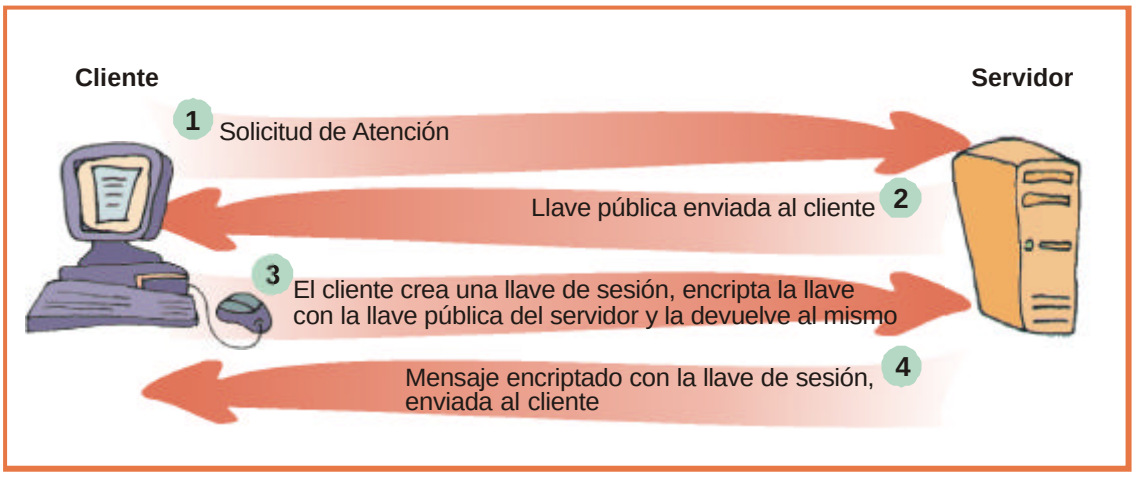


Figura V.: Intercambio de mensajes cliente – servidor en el protocolo SSL.

Este protocolo sigue las siguientes fases:

?? **La fase Hello**, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

?? **La fase de autenticación**, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).

?? **La fase de creación de clave de sesión**, en la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos intercambiados posteriormente haciendo uso del algoritmo

de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.

?? **La fase Fin**, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras HTTP.

El protocolo SSL se divide en dos capas complementarias

1. **Protocolo Handshake**. Realiza las siguientes funciones:

   ?? Autenticación de usuario y servidor.
   ?? Selección de los parámetros de la sesión y de la conexión.
   ?? Establece la conexión segura.

2. **Protocolo de registro (Record protocol)**. Se utiliza para la encriptación de los protocolos de las capas más altas: Handshake y aplicaciones.

El protocolo SSL se comporta como una máquina de estados, durante el intercambio de información siempre hay un estado de escritura activo y otro pendiente. Entre dos entidades cliente y servidor se pueden abrir varias sesiones SSL, aunque no es habitual, y dentro de cada sesión se pueden mantener varias conexiones SSL. Las conexiones se abren o cierran a través del protocolo de Handshake.

Evaluación del protocolo

Si bien SSL provee un enfoque práctico y fácil de implementar, no ofrece una solución comercialmente integrada ni totalmente segura. A medida que el comercio crece, esta arquitectura podría llegar a resultar difícil de expandir o de incorporar nuevas tecnologías y componentes a medida que vayan apareciendo. Existen una serie de desventajas al utilizar exclusivamente SSL para llevar adelante ventas por Internet:

?? SSL ofrece un canal seguro para el envío de números de tarjeta de crédito, pero carece de capacidad para completar el resto del proceso comercial: verificar la validez del número de tarjeta recibido, autorizar la transac-

ción con el banco del cliente, y procesar el resto de la operación con el banco adquiriente y emisor.

?? Es importante recalcar que SSL sólo garantiza la confidencialidad e integridad de los datos en tránsito, ni antes ni después. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, el DNI, etc., SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito.

?? SSL permite realizar ataques sobre servidores de comercio creados de forma poco confiable, para averiguar números de tarjeta reales. Un programa escrito por un hacker va probando números de tarjeta válidos, pero que no se sabe si corresponden o no a cuentas reales, realizando compras ficticias en numerosos servidores. Si el número de tarjeta no sirve, el servidor devuelve un error, mientras que si es auténtico, el servidor lo acepta. El programa entonces cancela la compra y registra el número averiguado, para seguir adelante con el proceso. De esta forma, el hacker puede hacerse en breve con cientos de números auténticos.

?? Permite ataques a la versión del protocolo. Las nuevas versiones del protocolo van siendo mucho más seguras que las anteriores, por lo que un ataque común es hacer que los browsers y servidores que soportan SSL crean que deben utilizar versiones anteriores de SSL por cuestiones de compatibilidad. Esto puede lograse mediante una intercepción en el handshake: El servidor “cree” que el cliente sólo soporta una versión anterior de SSL y utilizará este protocolo para encriptar los datos. Tomando todas las debilidades de esa versión.

?? SSL, también es permeable a ataques al algoritmo de encriptación. De forma similar que en el caso anterior, un atacante podría intervenir el handshake para forzar a ambas parte a utilizar un algoritmo de encriptación menos seguro o con una clave con pocos bits (que permite quebrar la seguridad fácilmente). Por suerte, este tipo de ataque puede ser detectado con técnicas especificas.

?? Ataque de “Hombre en el camino”: Ciertas versiones de SSL utilizan el método de encriptación Diffie-Hellman (DH) que es vulnerable a este tipo de ataques, por lo que no se recomienda su utilización bajo ninguna circunstancia.

Todos estos inconvenientes convierten a SSL en una solución deficiente desde el punto de vista del pago electrónico, lo cual no significa que no se deba utilizar ni que no sea útil en otras muchas facetas igualmente necesarias de la actividad empresarial. **Al proporcionar un canal seguro de comunicaciones, el comerciante puede ofrecer al cliente de manera confidencial una serie de servicios para estrechar las relaciones de confianza: autenticación del cliente frente al comercio, trato personalizado, evitar que terceras partes**

espíen las compras de los clientes, intercambio de información privada, etc.

Dado que SSL es un protocolo seguro de propósito general, que no fue diseñado para el comercio en particular, se hace necesaria la existencia de un protocolo específico para el pago. Este protocolo existe y se conoce como SET.

Protocolo de Transacciones Electrónicas Seguras (SET, Secure Electronic Transactions)

Este protocolo criptográfico ha sido diseñado especialmente para el envío de números de tarjetas de crédito por Internet. Consta de tres partes: una "billetera electrónica" que reside en la computadora del usuario; un servidor que se ejecuta en el sitio Web del comerciante; y un servicio de pagos SET que se ejecuta en el banco del comerciante. Para utilizar este sistema el usuario introduce su número de tarjeta de crédito en el software de billetera electrónica, el cual se almacena encriptado en el disco duro; se crea también una llave pública y una privada para encriptar la información financiera antes de enviarla a través de Internet. Cuando un usuario desea comprar algo, su número de tarjeta de crédito es enviado encriptado al comerciante quien firma digitalmente el mensaje de pago y lo envía al banco, donde el servidor de pagos desencripta la información y realiza el cargo a la tarjeta. [W-4]

Características de SET

?? El número de tarjeta de crédito pasa encriptado por las manos del comerciante disminuyendo enormemente las posibilidades de fraude, ya que, pese al imaginario popular, en su mayoría los fraudes con tarjetas de crédito en todo el mundo se deben más a los comerciantes y sus empleados que a los "maliciosos" hackers que aguardan agazapados detrás de nuestra computadora con el único fin de robarnos. Esta es su principal ventaja.

?? Encripta los números de tarjetas de crédito mediante el algoritmo RSA, brindando confidencialidad, proporciona además integridad, autenticación y no repudiación mediante funciones de compendio de mensajes y firmas digitales. Sin embargo SET protege sólo el número de tarjeta de crédito no brindando confidencialidad y privacía a los demás elementos de la transacción.

?? Es un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras.

?? Todas las partes implicadas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden autenticarse mutuamente mediante certificados digitales. De esta forma, el comerciante puede asegurarse de la identidad del titular de la tarjeta y el cliente, de la identidad del comerciante. Se evitan así fraudes debidos a usos ilícitos de tarjetas y a falsificaciones de comercios en Internet imitando grandes Web comerciales. Por su parte, los bancos pueden verificar así las identidades del titular y del comerciante.

?? La información de pago se cifra para que no pueda ser espiada. Es decir, solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere cifrar el resto de datos de la compra, como por ejemplo qué artículos se han comprado, debe recurrirse a un protocolo de nivel inferior como SSL.

?? Garantiza que la información intercambiada no podrá ser alterada de manera accidental o maliciosa mientras viaja a través de la red. Para lograrlo se utilizan algoritmos de firma digital.

?? Gestiona tareas asociadas a la actividad comercial de gran importancia como registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

Implementación del protocolo

El pago mediante tarjeta es un proceso complejo en el cual se ven implicadas varias entidades, graficadas en la Figura W.

• **Comprador:** Adquiere un producto utilizando la tarjeta de crédito de su propiedad.
• **Banco o entidad financiera:** Emite la tarjeta de crédito del comprador.
• **Comerciante:** Vende los productos.
• **Banco del comerciante:** Banco donde el comerciante tiene la cuenta.
• **Pasarela de pagos:** Gestiona la interacción con los bancos. Puede ser una entidad independiente o el mismo banco del comerciante.

Dos agentes relacionados pero que no actúan directamente en las transacciones son:

• **Propietario de la marca de la tarjeta:** Avalan las tarjetas: Visa, MasterCard, American Expres, etc...
• **Autoridad de certificación:** Crea los certificados que se utilizan en las transacciones de la pasarela, el vendedor y el comprador. Pueden ser los bancos, los propietarios de la marca de la tarjeta o entidades independientes.

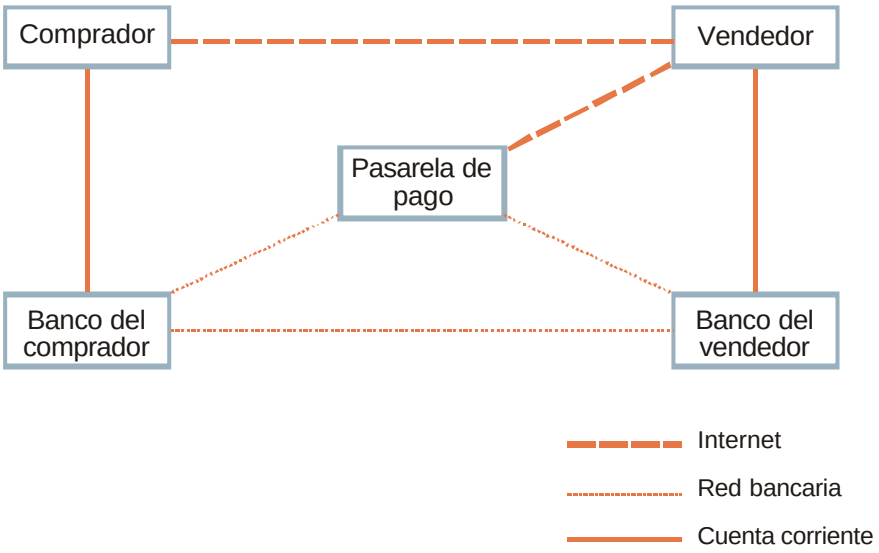


Figura W.: Actores de SET.

Para poder utilizar el SET se deben incorporar unos módulos de software que adaptan los programas existentes al protocolo. Se han definido 4 módulos:

• **Cartera:** Es una aplicación que se instala en el navegador del comprador como plug-in.
• **De venta:** Se conecta a la Web del vendedor, similar a un Punto de Venta (POS, Point Of Sale) para tarjetas de crédito.
• **Pasarela de pagos:** Cumple las funciones de este agente.
• **Autoridad de certificación:** Crea certificados de clave pública adaptados al estándar SET.

Una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito y consta de los siguientes pasos:

1. *Decisión de compra del cliente*. El cliente está navegando por el sitio web del comerciante y decide comprar un artículo. Para ello llenará algún formulario a tal efecto y posiblemente hará uso de alguna aplicación de carrito de compras, para ir almacenando diversos artículos y pagarlos todos al final. El protocolo SET se inicia cuando el comprador pulsa el botón de Pagar.
2. *Arranque del monedero*. El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.
3. *El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante*. La aplicación monedero crea dos mensajes que envía al comerciante. El primero, con la información del pedido; el segundo con las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el software monedero del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni

el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.

4. *El comerciante envía la petición de pago a su banco*. El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante acerca de la misma, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago (que el comerciante no puede examinar, ya que van cifradas con la clave pública del adquiriente).

5. *El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente*. El banco del comerciante descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene a continuación las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso (el enviado por el comerciante y el codificado en las instrucciones de pago) y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.

6. *El emisor autoriza el pago*. El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.

7. *El adquiriente envía al comerciante un testigo de transferencia de fondos*. En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.

8. *El comerciante envía un recibo al monedero del cliente*. Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados.

9. *El comerciante usa el testigo de transferencia de fondos para cobrar el importe de la transacción*. Después de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.

A su debido tiempo, el dinero se descuenta de la cuenta del cliente (cargo).

El protocolo definido por SET especifica el formato de los mensajes, las codificaciones y las operaciones criptográficas que deben usarse. No requiere un método particular de transporte, de manera que los mensajes SET pueden transportarse sobre HTTP en aplicaciones Web, sobre correo electrónico o cualquier otro método. Como los mensajes no necesitan transmitirse en tiempo

real, se puede realizar implementaciones basadas en correo electrónico u otros sistemas asíncronos.

Otros protocolos para asegurar la información en tránsito

A continuación, enunciamos un conjunto de protocolos que si bien son menos utilizados en el comercio electrónico tienen aplicabilidad.

?? **Protocolo Privacía Bastante Segura (PGP, Pretty Good Privacy):** es un sistema de encriptación híbrido que utiliza encriptación de llave pública RSA para la administración de llaves y un código simétrico para la encriptación de datos. PGP es un desarrollo de PGP Inc que comercializa este producto como un programa integrado de correo electrónico o como un agregado para los sistemas de correo más populares, permitiendo enviar y recibir mensajes encriptados con PGP. PGP tiene problemas en la administración y certificación de sus llaves públicas ya que las mismas nunca expiran; la habilidad de PGP para certificar la identidad en forma confiable es muy limitada ya que no tiene una infraestructura de llaves públicas para validar la autenticidad de las llaves.

?? **Protocolo de Extensiones Multipropósito de Correo de Internet Seguro (S/MIME, Secure Multipurpose Internet Mail Extensions):** este sistema ofrece confidencialidad mediante algoritmos de encriptación especificados por el usuario, integridad mediante una función de hash, autenticación mediante certificado de llave pública X.509 v3 y no repudiación mediante firma digital. Para enviar un correo electrónico encriptado con S/MIME es necesario tener una copia de sus llaves privadas, las que se pueden obtener en VeriSign y otras autoridades certificadoras. Se espera que los sistemas de correo electrónico adopten S/MIME en lugar de PGP debido a que las principales empresas ya tienen una relación de negocios con RSA que es la autora de este sistema de encriptación.

?? **Protocolo de Seguridad de Capa de Transporte (TSL, Transport Secure Layer)**: Intento de estandarización de protocolos de seguridad en la capa de transporte muy similar a SSL 3.0.

?? **Protocolo de Tecnología de Comunicaciones Seguras (PCT, Private Communications Technology):** Es un protocolo de seguridad de nivel de transporte similar a SSL pero propietario de Microsoft que surgió como respuesta a problemas asociados con SSL 2.0 que fueron luego corregidos en la versión SSL 3.0; si bien Microsoft soporta SSL, continúa manteniendo PCT por cuestiones políticas.

?? **Protocolo de HTTP Seguro (S-HTTP, Secure HTTP):** Es un sistema para firmar y encriptar información enviada mediante el protocolo HTTP.

Este sistema es precursor de SSL y actualmente cae en desuso al verse reemplazado por el mismo. Fue desarrollado por Tecnologías de Integración Empresarial (EIT, Enterprise Integration Technologies).

Permite el intercambio seguro de archivos en la Web, mediante el encriptado y la certificación digital. La mayor diferencia con SSL es que el servidor solamente es autenticado mientras que en este protocolo el cliente también envía un certificado.

La implementación se realiza a través de la extensión de las cabeceras HTTP. En el momento que se establece la conexión para enviar el archivo se acuerda el sistema a utilizar.

Generalmente un mensaje S-HTTP consiste de tres partes:

a. El mensaje HTTP
b. Las preferencias criptográficas del emisor
c. Las preferencias criptográficas del receptor

La desventaja esencial de este protocolo es que el envío de certificados / autenticación debe realizarse por cada archivo que se desea transmitir, lo que puede producir una sobrecarga de transacciones en el servidor si se envían muchos archivos seguros por conexión, además de que la implementación de aplicaciones de comercio electrónico es mucho más compleja ya que deben considerarse aspectos como certificados de cliente, método de encriptación a utilizar, etc.

?? **Protocolo de Kerberos:** Sistema de seguridad de red desarrollado por el MIT (Instituto de Tecnología de Massachussets, Massachusetts Institute of Technology). A diferencia de los otros sistemas mencionados no posee tecnología de llaves públicas ya que en el momento en que se lo desarrolló (1985) los procesadores eran muy lentos y no soportaban la encriptación y desencriptación por medio de llaves públicas. Este sistema se basa en códigos simétrico y en secretos compartidos entre el servidor Kerberos y cada usuario quien tiene su propia clave de acceso. El servidor Kerberos encripta los mensajes enviados por el usuario de forma que no puedan leerlos nadie más. Es un sistema difícil de configurar y de administrar y que no cuadra con los actuales estándares de seguridad. Aunque se encuentra bastante generalizado en los servicios Telnet, FTP, POP y RPC.

?? **Protocolo de Interprete de Comandos Seguro (SSH, Secure Shell):** Es un protocolo de terminal remota encriptada.

?? **Seguridad del Sistema de Nombre de Dominio (DNSSEC, Domain Name System Security):** Proporciona seguridad al sistema de nombres de dominio de Internet

?? **Protocolo de Internet Seguro (IPsec, Internet Protocol Secure):** Protocolo de bajo nivel para encriptar paquetes IP utilizado para crear redes virtuales privadas a través de Internet.

Como proteger un sitio Web

La seguridad en la Web comienza por la computadora donde se ejecuta el servidor Web. No se puede construir una receta genérica de como debería ser un sitio seguro, en lugar de eso, analizaremos los problemas más comunes de seguridad que afectan a Internet y las prácticas que permiten aumentar la seguridad, para luego describir las arquitecturas de servidores Web que reducen los riesgos.

Principales problemas de seguridad de las máquinas en la actualidad

Sorprendentemente, los problemas de Internet identificados por los pioneros, siguen siendo los más comunes [L-9]. En 1973 Bob Metcalfe, escribió la RFC 602 (Solicitud de comentarios, Request For Comments, informes elaborados por el grupo de trabajo de redes ARPA). En este documento, transcripto en la Figura X se identifican tres problemas de la red de aquella época:

- Los sitios no estaban asegurados contra ingresos remotos.
- Había gente no autorizada utilizando la red.
- Algunos malhechores irrumpían en las computadoras y en ocasiones bajaban los sistemas sólo por diversión.

La mayoría de estos problemas de seguridad identificados en 1973 perduran hoy en nuestros días:

- Muchos sitios de Internet aun no aseguran sus servidores contra ataques externos.
- Los usuarios continúan eligiendo claves sencillas de deducir con la dificultad de que ahora existen programas que pueden montar un ataque de adivinación de claves probando miles de claves en unos segundos
- Algunos individuos aun derriban sistemas por diversión, y lo seguirán haciendo, pero hay que agregar que otros lo hacen para obtener importantes beneficios financieros. El problema mencionado por Metcalfe de los accesos no autorizados por módems irrestrictos, no se solucionó pero cambio de forma. Para ingresar a la red hoy es necesario un nombre de usuario y contraseña provistos por un proveedor oficial, pero su obtención es muy sencilla y hasta gratuita en muchos casos.

RFC 602

Grupo de trabajo de redes ARPA *Bob Metcalfe (PARC-MAXC)*

Solicitud de comentarios 602 *DIC 1973 NIC #21021*

Las medias estaban cuidadosamente colgadas junto a la chimenea[20]

La red de computadotas ARPA es susceptible a violaciones de seguridad por lo menos por las tres siguientes razones:

1. Los sitios individuales, acostumbrados a las restricciones físicas sobre el acceso de las máquinas, aún no ha tomado suficientes precauciones para asegurar sus sistemas contra el uso remoto no autorizado. Por ejemplo, muchos usuarios aún utilizan claves de acceso fáciles de adivinar: sus nombres de pila, sus iniciales, el nombre de la máquina deletreado a la inversa, una cadena de caracteres fáciles de teclear en secuencia (por ejemplo, ZXCVBNM).

2. El TIP[21] *permite el acceso a ARPANET a un público mucho mayor del supuesto o deseable. Los números de teléfono de los TIP son enviados a grupos de discusión, como si estuvieran garabateados en paredes de casetas telefónicas y baños de hombres. El TIP no requiere ninguna identificación del usuario antes de dar servicio. Por ello, muchas personas, incluidos quienes solían desperdiciar su tiempo robando a la compañía telefónica, obtienen acceso a nuestra media: en forma extremadamente anónima.*

3. Existe una tendencia innata en algunas personas a romper el sistema de alguien. Esta tendencia permanece a pesar de que es bien sabido que es fácil quebrantar sistemas –y aún más fácil tirarlos-.

Todo esto sería bastante gracioso y causa de guiños de ojo y codeos si no fuera por el hecho de que hace poco fueron tiradas por lo menos dos máquinas servidoras principales bajo circunstancias sospechosas, por personas que sabían a que se arriesgaban; en un tercer sistema se divulgó la clave de acceso de Súper Usuario –nada menos que por dos estudiantes de bachillerato de Los Ángeles-.

Sospechamos que el número de violaciones peligrosas a la seguridad es mayor de lo que ninguno de nosotros cree y que está creciendo. Por ello hay que recomendar no sentarse "en espera de que llegue Santa Claus".

RMV: mv

Figura X: Trascripción de la RFC 602

Prácticas que permiten aumentar la seguridad

Aunque es imposible protegerse contra todas las amenazas existen métodos muy difundidos en la Internet actual, que hacen que la seguridad del servidor sea menos vulnerable. A continuación se tratan algunos de ellos.

[20] El título hace referencia al poema "It was the night before Christmas" ("Era la noche antes de Navidad") muy popular en los Estados Unidos

[21] Procesador de Interfaz Terminal, Terminal Interfaz Processor; era el servidor de modems anónimo de ARPANET

Definir políticas en tiempo de diseño

La seguridad se define mediante políticas. Las mismas no son una receta aplicable a todas las empresas por igual ya que dependerán de los tipos de datos que manejan los sistemas de información. Así en algunos ambientes cualquier usuario puede acceder a los servidores Web e instalar o modificar cualquier página, apagar o reinicializar el sistema mientras que en otros ambientes sólo algunos usuarios podrán acceder con permiso de sólo lectura a algunas páginas y si desearan modificar un archivo necesitarán una autorización firmada por el director del área de sistemas. Estas son distintas políticas.

Las políticas de seguridad son un tema complejo, su función es guiar a los usuarios hacia el conocimiento de las acciones permitidas y a la elección en cuanto a la configuración y uso del sistema. [E-1]

En el momento de crear una política de seguridad, los administradores deberían hacerse las siguientes preguntas:

- ¿Quiénes tendrán acceso?
- ¿Qué tipos de accesos se otorgarán?
- ¿Quién autorizará los accesos?
- ¿Quién será el responsable de la seguridad, de las actualizaciones, de los respaldos y del mantenimiento?
- ¿Qué tipo de material es permitido en las páginas?
- ¿A qué sitios y usuarios externos se les permitirá acceso a las páginas e información?
- ¿Qué tipos de pruebas y evaluaciones deben hacerse al software antes de instalarlo?
- ¿Cómo se manejarán las incidencias acerca del servidor y de la información?
- ¿Cómo se reaccionará ante un incidente de seguridad?
- ¿Cómo y cuándo debe actualizarse la política?
- ¿Quién es el representante ante miembros externos a la organización ante un incidente de seguridad?
- Ante una falla, ¿se seguirá brindando servicio?
- ¿Se tomará el criterio de negación preestablecida (lo que no está permitido está expresamente prohibido) o de permiso preestablecido (lo que no está prohibido expresamente está permitido)?

Las políticas de seguridad deben estar al alcance y disposición de todas las personas asociadas a la organización y **en algunos casos es aconsejable difundirlas externamente para generar confianza en los usuarios externos**.

Si se pone especial cuidado en el desarrollo de las políticas es posible evitar muchos problemas potenciales. Pero para constituir las políticas de seguridad se debe ir contra la cultura de muchas organizaciones que ponderan el **hacer** sobre el **planificar**. Para cambiar esta situación se debe comprender la importancia de los planes y los beneficios en tiempo, costo y calidad de los procesos planificados sobre los improvisados. No es fácil pero nunca debemos perder de vista que una organización es la suma de los miembros que la componen.

Prevenir la intercepción de claves de acceso

El envío de claves de acceso reutilizables en texto llano a través de redes internas y externas, es tal vez el riesgo de seguridad más importante que se corre en Internet. Por ejemplo al utilizar el servicio FTP para actualizar páginas Web, el nombre de usuario y la clave viajan por la red sin ser encriptados de modo de que si alguien está monitoreando la red obtendrá acceso al servidor ya que la clave es reutilizable hasta que el propietario la cambie.

La única forma de prevenirse contra la intercepción de claves es no enviar las mismas en texto llano y que las mismas no sean reutilizables.

Utilizar herramientas de seguridad

Son programas que se utilizan para evaluar o mejorar la seguridad de un sitio. Las podemos dividir en cuatro categorías:

?? ***Herramientas de instantánea*:** estos sistemas toman una foto del servidor y buscan debilidades potenciales notificándolas a la persona que la ejecuta, se caracterizan por hacer muchas revisiones en poco tiempo. También se las conoce como herramienta de auditoría estática. Estos programas deben ejecutarse con regularidad y se debe evaluar con mucho cuidado la salida que producen, ya que en ellos se pueden encontrar los agujeros de seguridad del sistema.

?? ***Herramientas de detección de cambios no autorizados*:** cuando un atacante ingresa en un sitio restringido lo primero que suele hacer es crear puertas traseras que le faciliten futuros ingresos al sistema y también modificar el mismo para ocultar evidencia de intrusión. Dejando a su paso

cambios no autorizados en el sistema. El hecho de encontrar estos cambios no evita la irrupción pero puede indicar que el sistema ha sido violado.

?? ***Herramientas que escudriñan la red, buscando debilidades en ella*:** estas herramientas buscan errores de programación conocidos relacionados con la seguridad. Es sabido que los crackers escudriñan la red con estas herramientas, así que lo mejor es utilizar uno mismo estos programas para mantenerse consciente de las falencias de nuestro sistema.

?? ***Herramientas que monitorean el sistema y la red buscando ataques en progreso*:** estas herramientas funcionan como alarma antirrobo registrando la computadora mientras opera, en busca de señales de una irrupción.

Evitar fallas y errores de programación

"La mayoría de los problemas de seguridad son errores o trampas de programación." [L-9]

Una de las cosas más peligrosas que se puede hacer estando conectado a Internet es descargar y ejecutar un programa ya que la mayoría de los sistemas operativos no controla lo que un programa puede hacer una vez que se está ejecutando. Por lo tanto al ejecutar un programa descargado de Internet ponemos toda nuestra computadora y hasta nuestra red en manos del autor del programa. Aunque la mayoría de estos programas se comportan como se espera; muchos tienen errores de programación, son hostiles, buscan la información almacenada y la transmiten a algún lugar de Internet o realizan algún otro tipo de fraude.

Es imposible determinar lo que hará un programa antes de ejecutarlo y a veces es imposible determinar qué ha hecho un programa después de ejecutarlo, ni siquiera NT, W2K o UNIX que son sistemas operativos con extensos mecanismos de seguridad, ofrecen a los usuarios una seguridad real contra los programas descargados y ejecutados ya que una vez que se corre el programa éste hereda todos los privilegios y derechos de acceso del usuario que lo ha invocado y la mayoría de los usuarios de Internet descargan y ejecutan programas como una tarea diaria.

Los atacantes buscan hurgar documentos confidenciales para transmitirlos a otros sistemas, dañar la información o el hardware del usuario, crear agujeros en la seguridad de los sistemas, realizar fraudes.

Mediante aplicaciones auxiliares es posible extender las funciones del navegador. Estas brindan una forma flexible y extensible de mostrar la información, pero también pueden crear problemas de seguridad.

Existen también varios lenguajes de programación (Java, JavaScript, Visual Basic Script) que se utilizan para escribir programas que se incluyen en las páginas Web para descargarse en el navegador del usuario y ejecutarse en su máquina los cuales también crean problemas de seguridad.

El 5 de julio de 2002 la compañía Euro Trust 112 difundió el descubrimiento de un agujero de seguridad que afecta a todas las versiones del navegador Internet Explorer de Microsoft [L-9]. Debido a esta vulnerabilidad, al presionar la tecla 'Ctrl' mientras se navega por Internet se corre el riesgo de que intrusos bajen contenidos de la computadora del usuario. Internet Explorer posibilita al usuario para usar la tecla 'Ctrl' en combinación con otras para ejecutar funciones de uso corriente, al igual que sucede con otros programas. Así, para imprimir una página se puede presionar 'Ctrl+P' y para abrir una nueva ventaja se puede hacer lo propio con 'Ctrl+N'. El agujero se produce por un 'script'[22] en una página HTML, que se puede ejecutar con menos restricciones que lo normal, al inducir al usuario a iniciarlo presionando la tecla 'Ctrl'. De este modo, el 'script' puede ser usado para acceder al disco rígido de la víctima, sin que ésta sospeche lo que está ocurriendo. Según Euro Trust 112, Microsoft señaló que el problema descripto no le compete según su política de seguridad, por lo que no tiene contemplado crear un parche o código reparador para su navegador. [23]

A continuación se enumeran algunos factores a tener en cuenta a la hora de comprar software:

- La reputación del proveedor en producir software exento de errores y bien documentado.
- Si el proveedor responde en forma oportuna y abierta a reportes de fallas de seguridad relativas a sus productos.
- Pruebas de buenas prácticas de ingeniería de software en el diseño, codificación y evaluación.
- Documentación de pruebas relativas a la seguridad.
- Políticas de respuesta a fallas en el producto del proveedor.

[22] Conjunto de caracteres formado por mandatos y secuencias de tecleo, que se utiliza muy a menudo en Internet para automatizar tareas muy habituales.
[23] Este es sólo un ejemplo de falla seguridad detectada en los navegadores. Una lista actualizada de encuentra en [W-19]

?? Garantía de notificación a los clientes de fallas de seguridad descubiertas en sus productos.

Cuando una falla de seguridad o error de programación es descubierto en un sistema comercial suele enviarse rápidamente la información por todo el mundo por lo tanto el administrador de un servidor debe leer todos los boletines emitidos por los proveedores e instalar parches tan pronto como estén disponibles ya que es posible que un atacante pueda enterarse de que la puerta está sin llave antes que el dueño de la casa. Existen grupos de correo para mantenerse informado de fallas y correcciones en los sistemas, estos foros se llaman FIRST (Foro de Equipos de Respuesta a Incidentes y Seguridad, Forum of Incident Response and Security Teams) para suscribirse a algunos de ellos se debe enviar, por ejemplo un mail en blanco a nt-security@iss.net o firewalls@greatcircle.com.

Antes de instalar un parche, debe asegurarse de que el mismo es auténtico, esto es posible gracias a la firma digital. Ya que al instalarlos, si no son auténticos, corremos el riesgo de agregar vulnerabilidad.

Una tecnología de firma digital de código, como el Authenticode, permite saber si el programa fue escrito por quien dice ser, de forma que podemos decidir en que firmas confiamos y el navegador las bajará automáticamente mientras que si en una firma no confiamos no se instalará el programa.

No todos los programas tienen las mismas implicancias de seguridad ya que los mismos pueden estar compilados en código de máquina nativo, el cual se descarga y ejecuta en la máquina del cliente o pueden estar en código byte de Java y ser ejecutado dentro de una máquina virtual.

Para los programas distribuidos como código de máquina la firma de Authenticode se utiliza para decidir si se descarga o no el control, en el caso de los distribuidos como código de byte de Java también puede usarse para determinar qué permiso de acceso se le otorga al ejecutable.

Si una página posee código de máquina y de Java el acceso controlado por capacidades que permite el sistema de Java se anula. Las firmas de Authenticode sólo se verifican al descargar el control de la red con un mensaje como el de la Figura Y. Una vez instalado el control en el disco duro tiene acceso irrestricto.

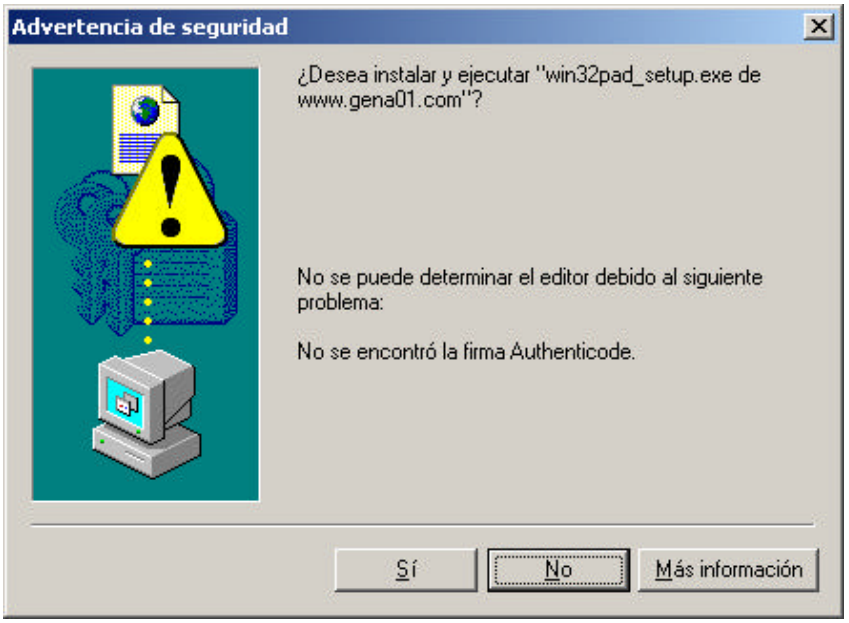


Figura Y.: Mensaje de advertencia cuando no se ha encontrado la firma Authenticode de un soft que se está instalando desde Internet.

La seguridad mediante firma de código tiene muchos problemas, algunos de ellos son los siguientes:

?? Los rastros de auditoría pueden ser borrados por los mismos programas.

?? El daño causado puede no ser visible de inmediato.

?? El Authenticode no protege al usuario contra errores de programación ni contra virus, ni contra el uso incorrecto de programas benignos.

?? Las rutinas de validación que utiliza el sistema Authenticode es vulnerable.

Puede ser difícil o imposible reconstruir un ataque después de ocurrido.

A continuación se enumeran reglas generales para la codificación segura de programas que deben ser tenidas en cuenta por los desarrolladores de sitios web de comercio electrónico:

1. ***Diseño*:** Se debe comprender claramente lo que se intenta construir, considerar el ambiente en que se ejecutará, el comportamiento de entrada y salida, los archivos utilizados, los parámetros reconocidos. Utilizar herramientas adecuadas de diseño y procesos de calidad. Hace no mucho tiempo, el hincapié puesto en el diseño era mínimo. Los recursos fuertes de un proyecto eran puestos en la codificación. Hoy la visión ha cambiado de forma diametral, y el diseño y la arquitectura de un proyecto conforma su parte esencial.

2. ***Verificar los valores proporcionados por el usuario*:** la mayoría de errores de seguridad ocurren cuando el programa recibe un valor o for-

mato inesperado. Esto es evitable verificando los parámetros. Se debe prestar especial atención en el filtrado a que los caracteres sean los adecuados, la longitud sea la permitida y que el valor sea legal.

3. ***Verificar los parámetros enviados al sistema operativo*****:** como se explicó anteriormente al darle acceso al sistema operativo al usuario se debe tener especial cuidado de que las funciones ejecutadas sean las que se esperan.

4. ***Verificar los códigos de retorno del sistema operativo*****:** cuando una llamada al sistema operativo falla se debe registrar en una bitácora el valor inesperado, proporcionando una salida limpia.

5. ***Incluir código de verificación de consistencia interna***: si una variable dentro de un programa sólo se supone que tome una número finito de valores, se debe comprobar que así sea, generando un error en caso contrario.

6. ***Incluir mucha información en las bitácoras*****:** es mejor que sobre información y no que falte, además de la bitácora del servidor Web se deben reportar los errores en bitácoras dedicadas a cada sistema, esto facilitará la localización de problemas.

7. ***Dividir el programa*****:** la modularidad y unicidad van asociadas a la simplicidad y facilidad de mantenimiento y detección de errores. “Divide y vencerás”

8. ***Atacar el código*****:** debe pensar como un atacante y buscar las fallas de seguridad que un atacante buscaría.

9. ***Probar el programa a profundidad.***

10. ***No confiar demasiado en al dirección IP de origen de los paquetes ya que la misma puede ser falsificada o alterada*****.**

11. ***Imponer límite de tiempo de ejecución*****:** si el programa rebasa éstos tiempos es posible que esté bloqueado.

12. ***No utilizar nombre de usuario y clave de acceso en texto llano*****:** si se emplea esta manera de autenticación debe hacerse con facilidades criptográficas.

En 1975 Jerome Saltzer y M. D. Schroeder describieron siete criterios para construir sistemas de cómputos seguros, los cuales son notables aún hoy. Los mismos aparecen entre los procedimientos del Instituto de Ingenieros Electricistas y Electrónicos (IEEE, Institute of Electrical and Electronics Engineers) bajo el nombre de “La Protección de Información en los Sistemas de Cómputos” (The Protection of Information in Computer Systems) que transcribimos a continuación [L-9]

1. ***Mínimo privilegio*****:** cada usuario y proceso debe tener el conjunto mínimo necesario de derecho de acceso. El mínimo privilegio limita el daño que

puedan causar tanto los atacantes como los errores. Los derechos de acceso deben solicitarse explícitamente, no otorgándose de manera preestablecida.

2. ***Economía de mecanismo*:** el diseño del sistema debe ser pequeño y sencillo, de forma que pueda revisarse e implementarse correctamente.

3. ***Mediación completa*:** en todo acceso se debe verificar la autorización adecuada.

4. ***Diseño abierto*:** la seguridad no debe depender de la ignorancia del atacante. Este criterio evita las puertas traseras en el sistema, las cuales otorgan acceso a quienes las conocen.

5. ***Separación de privilegios***: siempre que sea posible, el acceso a los recursos del sistema debe depender de satisfacer más de una condición.

6. ***Mecanismo de mínimo común*:** el sistema debe aislar a unos usuarios de otros. Esto limita tanto el monitoreo encubierto como los esfuerzos cooperativos para saltar los mecanismos de seguridad del sistema.

7. ***Aceptabilidad psicológica*:** los controles de seguridad deben ser fáciles de utilizar de forma de que en verdad se usen y no sean pasados de largo.

Utilizar Firewalls

El firewall es un dispositivo que aísla una red interna del resto de Internet, permitiendo pasar conexiones específicas y aislando otras. Si bien los firewalls son parte de la estrategia global de seguridad de una organización no deben tomarse como la única, debe emplearse sólo para obtener seguridad adicional junto con controles internos, ya que el mismo no protege de ataques internos. [L-5] [L-8]

Existen tres formas de proteger la red interna de ataques externos mediante un firewall:

1. Colocar el servidor Web fuera del firewall. (Figura Z)

En caso que el servidor sea violado el atacante no podrá ingresar al resto de la red. Por otro lado el servidor Web no cuenta con la protección del firewall.

2. Colocar el servidor dentro del firewal. (Figura AA)

De esta forma se evita que los usuarios externos utilicen servicios para los que no están autorizados, pero si se logra subvertir el servidor mediante un ataque se tiene acceso completo a la red interna.

3. Colocar el servidor entre dos firewalls. (Figura BB)

Combina las ventajas de los dos sistemas anteriores pero también las restricciones a los servicios.

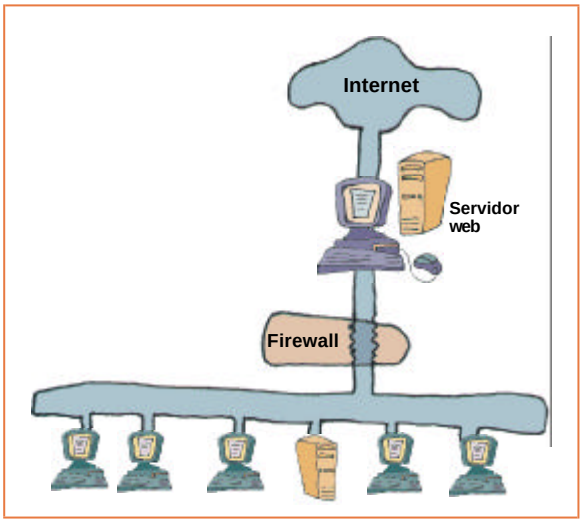


Figura Z.: Servidor Web fuera del firewall.

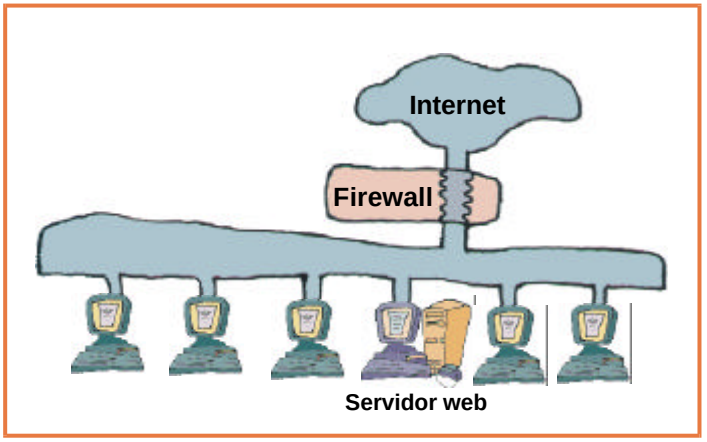


Figura AA.: Servidor Web dentro del firewall.

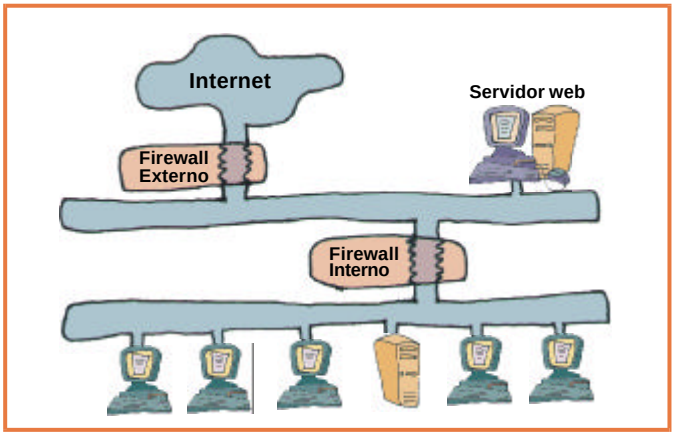


Figura BB.: Servidor Web entre dos firewall.

Los firewalls protegen los datos aportando a su confidencialidad (evitan que los datos se conozcan), integridad (impiden que los datos se cambien) y disponibilidad (permite que los datos se usen cuando se los requiere).

Sin embargo los firewalls no pueden proteger contra personas maliciosas dentro de la empresa, no defiende las conexiones que no pasan por él, ni brinda seguridad contra amenazas desconocidas ni contra virus.

Utilizar bitácoras

Las bitácoras, son registros de las actividades de los sistemas, la mayoría de los sistemas operativos pueden configurarse para llevarlas, escribiéndolas en archivos, distribuyéndolas a través de la red, imprimiéndolas o almacenándolas en algún otro dispositivo.

Son invaluables a la hora de la recuperación después de un incidente de seguridad ya que nos pueden dar pistas de como entró el atacante y hasta ayudarnos a identificarlo. A veces pueden presentarse como evidencia en un juicio. Sin embargo si alguien entra en un sistema lo primero que hará será borrar sus huellas en las bitácoras ya sea eliminándolas o modificándolas. Esto se puede evitar con un servidor de bitácoras seguro que recolecta las bitácoras de otras computadoras en la red. Este servidor no soporta cuentas de usuario para evitar que un atacante pueda entrar al mismo.

Las bitácoras pueden ser examinadas con regularidad, existe un software llamado analizador de bitácoras que descarta los eventos esperados dejando sólo aquellos inesperados que merecen atención. La desventaja de las bitácoras es que generan mucha información en corto tiempo y es importante respaldar las bitácoras históricas ya que podemos necesitarlas cuando se descubre el ataque y puede que haya pasado un tiempo considerable desde que el mismo se produjo.

Utilizar respaldos

El respaldo, es una copia de los datos, escritos en un medio de almacenamiento duradero. Protegiendo contra fallas del equipo, borrado accidental de datos, irrupciones (ya que los archivos borrados o modificados por un atacante pueden ser restaurados), ayudan a detectar cambios en el sistema.

Sin embargo los sistemas de respaldo no están exentos de problemas: se debe verificar que los datos respaldados sean correctos y que puedan emplearse para restaurar el sistema, si los archivos respaldados se transmiten a través de la red sin encriptación, se corre el riesgo de que un atacante pueda acceder a su contenido, los medios de almacenamiento de respaldo exigen protección especial contra robo o destrucción ya que las mismas por definición contienen los datos históricos del sistema.

Minimizar servicios

Una forma fundamental de reducir las amenazas a un servidor Web es minimizar los servicios que ofrece la computadora donde este se ejecuta [L-9]. Al quitar los servicios no esenciales se eliminan entradas potenciales al sistema. Una buena práctica es: si un servicio no es necesario, deshabilitarlo. En la Figura CC se detallan los servicios que se recomienda restringir y el motivo de esta recomendación.

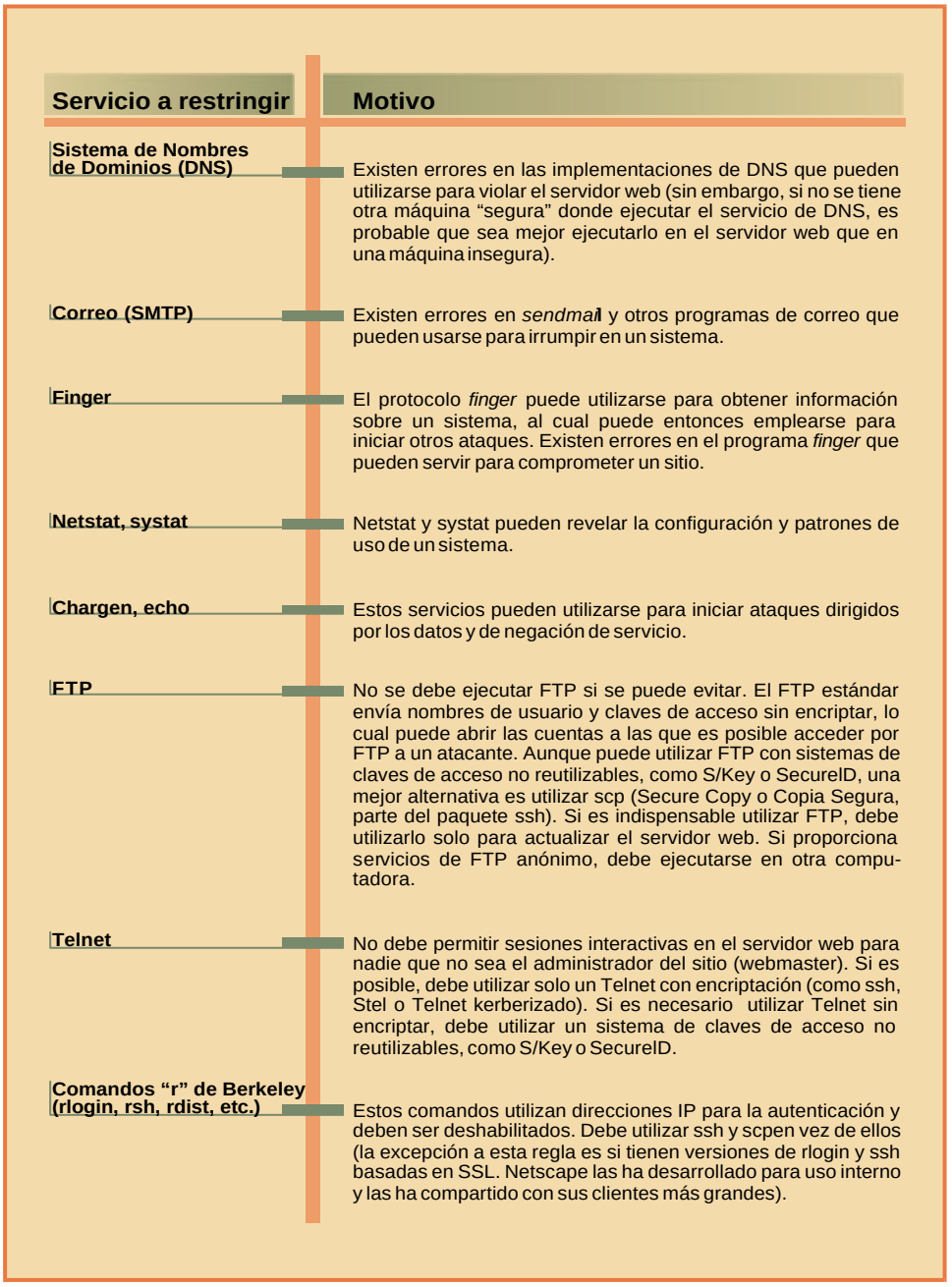


Figura CC.: Servicios que se deben deshabilitar o restringir para que un servidor Web sea considerado seguro [L-9]

Restringir el acceso a servidores Web

Algunas veces no se desea que la información publicada en Internet se encuentre visible para todo el universo de personas; esto puede ser porque el servidor Web contiene información exclusiva para un grupo de personas ya sea, que son miembros de una organización, clientes que pagan para ver la información, clientes que hayan firmado acuerdos de confidencialidad.

Existen varias técnicas para controlar el acceso a la información colocada en la Web, a continuación veremos algunos de ellos:

URL ocultos:

Consiste en no publicar y mantener secreto el URL de acceso a una página. Son los más fáciles de implementar aunque la seguridad que proporcionan es la equivalente a tener una llave escondida debajo del felpudo en la entrada de una casa. Se basa en el concepto de que nadie puede acceder a datos que no sabe dónde están, pero de la misma manera cualquiera que conozca como acceder a ellos, tendrá toda la información. Además esta información es transitiva ya que esta URL puede divulgarse de boca en boca, vía e-mail o de alguna otra manera. Otra forma de divulgación de la URL son los programas "araña" que buscan por toda la red agregando las palabras claves de cada página que encuentran a una base de datos central, como por ejemplo Lycos y AltaVista que son dos buscadores[24] muy conocidos que utilizan este método para completar sus bases de datos con información de los contenidos de la Web.

Restricciones basadas en la dirección:

Se permite el acceso al servidor Web a un grupo específico de computadoras basándose en sus direcciones de Internet mediante la dirección IP específica o un rango dentro de una subred. Es una técnica de limitar el acceso a la información en la Web. Este sistema no es perfecto ya que se pueden utilizar engaños de IP para enviar paquetes que aparente provenir de una computadora distinta de la que en verdad provienen. A aquellos que tengan permiso explícito de acceso se les mostrará la página correspondiente y a los usuarios que no tienen permiso de acceso se les mostrará el mensaje de la Figura DD.

[24] Motores de búsqueda que permiten localizar en Internet información determinada.

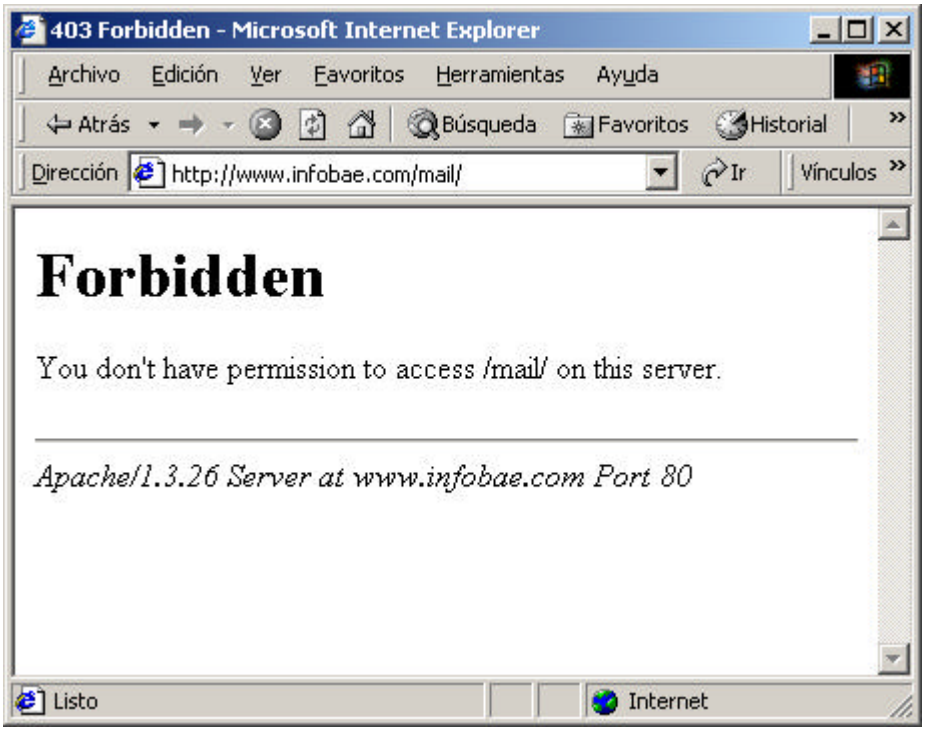


Figura DD.: Mensaje de advertencia cuando se intenta acceder a un sitio restringido y no se tienen los privilegios necesarios.

Control de acceso basado en identidad:

Este sistema se basa en restringir la entrada a un servidor Web utilizando nombres de usuario. Es una de las formas más efectivas de controlar el acceso. A cada usuario se le da un nombre que lo identifica y una clave de acceso que lo autentica. También se puede corroborar la identidad con algunos de los métodos antes visto de llave pública o prendas físicas.

Utilizar seguridad física

La seguridad física de un sitio Web intenta defender las máquinas comprometidas con el mismo contra cualquier ataque o accidente, contra personas internas y externas; a continuación se enumeran recomendaciones útiles a la hora de elaborar un plan de seguridad física:

?? Elaborar un detalle completo de qué es lo que se protege y contra qué o quién.
?? Proteger contra incendio, humo, explosiones, humedad y polvo.
?? Proteger contra desastres naturales.
?? Proteger contra ruidos eléctricos y rayos.
?? Proporcionar ventilación adecuada.
?? Alejar los alimentos y bebidas de las computadoras de misión crítica.

?? Restringir el acceso físico a las computadoras.

?? Asegurar físicamente las computadoras de forma que no puedan ser robadas ni transgredidas. Usar marcas indelebles de control de inventario.

?? Proteger el cableado de red contra destrucción, escucha e intercepción.

?? Crear una lista de procedimiento estándar de operación para el sitio.

Auditar la seguridad

La auditoria permite que controlemos los desvíos entre lo que en un momento se pretendió hacer y lo que se está haciendo dentro de la empresa. Es decir como los procedimientos y políticas que se han establecido, se van modificando en el accionar del día a día.

Al auditar la seguridad de un sistema informático deben tenerse en cuenta factores como la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones, las violaciones al sistema de seguridad de acceso que se puedan realizar, los defectos y errores evitables, fallas en los sistemas, etcétera.

Esto nos permite saber donde nos encontramos, si tenemos que trabajar en el cumplimiento de los procedimientos y políticas o la posible necesidad de actualizarlas.

Hay algunos puntos a tener en cuenta, para evaluar un sistema de seguridad informática:

Uso de la computadora: se debe observar el uso adecuado de la computadora y su software dentro de la organización. Evitar copias de programas de la organización para fines de comercialización y acceso a bases de datos con fines que dañen los conceptos de privacidad de los datos.

Sistema de acceso: para evitar los fraudes computarizados se debe contemplar de forma clara los accesos a las computadoras de acuerdo al nivel de seguridad de cada usuario y de sus privilegios. Evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo.

Control de programación: se debe conocer que las fallas más comunes están presentes en el momento de la programación, ya que pueden ser introducidas intencionalmente o no, para lo cual se debe controlar que los programas no contengan bombas lógicas; los programas deben contar con fuentes y sus ultimas actualizaciones; los programas deben contar con documentación técnica, operativa y de emergencia.

Personal: se debe observar este punto con mucho cuidado, ya que hablamos de las personas que están ligadas al sistema de información de forma directa y se deberá contemplar principalmente la dependencia del sistema a

nivel operativo y técnico, el grado de capacitación del grupo en cuanto a procesos de seguridad informática, contemplar el conocimiento y respeto de las políticas de seguridad informática. Es importante el perfil del personal relacionado con el sistema, ya que pueden surgir malos manejos de administración, negligencia o ataques deliberados.

Medios de control: se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o un fraude en el sistema.

Instalaciones: es muy importante no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar la continuidad del flujo eléctrico, efectos del flujo eléctrico sobre el software y hardware, evaluar las conexiones físicas de los sistemas; verificar si existe un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones.

Establecer las áreas y grados de riesgo: es muy importante el crear una conciencia en los usuarios de la organización sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo. Para esto se deben conocer los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe establecer el costo del sistema de seguridad teniendo en cuenta el factor costo – beneficio y el riesgo – impacto.

Para realizar estos estudios se debe considerar lo siguiente:

- clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- identificar las aplicaciones que tengan alto riesgo.
- cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo.
- formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- justificación del costo de implantar las medidas de seguridad.

Cada uno de estos puntos es de mucha importancia por lo que se sugiere clasificar estos elementos en áreas de riesgo que pueden ser:

Riesgo computacional: se debe evaluar las aplicaciones y la dependencia del sistema de información, para lo cual es importante considerar responder las siguientes cuatro preguntas:

¿Qué sucedería si no se puede utilizar el sistema?
¿Qué consecuencias traería la negación de servicio?
¿Cuál es el costo de no dar servicio?
¿Existe un procedimiento alternativo y que problemas ocasionaría?
¿Qué se ha hecho en casos de emergencia hasta ahora?

Cuando se ha definido el grado de riesgo se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas

en caso de desastre, señalando la prioridad de cada uno. Para que así, se trabajen los sistemas de acuerdo a sus prioridades.

Cultura y capacitación del personal: cuando hablamos de información, su riesgo y su seguridad siempre se debe considerar al elemento humano, ya que podría definir la existencia de los más altos grados de riesgo. Por lo cual es muy importante considerar la elaboración del plan observando el comportamiento con respecto al sistema, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

Motivar: se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial e individual.

Capacitación general: en un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo.

Este proceso incluye como práctica necesaria la implantación de planes de contingencia y la simulación de posibles delitos.

Capacitación de Técnicos: se debe formar técnicos encargados de mantener la seguridad informática como parte de su trabajo y que estén capacitados para transmitir a otras personas las medidas preventivas y correctivas.

Ética y Cultura: Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional.

Mantener la relación Costo – Beneficio

Resulta imprescindible a la hora de elaborar un plan de seguridad, ya sea definiendo políticas o implementando seguridad física, conocer completamente donde se encuentra ubicado nuestro sitio. Ya que no es lo mismo proteger una página con nuestras fotos familiares que un sitio de venta de servicios o artículos con medios electrónicos de pago.

“El costo de la seguridad no debe superar el valor de los datos pero el costo de obtener y descifrar esos datos debe ser superior a su valor”

Supongamos un sujeto **A** que tiene un servidor Web, físicamente ubicado en el microcentro de la ciudad de Buenos Aires, donde publica en Internet

las fotos de su familia. El sujeto **A** escuchó que un malicioso hacker del barrio prepara una estampida de elefantes que destruya los servidores de Internet de todo el mundo y nos contrata como administradores de seguridad de su sitio y nos pide que le demos una solución a este inminente problema. Nuestro trabajo se centrará en tranquilizarlo y transmitirle la idea de que el costo de proteger un servidor contra una estampida de elefantes es muy superior al riesgo de que esta ocurra y al de la información que se perdería y que con medios más económicos como respaldar la información podrá dormir relativamente tranquilo.

Ahora supongamos un sujeto **B** que tiene una tienda de CD virtual en el mismo servidor que el sujeto **A** para abaratar costos y recomendados por su amigo **A**, nos contrata para que también le demos asesoramiento de seguridad. Nuestro trato será radicalmente opuesto ya que **B** estará trabajando con información sensible de los clientes y requerirá políticas de seguridad mucho más estrictas. Esto se debe a que por más que a **A** le gusten las fotos que está publicando, la información no tiene siempre el mismo valor y necesitan de mayores inversiones y si el valor y sensibilidad de los datos lo justifica, el siguiente axioma se hace verdadero:

La seguridad no es un costo, el costo es no tener seguridad.

Arquitecturas de e-commerce

La arquitectura de una tecnología es la forma de interacción que tendrán sus componentes. La intención de detallar las más comunes, responde a la necesidad de conocer que existen muchas formas de reducir los riesgos en el comercio electrónico. [L-2] [L-3] [L-4] [L-6] [L-9] [W-8]

En el comercio electrónico podemos identificar los siguientes actores:

- **El Cliente**: es un sistema de cómputo, usualmente una PC, conectada a Internet directamente por medio de un Proveedor de Servicios de Internet, o indirectamente a través de una red corporativa. El comprador utiliza la computadora cliente para navegar y comprar.
- **El Vendedor**: es el sistema computacional que contiene el catálogo electrónico del vendedor, y en el caso de los bienes en línea, contiene productos para ser entregados a través de la red.
- **El Sistema de Transacción**: es el sistema computacional que procesa una orden en particular y que es responsable del pago, almacenamiento de los registros y otros aspectos comerciales de la transacción.

?? **El Medio de Pago**: es el sistema computacional que rutea las instrucciones de pago en las redes financieras existentes. Por ejemplo, aquellas instrucciones para la autorización de las tarjetas de crédito y el pago.

Las diversas arquitecturas de comercio electrónico existentes hacen uso de estos cuatro elementos de diferentes formas. En algunos sistemas, algunos de estos componentes se encuentran combinados en un solo sistema computacional, mientras que en otros cada uno de estos elementos se encuentra implementado en diferentes computadoras.

Arquitectura 1: Servidor de Web con forma de pedido

Un servidor de Web con páginas de catálogo y formularios de pedido es una de las maneras más simples de construir un sistema de comercio electrónico. Esta propuesta es comúnmente llamada servidor del vendedor .

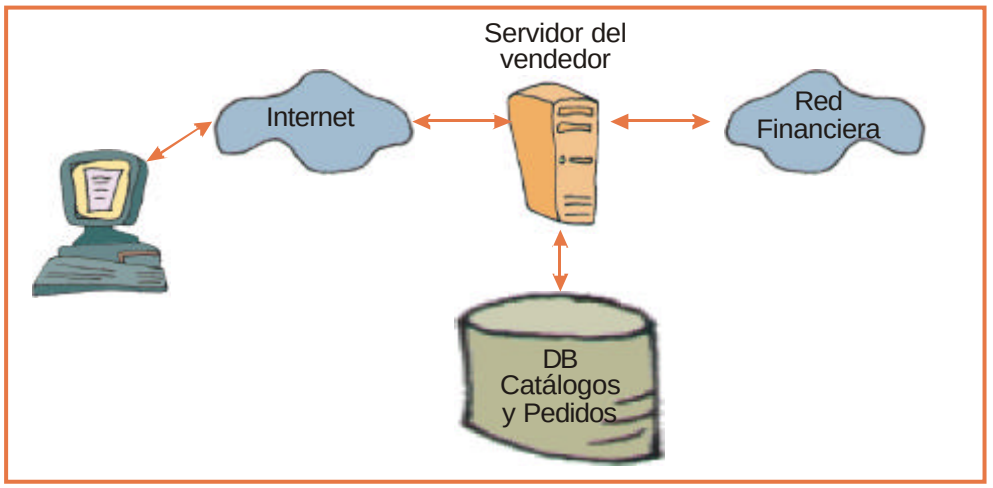


Figura EE.: Arquitectura de servidor Web con forma de pedido.

En la Figura EE, un servidor de Web proporciona tanto el catálogo de productos como la orden de pedido. Es decir, que el servidor del vendedor y el servidor de transacción están en un solo sistema, y no hay algún medio de pago explícito. Cuando el comprador ya esta listo para comprar el o los artículos que ha seleccionado, el comprador hace click en un botón denominado "checkout", el cual inicia el proceso de pago dentro de la transacción.

Pagar por medio de la tarjeta de crédito es el medio más usado hoy en Internet, una simple orden de pedido consiste de una lista de los artículos que el comprador puede adquirir y una serie de campos que el comprador debe llenar con la información del pago, incluyendo el número de tarjeta, la fecha de vencimiento, y la dirección donde se deberán entregar los artículos que adquirió, si es que éstos son en forma física.

Una de las medidas de seguridad que se toma para asegurar mínimamente la autenticidad del poseedor de la tarjeta, es solicitar la dirección de facturación, como se hace en algunos sistemas de tarjeta de crédito para corroborar que sea la misma dirección del propietario de la tarjeta.

Por su simplicidad, la aplicación comercial no requiere software adicional para los mecanismos de pago. Las tarjetas de crédito, las ordenes de compra y otros tipos de pagos pueden ser usados con tales sistemas, tomando ventaja de las capacidades básicas de seguridad más comunes que ofrece la Web hoy día. Puede observarse que el punto crítico de este proceso se produce cuando el comprador envía su número de tarjeta al vendedor a través de una red pública potencialmente insegura como Internet.

El estándar que se utiliza para asegurar esta transferencia de datos es el SSL.

Su principal virtud es su simplicidad; por otro lado ofrece la desventaja de ser más difícil de actualizar conforme las negociaciones en línea crezcan, o adaptarle nuevas tecnologías y componentes conforme vayan estando disponibles.

Arquitectura 2: Transacciones Electrónicas Seguras (SET)

Esta arquitectura utiliza el protocolo SET que se ha explicado con anterioridad. Es específica para realizar pagos con tarjeta de crédito en Internet. Las diferencias principales con respecto a la arquitectura servidor de Web con orden de pedido son respecto al manejo de la orden de pedido y la forma de manejar las comunicaciones relacionadas con el pago.

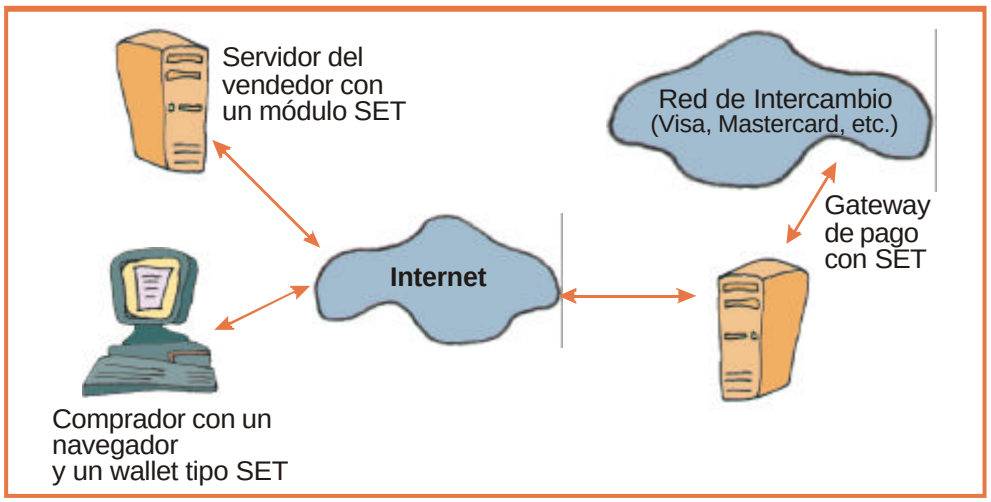


Figura FF.: Arquitectura SET.

En su forma simple, la arquitectura SET adquiere la orden de pedido del servidor vendedor en el momento que el pago por tarjeta de crédito es apropiado, como vemos en la Figura FF. El servidor vendedor incorpora un modulo SET vendedor en lugar de conectarse directamente a una red de autorización de tarjetas de crédito.

Una transacción SET típica funciona de forma muy parecida a una transacción convencional con tarjeta de crédito y consta de los siguientes pasos:

- ***Decisión de compra del cliente***. El cliente está navegando por el sitio Web del comerciante y decide comprar un artículo. Para ello rellenará algún formulario al efecto y posiblemente hará uso de alguna aplicación tipo carrito de la compra, para ir almacenando diversos artículos y pagarlos todos al final. El protocolo SET se inicia cuando el comprador pulsa el botón de Pagar.
- ***Arranque del monedero:*** El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.
- ***El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante:*** La aplicación monedero crea dos mensajes que envía al comerciante. El primero, la información del pedido, contiene los datos del pedido, mientras que el segundo contiene las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el software monedero del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.
- ***El comerciante envía la petición de pago a su banco:*** El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción y otra información relevante acerca de la misma, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago (que el comerciante no puede examinar, ya que van cifradas con la clave pública del adquiriente).
- ***El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente:*** El banco del comerciante

descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene a continuación las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso (el enviado por el comerciante y el codificado en las instrucciones de pago) y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.

- ***El emisor autoriza el pago:*** El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.
- ***El adquiriente envía al comerciante un testigo de transferencia de fondos:*** En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.
- ***El comerciante envía un recibo al monedero del cliente:*** Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados.
- ***Más adelante, el comerciante usa el testigo de transferencia de fondos para cobrar el importe de la transacción:*** Después de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.

  A su debido tiempo, el dinero se descuenta de la cuenta del cliente.

Arquitectura 3: Comercio de mercado abierto

La idea fundamental de esta arquitectura es separar la administración del catálogo, de la administración de la transacción a través de una tecnología llamada SecureLink. Esta idea permite a diversos servidores de catálogos compartir la capacidad de una máquina de transacciones y permite a las partes orientadas al contenido del sistema escalar independientemente de las partes orientadas a la transacción del sistema. El enfoque también permite a las organizaciones de servicio llegar a ser proveedores de servicios de comercio elec-

trónico quienes proporcionan servicios de administración de transacciones de manera externa a otras empresas.

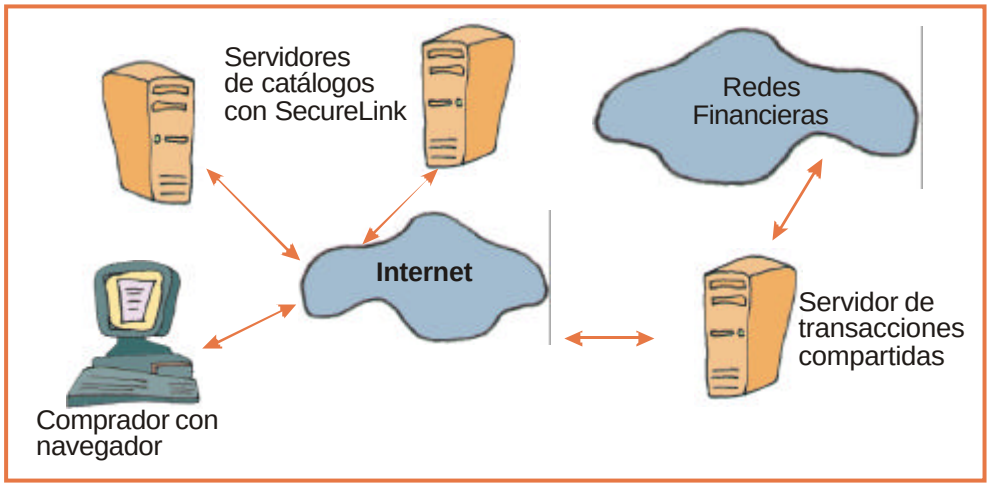


Figura GG.: Arquitectura de comercio de mercado abierto.

Dentro de esta arquitectura la máquina servidora de transacciones se encuentra separada de la máquina servidora del vendedor como se muestra en La Figura GG.

. La tecnología usada, SecureLink, es un sistema seguro de llamada a procedimiento remoto que trabaja a través de vínculos confiables utilizando protocolos de Web estándar. Es seguro porque las partes no autorizadas no pueden falsificar o estropear un mensaje (autenticidad e integridad). Es una llamada a procedimiento remoto porque empaqueta los parámetros y los entrega a los sistemas localizados remotamente. El hecho de trabajar con vínculos confiables quiere decir que los sistemas contenedores son más usados por diferentes organizaciones que los sistemas de transacciones. SecureLink esta basado en HTML y HTTP, que son los protocolos base de la Web.

SecureLink incluye cinco tipos de mensajes, conocidos como Objetos de Comercio SecureLink (SecureLink Commerce Object), los cuales se detallan a continuación:

- **Oferta Digital:** Ofrece productos para la venta. Contiene el precio, descripción, clasificación del impuesto, pedido de envío, etc.
- **Cupón Digital:** Descuentos y mercadeo. Contiene los parámetros de descuento y relaciona la información con el producto.
- **Boleto Digital:** Control de acceso para la suscripción a productos digitales.

  Contiene la identificación de los usuarios autorizados, agrupa en base a

la identificación denotando el empaquetamiento del contenido y la fecha de vencimiento.

- **Consulta Digital:** Acceso remoto a la base de datos de clientes. Contiene la identificación o su nombre para localizarlo y muestra la información del usuario.
- **Recibo Digital:** Control de acceso para la entrega de los bienes digitales. Contiene la identificación de la transacción para auditar, dominio del contenido para el cual el acceso es permanente y la fecha de vencimiento.

Estos objetos se encuentran codificados como Localizadores de Recursos Universales (URL, Universal Resources Localizator). Esta codificación hace posible que estos objetos puedan estar incrustados en cualquier tipo de contenedor de Web que soporte hipertexto.

Arquitectura 4: Compra abierta en Internet

Es una propuesta estándar liberada por un consorcio conformado por un grupo de organizaciones de compra, organizaciones de venta, organizaciones de pago y compañías de tecnología que está enfocando el problema del tipo de comercio "business-to-business" en Internet. La idea central es dividir la funcionalidad del sistema de comercio entre las actividades de venta y las de compra de tal forma que cada organización maneje aquellas funciones lógicamente conectadas a ella.

En este modelo el análisis lógico de las actividades es colocar la base de datos del cliente, los archivos del solicitante, y los procesos de aprobación del lado del comprador, y colocar el catálogo, el manejo de la orden, la entrega y pago del lado del vendedor. Esta estructura da como resultado la arquitectura que se representa en la Figura HH.

La idea fundamental de esta arquitectura es la división del servidor de transacciones en sus partes de compra y venta.

Para hacer que esta arquitectura funcione, se necesitan dos elementos de interoperabilidad entre los componentes de compra y venta que son: autenticación del solicitante y el manejo de la orden.

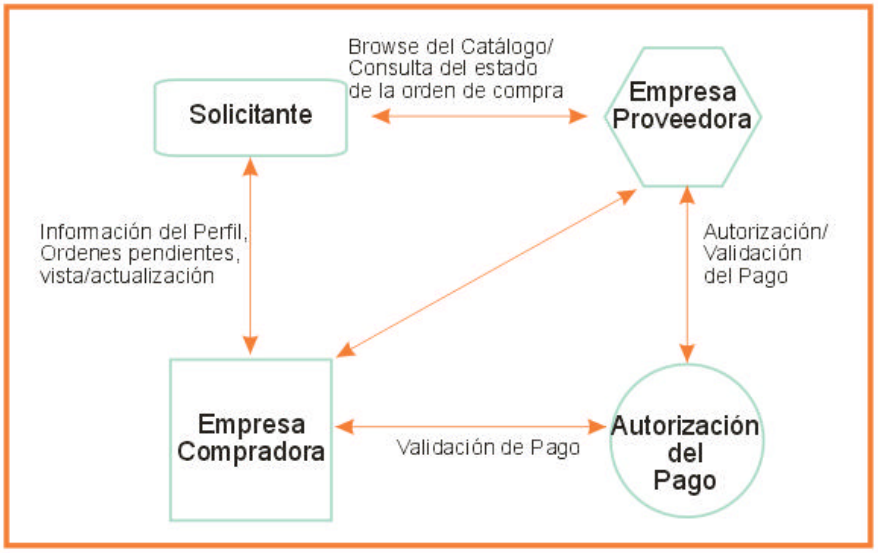


Figura HH.: Arquitectura de compra abierta en Internet.

?? **Autenticación del solicitante:** Dado que la organización compradora asume la responsabilidad dentro del modelo para administrar el grupo de solicitantes, el vendedor deberá tener medios estandarizados para autenticar solicitantes señalados como autorizados por la empresa compradora. Se hace uso de una clave pública certificada para este propósito. Cuando el solicitante navega por el catálogo del proveedor, éste presenta un certificado firmado por la organización compradora para validarlo. Este enfoque implica que al momento de realizarse la relación comercial entre las compañías, el catálogo del proveedor debe ser configurado para aceptar los certificados.

?? **Manejo de la orden:** Dentro del modelo arquitectónico, el solicitante llena una orden de pedido interactuando con el catálogo del proveedor. La orden es enviada en un formato estandarizado llamado solicitud de orden desde el servidor del vendedor hasta la empresa compradora. Una vez ahí, procede cualquier proceso de aprobación necesaria. Después de que la orden es terminada, ésta regresa al vendedor como una orden para ser entregada.

Los beneficios reales del modelo, pueden verse solamente cuando existen múltiples compañías compradoras comerciando con múltiples compañías vendedoras. Cuando esto sucede, el comprador es capaz de manejar centralmente su base de datos de solicitantes y su sistema de aprobaciones, y usar esos sistemas juntamente con múltiples socios comerciales. Similarmente, las empresas vendedoras pueden relacionar un catálogo maestro y un sistema de administración de ordenes con múltiples compradores.

Arquitectura 5: Ecash

Ecash, es una tecnología que permite realizar transacciones de pago en tiempo real de bienes y servicios, aplicando la metodología de comercio electrónico. La Figura II muestra un diagrama con la arquitectura básica de un sistema de comercio electrónico que maneja Ecash:

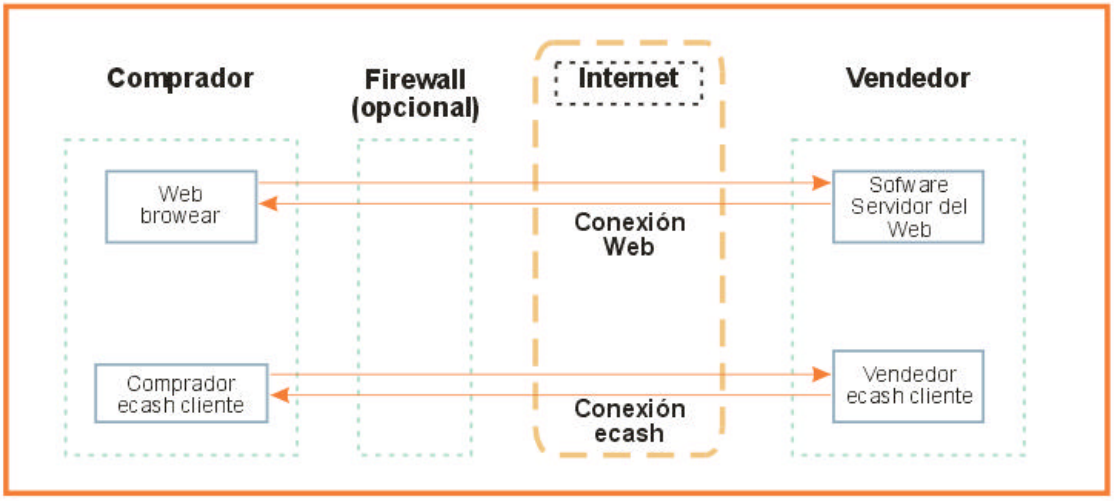


Figura II.: Arquitectura de ECash.

El software ECash del vendedor se encuentra integrado dentro del sitio Web del vendedor. Para realizar una transacción comercial se siguen los siguientes pasos:

1. El cliente entra al sitio Web del vendedor y solicita los bienes.
2. El vendedor envía una solicitud de pago ECash, la cual responde el comprador con el pago.
3. El software de ECash del vendedor automáticamente finaliza el pago depositándolo en la cuenta del vendedor y esperando la confirmación del banco.
4. Cuando el pago es confirmado por parte del banco, entonces el vendedor envía los bienes al cliente.

El software ECash del vendedor esta conectado al banco y a los clientes vía Internet. Usando la red corporativa, la empresa se encuentra completamente integrada a un sistema de control de inventario, sistemas de información y contabilidad, permitiendo el flujo de información entre los componentes. Actualmente, ya no se necesita una solución estándar para integrar al vendedor dentro de la red corporativa.

Parte 3
Poniendo en práctica lo que está en palabras

Hasta aquí vimos los temas relacionados con el comercio en la Web. La privacía de los datos, su tratamiento, la legislación vigente y el delito informático. Tratamos los conceptos de seguridad Web, los motivos que llevan a atender esta problemática y qué tecnologías se utilizan en defensa de los servidores Web. Analizamos la necesidad de proteger los datos y la privacidad del cliente, brindándole seguridad. Nos acercamos a los conceptos involucrados en las técnicas de identificación digital, certificados digitales y firma electrónica como medio de lograr que los clientes sientan la confianza necesaria para realizar transacciones que impliquen el intercambio de datos sensibles.

En particular nos concentramos en la problemática de proteger un sitio Web, las soluciones arquitectónicas que se pueden implementar y cuáles son sus diferentes implicancias.

Pero, ¿cómo podemos trazar una hoja de ruta para recorrer en la construcción de un sitio Web de comercio electrónico?

El mercado nos habla, es nuestro deber escuchar qué nos dice. Para esto realizamos una encuesta entre un grupo de profesionales de la informática y analizamos sus resultados, comparando los mismos con algunos trabajos sobre el mercado informático y el comercio electrónico publicados por la consultora D´Alessio Irol [W-25].

Luego, y teniendo en cuenta los resultados obtenidos exponemos un camino a seguir tendiente a evitar que un sitio de comercio electrónico fracase.

Encuesta transacciones online de comercio electrónico

La presente encuesta, cuyo formulario se encuentra en el Anexo A, es un relevamiento de la percepción de un grupo de profesionales del área informática sobre el comercio electrónico, contrastando la visión de usuarios con la de profesionales de sistemas y comparando los resultados con algunos trabajos sobre el mercado informático y el comercio electrónico publicados por la consultora D´Alessio Irol [W-25].

Se realizaron 21 encuestas mediante un formulario auto dirigido, con posibilidad de asesoría y de profundización mediante una entrevista personalizada en los casos que se requirieron. Las preguntas iniciales del cuestionario hacen referencia a la visión del comercio electrónico como usuario para luego registrar la percepción del mismo como profesional de TI.

OBJETIVO

Conocer el comportamiento del sector de profesionales de sistemas con respecto al comercio electrónico.

TIPO DE INVESTIGACIÓN

Encuesta por muestreo probabilístico.

MARCO MUESTRAL

Para construir el marco muestral de la encuesta se seleccionó aleatoriamente un grupo de 21 profesionales del área sistemas que sean usuarios del comercio electrónico. La figura JJ representa la muestra dentro de la población de estudio.

PERÍODO DE REFERENCIA

Las entrevistas tuvieron lugar en la ciudad de Neuquén durante el mes de enero de 2004.

MÉTODO DE RECOLECCIÓN

Formulario auto diligenciado, con posibilidad de asesoría en los casos que se requieran.

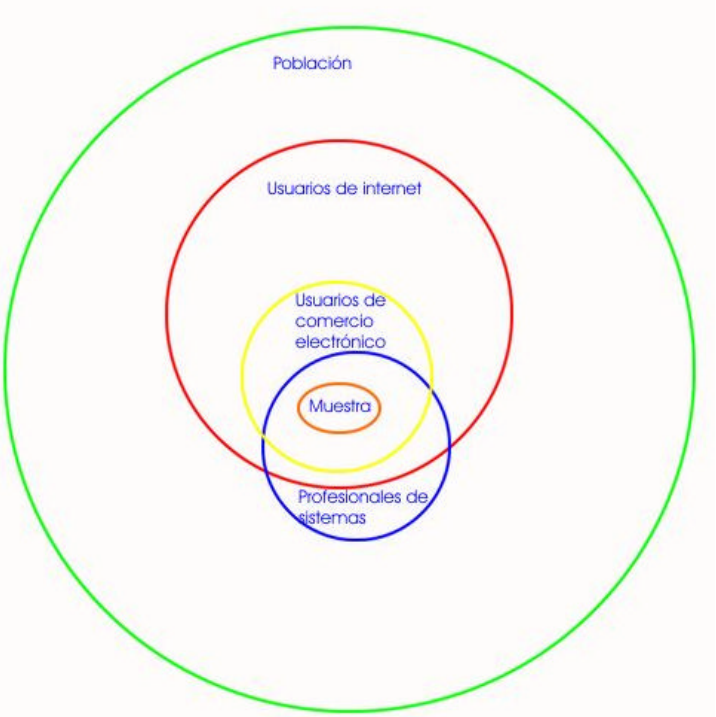


Figura JJ.: Distribución de la muestra.

Los entrevistados son usuarios de Internet desde antes de 1998. Sus niveles académicos se distribuyen entre 33% de ingenieros en sistemas, 14% licenciados en sistemas y el resto analistas de sistemas. A su vez, dentro del ámbito laboral se desempeñan en roles de consultores el 19%, analistas de negocios el 24%, analistas programadores el 29% y soportes funcionales de aplicaciones los restantes.

Resultados de la encuesta

?? Todos los encuestados coincidieron en que la información que se puede consultar en Internet sobre productos y/o servicios es confiable. Por lo que el comercio electrónico resulta una gran herramienta de decisión antes de realizar una compra.

?? Sólo el 5% de los compradores tuvo alguna vez un inconveniente con su compra y en todos los casos fueron resueltos.

?? Se compran menos productos de los consultados. Algunos rubros, en especial las transacciones bancarias realizadas por Internet, han ganado confianza cómo. Mientras que otros rubros, como la contratación de paquetes

turísticos, son muy consultados pese a que presentan un muy bajo índice de concertación vía Web. En la figura KK vemos Los distintos rubros que fueron consultados, comparados con los que registraron transacciones entre los encuestados.

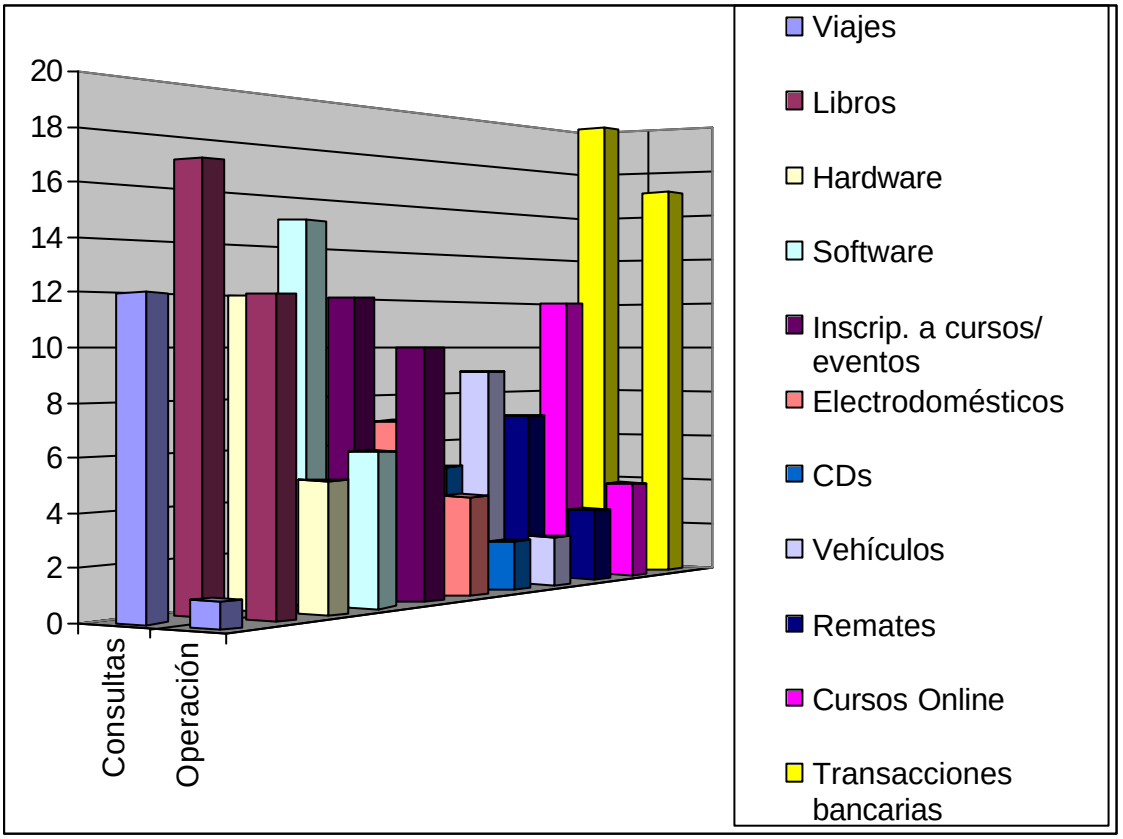


Figura KK.: Rubros consultados vs. rubros que han registrado transacciones.

?? El 80% de los consultados considera que el comercio electrónico ha cambiado la forma de comprar ya que ahora puede acceder a más ofertas antes de realizar la compra.

?? El 60% de los consultados opina que el comercio electrónico es un espacio para crear nuevas estrategias de comercialización online y offline. El resto de las opiniones se dividen por igual en considerarlo una herramienta de venta o un medio de difusión. Esta distribución se grafica en la figura LL.

?? El 10% de los encuestados no se comprometería a recomendar ni profesionalmente ni extraoficialmente el comercio electrónico como medio seguro para realizar una compra.

?? El 50% de los profesionales tiene conocimiento de casos en los que ha habido algún inconveniente con la compra de servicios; en su mayoría relacionados con la no correspondencia entre el producto y lo promocionado, en sitios de compraventa de productos usados y no es considerado por los encuestados, fundamento para descreer del comercio electrónico.

?? Si bien el 95% de los profesionales alegan estar preocupados por la seguridad y en transmitir a los clientes sensación de seguridad, admiten no conocer en profundidad muchas de los procesos que la aumentan tangiblemente y no ponerlas en prácticas aplicadas a sus proyectos de TI.

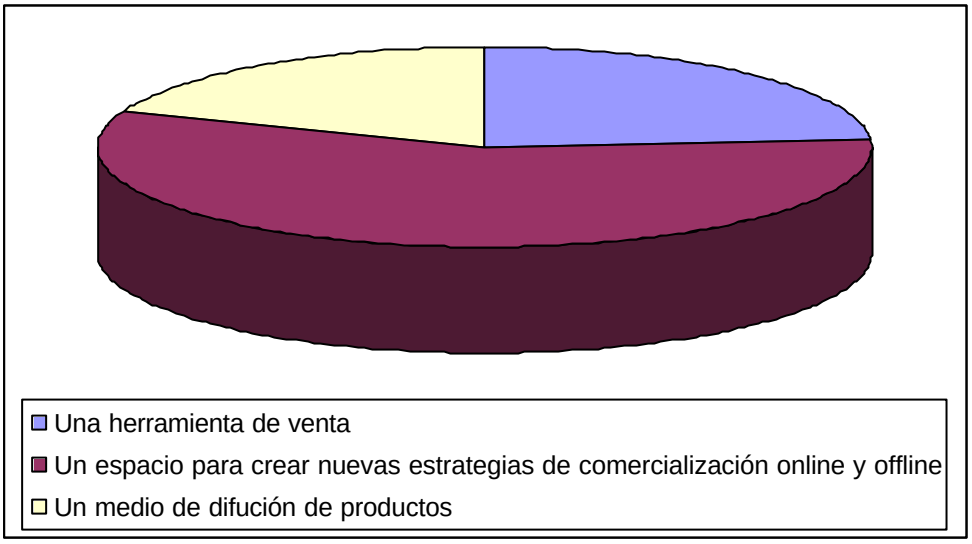


Figura LL.: Apreciación del comercio electrónico.

La consultora D´Alessio Irol publicó en su sitio web resultados de un estudio del mercado de comercio electrónico. Entre los datos presentados identificamos como de especial interés el que el 51% de los usuarios de Internet tienen más de 35 años, el 32% se encuentra entre los 25 y 34 años y sólo el 18% tiene menos de 24 años, lo que desmitifica el paradigma de que Internet es utilizado en su mayoría por adolescentes; el 61% del total de usuarios, son hombres; el perfil socioeconómico pertenece en un 48% a los niveles ABC1 que son los más altos, el 36% a un nivel C2 correspondiente a un nivel medio y el resto, 16% a los niveles bajos; por lo general, los usuarios de Internet pertenecen a hogares, en los cuales el principal sostén del hogar tiene estudios terciarios/universitarios. Con estos resultados queda demostrado que el mercado de usuarios de Internet es altamente atractivo ya que su poder de compra es grande. Sobre una muestra de 400 usuarios, se obtuvo que tres cuartas partes de los encuestados han efectuado algún tipo de consulta sobre productos y/o servicios en al Red; pero sólo el 15% indicó efectuar algún tipo de transacción online. Entre los encuestados, la relación consulta y compra/contratación resultó del 20%. Por otro lado un 71% compró/contrató por medios tradicionales bienes y/o servicios que había consultado previamente por Internet.

Comparando los resultados obtenidos por D´Alessio Irol con los de la encuesta realizada a profesionales de sistemas, presentados anteriormente,

concluimos que, si bien los profesionales de sistemas son notoriamente más propensos a concretar transacciones online que los usuarios comunes, todavía la relación consulta/compra es muy baja, transformando el comercio electrónico en una herramienta de consulta donde se pueden desarrollar nuevas estrategias de comercialización online y offline. También concluimos que hay rubros que se han ganado la confianza mientras que otros van en detrimento. Surge de la encuesta que los usuarios confían en las transacciones bancarias vía Web, pero no así en los sitios de remate o compra venta de productos usados; aunque la seguridad en el medio de pago, eje de este trabajo, sea la misma. De entrevistas realizadas con los encuestados, se observa una coincidencia en la sensación de seguridad que transmite un banco por ser conocido y tener un lugar donde efectuar reclamos si hubiese alguna disconformidad o problema. Se hace evidente que todavía queda mucho trabajo por hacer para que el comercio electrónico sea confiable y aceptado masivamente, pero sin duda ese es el camino que estamos transitando.

Hoja de ruta

A lo largo del desarrollo de este trabajo hemos enumerado los aspectos técnicos a tener en cuenta en el proceso de desarrollo de un sitio dedicado al comercio electrónico. ¿Se pueden trazar mapas con los puntos a transitar para garantizar el éxito de un emprendimiento de este tipo?

Desarrollar y mantener un comercio electrónico con miles de compras al día como Amazon, no es lo mismo que montar nuestro pequeño emprendimiento virtual en Internet. El comercio electrónico es comparable con poner en marcha y mantener una superficie comercial. A la hora de poner manos a la obra con un sitio de comercio electrónico hay que seguir una serie de pasos comenzando por el planteo de la dimensión del proyecto.

Hemos dicho que el comercio electrónico es una metodología moderna para hacer negocios que se apoya en la tecnología informática. Por lo que al construir un sitio de comercio electrónico, bien podemos estar hablando de una tienda virtual enorme como de un catálogo online con un sencillo sistema de envío de pedidos en Internet.

Las grandes estructuras traen aparejados grandes costos de desarrollo y complejos mantenimientos del sistema.

Antes de hacer una página web, debemos plantearnos la disponibilidad de stock que tendremos del producto, la logística de entrega que utilizaremos,

el conocimiento que tenemos del mercado del producto , y los requerimientos legales que implica la comercialización del producto.

Luego nos fijaremos en aspectos técnicos del sitio Web a desarrollar: el tipo de seguridad del comercio electrónico que necesitaremos, la arquitectura que utilizaremos para garantizar la seguridad, de que manera garantizaremos que somos un "sitio seguro", las implicaciones de seguridad que tendremos en cuenta según la forma de concretar las transacciones, y la transmisión de seguridad al cliente.

Recordemos que ya sea por publicidad, dinero, extensibilidad de los servidores, extensibilidad de los navegadores, soporte complicado, o ritmo de desarrollo siempre estaremos en la mira de potenciales atacantes por lo que debemos adoptar medidas de seguridad adecuadas. Hemos visto que hablar de seguridad en el comercio electrónico significa asegurar el servidor y los datos que contiene, asegurar la información que viaja entre el servidor Web y el usuario, y asegurar la computadora del usuario. Debemos planificar, diseñar e implementar los métodos que utilizaremos de acuerdo a nuestra forma de comercialización del producto. Si la comercialización será con tarjetas de crédito debemos decidir si las procesaremos fuera de línea o si implementaremos un protocolo de transacciones seguras atendiendo a las recomendaciones para asegurar los datos del cliente.

Hemos dicho que es importante prestar atención a la protección de la privacía personal en la Web ya que ésta es una razón por la que muchos potenciales usuarios del comercio electrónico permanecen renuentes a serlo, además de tener presente la defensa que otorga la legislación a los usuarios.

A la hora de elaborar un plan de seguridad, ya sea definiendo políticas o implementando seguridad física, debemos tener claro la categoría en la que se encuentra nuestro sitio de comercio electrónico. De esto dependerán la elección de la arquitectura y de la estrategia de comercio electrónico .

Podemos identificar tres categorías: los grandes comercios, los medianos y los pequeños.

Pequeños comercios electrónicos

Hablamos de un pequeño comercio cuando esperamos recibir hasta 100 visitas por día. De acuerdo con la encuesta presentada anteriormente, de esos clientes que consultan, sólo el 15% comprará en algún sitio de comercio electrónico, entre ellos el nuestro. Se puede esperar que de cada 100 visitas que

recibamos, si hacemos las cosas bien, se concrete la transacción en un promedio de 0,1 al día. Si recorremos el camino que describimos a continuación iremos creciendo paulatinamente.

Para este tipo de comercios podemos montar una estructura simple de catálogo de nuestros productos (para realizar la venta vía correo electrónico u offline) y alojarlos en sitios gratuitos que no nos darán un nombre de dominio propio pero permitirán que el costo sea bajo.

En primer lugar debemos crear una página de artículos. El título de la página debe contener las palabras adecuadas para que alguien interesado en dicho producto entre a nuestra tienda. No debemos descuidar los meta-tags ya que lo que los buscadores utilizarán para catalogar nuestro sitio y es muy probable que nuestros clientes lleguen a nosotros a través de un buscador. Un modelo de encabezado de la página principal es el que se muestra a continuación.

```
<html>
<head>
<title>Productos</title>
<META NAME="title" CONTENT="Productos">
        <META NAME="description"
        CONTENT="Descripción del contenido de la página">
        <META NAME="keywords" CONTENT="Palabras clave para la busqueda">
        <META NAME="subject" CONTENT="Rubro">
        <META NAME="DC.Language" CONTENT="Spanish">
        <META NAME="robots" CONTENT="ALL">
        <META NAME="category" CONTENT="categoría">
</head>
```

Las palabras clave son el anzuelo en los buscadores, por lo que es muy importante pensarlas bien.

La página de los artículos llevará un título con algún formato del tipo <H2></H2>, puesto que es el que los buscadores automáticos registran. Luego una descripción, lo más amplia y técnica posible y una fotografía del producto.

Por último, en la página índice, debemos colocar un enlace a todos y cada uno de nuestros artículos, con un texto simple o bien una pequeña imagen representativa. En esta página también debe haber un enlace a nuestro correo electrónico y si es posible una dirección física real, para que el usuario vea que existe una posible vía de reclamación, lo que le dará más confianza y tranquilidad.

Nunca deben ponerse títulos gráficos, que aunque mejoran considerablemente el aspecto, impiden a los robots de los buscadores indexar correctamente las páginas. En caso de tener nuestras páginas alojadas en un proveedor gratuito, debemos utilizar nombres que permitan identificar la URL de nuestras páginas con las palabras que buscan los navegantes interesados. Así, lo ideal es que la Web se encuentre en:

http://www.miproveedor.com/producto/

No es bueno tener prisa por que los clientes compren. Si colocamos un botón con la frase "Compre por Internet pulsando aquí!", nadie pulsará, jamás. En cambio, si ponemos "Más información", todo interesado pulsará. La venta en sí la haremos por correo electrónico u offline.

No debemos suponer que el comercio electrónico reemplaza al comercio tradicional. En algunos sectores, la venta por Internet es superior a la venta directa, pero en la mayoría de los casos, esto es al revés. Los productos más vendidos en Internet son aquellos que no se encuentran (o apenas se encuentran) en el mercado tradicional.

Con la publicidad debemos observar que anunciarse fuera del medio en el que nos movemos no es beneficioso ya que llegamos a mercados que no se interesarán en nuestra propuesta. Una campaña de publicidad de un comercio electrónico en televisión llegará a muchos televidentes pero a pocos navegantes de Internet. El medio más eficaz de promoción es el alta en buscadores, no sólo en buscadores genéricos, sino en buscadores de comercios electrónicos. Una fuente importante de visitas es ofrecer un servicio interesante y gratuito relacionado con el tema de nuestro producto. Por ejemplo una revista online con información que realmente interese a nuestras visitas. La revista será lo primero que se vea al entrar al dominio, la tienda virtual la colocaremos en un segundo plano. Los banners publicitarios son también una herramienta de promoción eficaz; deben tener un diseño atractivo que llame la atención y la idea de lo que ofrece nuestra web, sin mencionar que hay un comercio electrónico detrás. Se espera que 1 de cada 100 personas que ve el banner, haga clic en él. Si nuestra propuesta merece la pena, y renueva los contenidos periódicamente, las visitas volverán, logrando un incremento por esta vía en las visitas que recibimos.

Comercios electrónicos medianos

Cuando nos acerquemos a las 1.000 visitas diarias y 1 venta al día, será el momento de plantearnos cambiar la estructura del sitio. Tendremos que pen-

sar en un nombre de dominio propio ya que genera más confianza. Podremos mantener el que traíamos de la pequeña tienda virtual apuntado a la nueva dirección para permitir que nuestros clientes habituales nos encuentren. Será hora de pensar en un catálogo dinámico. El catálogo dinámico es una página de categoría y otra de artículo que se generan en tiempo real cuando alguien las solicita por Internet. Es requisito disponer de una base de datos con todo el catálogo: categorías y artículos. La página dinámica consulta a la base de datos y extrae el contenido solicitado, aplicándole el formato de la propia página. Convertir el catálogo en dinámico nos ahorrará trabajo a la hora de insertar y actualizar artículos o categorías, pero tiene sus dificultades:

1. Estamos hablando de un desarrollo más complicado que editar un simple código HTML
2. Debemos desarrollar un ABM para la base de datos del catálogo para que un administrador pueda mantener actualizados los datos.
3. Las páginas no son estáticas, sino dinámicas, por lo que el servidor responderá levemente más despacio a las solicitudes web.
4. Al ser páginas dinámicas, muchos buscadores no las indexarán.

Los puntos 1 y 2 nos van a suponer más trabajo y dinero, pero es inevitable si queremos hacer una apuesta mayor. El punto 3 y el punto 4, en cambio, son evitables. El punto 4, por ejemplo, se puede resolver usando técnicas de programación para convertir una URL estática en dinámica, de forma que al buscador le dará la impresión de que nuestro web sólo tiene URLs estáticas. Otro método es la renderización de páginas web, que consiste en que cada vez que se actualiza la base de datos del catálogo, un script genera páginas estáticas a partir de las páginas dinámicas, por medio de solicitudes web a sí mismo.

En este tipo de sitios, la venta ya no se hace por correo electrónico, sino que está integrada en el propio web. Sin embargo, es muy importante mantener el enlace de correo electrónico bien visible, o incluso con un botón "Más Información", porque, como hemos mencionado, muchos clientes desconfían de los sistemas electrónicos de compra, y prefieren contactar al comerciante antes de hacer el pedido.

Para realizar la venta debemos seleccionar la arquitectura que utilizaremos. La de servidor Web con forma de pedido es buena para este tipo de comercios ya que no requiere software adicional para los mecanismos de pago. Utiliza SSL para asegurar la transferencia de datos. Es una arquitectura simple; pero tiene la desventaja de ser más difícil de actualizar conforme las nego-

ciaciones en línea crezcan, o adaptarle nuevas tecnologías y componentes conforme vayan estando disponibles.

Es útil instalar un programa de análisis de logs. Tales programas permiten ver la evolución de visitas, la procedencia, las palabras más usadas en los buscadores para llegar a nuestra web, la nacionalidad de los visitantes, horario de mayor saturación y luego se puede utilizar la información reunida para analizar estrategias de mercado. Con estas herramientas sabremos mucho acerca de nuestros clientes, como en cualquier negocio, conoceremos los nombres, dirección, teléfono y nro de tarjeta de crédito. Pero también es posible registrar con quién intercambian correo electrónico, intereses de mercado, etc. Hemos hablado de La Fundación de la Frontera Electrónica y el proyecto e-trust (confianza electrónica) que consiste en someter a auditorias periódicas a las empresas de comercio electrónico. Es importante respetar el estándar que especifica lo que se puede hacer con los datos sensibles de los usuarios, hasta sería posible certificar como sitio e-trust, esto genera confianza en el cliente.

Debemos recordar las buenas prácticas tratadas en este trabajo: el no exigir a los usuarios que se registren para utilizar el sitio, permitir a los usuarios registrar su dirección de correo electrónico sólo si desean recibir boletines, no compartir con otra compañía los datos de un usuario sin la autorización explícita de este, siempre que se envíe un mensaje de correo electrónico a los usuarios, explicarles como se obtuvo su dirección y como puede hacer para borrarse de la lista de distribución si así lo desea, no permitir el acceso a las bitácoras, eliminar las bitácoras cuando ya no sean necesarias, encriptar las mismas, no dar ninguna información personal de los usuarios, aplicar políticas internas de privacía con los empleados, informar a los usuarios acerca de las políticas en la página principal y permitir que el emprendimiento sea auditado por terceros, definir políticas en tiempo de diseño, prevenir la intercepción de claves de acceso, utilizar herramientas de seguridad, evitar fallas y errores de programación, utilizar Firewalls, utilizar respaldos, minimizar servicios, restringir el acceso a servidores Web, utilizar seguridad física, auditar la seguridad.

Con estas prácticas estaremos por el buen camino, si nuestro servicio es bueno, la cantidad de visitas crecerá y el número de transacciones también.

Comercios electrónicos grandes

Estos están reservados para aquellos que hayan disfrutado del éxito de su comercio electrónico tras superar los niveles anteriores. Un comercio elec-

trónico se considera grande cuando ya recibe unas 10.000 visitas al día y el nivel de ventas ronda las 10 al día.

Aquí debemos pensar en alojar el sitio en un servidor que nos permita un dominio propio y subdominios o, si nuestro nivel de ventas lo permite, tener un servidor web propio. El crecimiento del sitio permitirá desarrollar alternativas como:

?? Carrito de compras: lo utilizaremos para permitir a nuestros clientes comprar más de un artículo por sesión.

?? Seleccionar una arquitectura de pago o una combinación de arquitecturas:

- o Arquitectura de pago de transacciones electrónicas seguras utilizando el protocolo SET, que como se ha explicado con anterioridad es específica para realizar pagos con tarjeta de crédito en Internet funcionando de forma muy parecida a una transacción convencional con tarjeta de crédito.
- o Arquitectura de comercio de mercado abierto que separa la administración del catálogo, de la administración de las transacciones permitiendo a diversos servidores de catálogos compartir la capacidad de una máquina de transacciones y a las partes orientadas al contenido del sistema escalar independientemente de las partes orientadas a la transacción del sistema.
- o Otra arquitectura a evaluar es la de compra abierta en Internet que es una propuesta estándar liberada por un consorcio conformado por un grupo de organizaciones de compra, organizaciones de venta, organizaciones de pago y compañías de tecnología que está enfocando el problema del tipo de comercio "business-to-business" en Internet. La idea central es dividir la funcionalidad del sistema de comercio entre las actividades de venta y las de compra de tal forma que cada organización maneje aquellas funciones lógicamente conectadas a ella. La idea fundamental de esta arquitectura es la división del servidor de transacciones en sus partes de compra y venta.
- o Arquitectura de Ecash que es una tecnología que permite realizar transacciones de pago en tiempo real de bienes y servicios, aplicando la metodología de comercio electrónico.

?? Bases de datos encriptadas: recordemos que, el punto más vulnerable en la seguridad de los datos, no está en la transmisión sino en el almacenamiento. Los números de tarjetas de crédito que usan los hackers para realizar compras fraudulentas, se suelen extraer de bases de datos de clientes de

tiendas virtuales. Para evitar esto, las y observar los conceptos que hemos desarrollado a lo largo de este trabajo.

?? El servicio de seguimiento de envíos permite al cliente ver en qué situación se encuentra su pedido. Amazon, por ejemplo, presenta esta posibilidad cuando se realiza un pedido, de forma que consultando su web se puede ver el recorrido geográfico de la compra, y estimar el día de la entrega.

?? Un buscador resulta interesante en un catálogo grande. La mayoría de las veces es preferible tener bien categorizados los artículos, a tener un buscador, puesto que es más difícil encontrar un producto por su nombre exacto que buscándolo por temas. Además, si el cliente recorre el catálogo tiene más probabilidad de que se fije en algún otro producto que le pueda interesar.

?? Una sección de los más vendidos y la de ofertas, nos permitirá llamar la atención sobre productos concretos, que normalmente no se encuentran fácilmente en el catálogo, otra opción interesante para catálogos muy grandes.

Es importante recordar que si nuestro comercio ha alcanzado un volumen de venta que nos permite categorizarnos como comercio electrónico grande, es porque nos hemos ganado la confianza de nuestros clientes. Debemos trabajar todos los días en fortalecer ese vínculo.

Conclusiones

El problema de la seguridad en los sistemas informáticos y por herencia en Internet y en sus transacciones de datos no es nuevo, de hecho hemos hablado de problemas detectados en 1973 y que aún perduran.

Los protocolos y arquitecturas para asegurar las comunicaciones en una red son, al igual que el resto de los componentes de software y hardware, propensos a ataques malintencionados. De los ataques conocidos muchos pueden ser evitados o al menos detectados, pero muchos otros logran concretarse.

A partir del intercambio de opiniones con usuarios, analistas y responsables de seguridad de infraestructura concluimos en que la tecnología de aseguramiento existe y se conoce, que las soluciones están al alcance de la mano pero que muchas empresas no desean pagar la seguridad ya que no es algo tangible. Simplemente perdieron de vista al usuario y sus intereses o no saben cómo justificar el costo de la seguridad.

Se ha dicho que la seguridad en la Web es difícilmente absoluta, pero se puede minimizar el riesgo utilizando medidas de seguridad apropiadas y planes para una recuperación rápida ante un incidente de seguridad. La seguridad Web no es fácil ni barata pero la inseguridad puede ser aún más costosa. La seguridad debe ser parte integral de una organización y de la mentalidad de sus componentes. Poner cuidado en el desarrollo de las políticas de seguridad, posibilita evitar muchos problemas potenciales. Sin embargo muchas organizaciones ponderan el hacer sobre el planificar; sin comprender la importancia de los planes y los beneficios en tiempo, costo y calidad de los procesos planificados sobre los improvisados. Es necesario producir un cambio de **cultura** en aquellas empresas en las que es preciso que las cosas ocurran para que se planifiquen las acciones a seguir.

Las estrategias de las empresas de comercio electrónico que florecieron en los 90, se basaron en publicidades masivas y simplemente lograron que los usuarios entren y salgan, como si se tratara de una puerta giratoria. Las leyendas urbanas corrieron por Internet, pasando por las máquinas de todo el mercado, divulgando historias con incidentes terribles que le sucedían a aquellos que osaban poner sus datos en la computadora y ni hablar si los datos eran los de su tarjeta de crédito. Estas leyendas contaban sobre personas que al comprar un artículo en un sitio Web eran estafadas o se utilizaban sus datos para algún tipo de fraude. La realidad es que hasta la fecha no hay ningún caso de-

clarado oficialmente de estafas a usuarios del comercio electrónico, lo que no significa que no hayan ocurrido. Además otros sistemas, como las ventas telefónicas, a pesar de ser más débiles, generan más **confianza,** por lo que son más aceptados. Y he aquí una palabra que consideramos clave ya que el ser humano desconfía de lo que no conoce y el común de los usuarios desconfía altamente de la tecnología. Admitamos que un candadito en el inferior derecho de nuestra pantalla no es suficiente para darle nuestro número de tarjeta de crédito a una empresa que no conocemos, sobre todo a la vista de toda la comunidad de hackers a la cual le tenemos pánico.

Sabemos que habrá sistemas mientras haya mercado, al menos mientras la sociedad sea capitalista. Por lo tanto no se puede dejar de escuchar al mercado y si el mercado dice que tiene miedo del comercio electrónico, es necesario dirigir todas las fuerzas a la difusión de la seguridad del comercio electrónico.

La confianza está ligada en gran medida al conocimiento. Para lograr captar la confianza del mercado es necesario mejorar los procesos profesionales y la manera de trabajar; dar a la planificación el lugar que se merece y producir un cambio de cultura en aquellos que aún dicen: “Estamos en tiempos de crisis y me vienen a hablar de lo que deberíamos hacer para mejorar o de perder tiempo planificando cuando lo que yo quiero es sacar soluciones YA”. Nadie discute que en estos tiempos los vientos están soplando muy duro, pero en las tormentas están quienes se ocultan en refugios, poniéndose a resguardo y hay quienes montan molinos de viento y recogen éxitos permanentes. Es necesario persuadir a los empresarios de que la recuperación de un incidente es más costosa que la toma de medidas preventivas.

La seguridad del sistema de transacción de datos no debe ser un agregado al comercio electrónico, sino algo que surja desde el propio diseño.

Dijimos que la mayor parte de los problemas de seguridad en los sistemas y por ende en los sistemas de comercio electrónico se debe, no a malicia, sino a errores de programación. Se debe tender a 100% de seguridad y 0% de error. Si bien la seguridad es difícilmente absoluta; existe tecnología, conocimiento y posibilidades suficientes para lograr una gran mejora en la seguridad y una minimización de los riesgos. Es sólo un tema de conciencia de todos los actores de este juego.

En este trabajo de tesis se analizó la barrera de muchas empresas de comercio electrónico que quieren expandir sus límites y pese a sus esfuerzos en el marketing del producto, fracasan por miedos, inseguridades y errores tec-

nológicos. Se investigó y estudió los conceptos teóricos relacionados con el comercio electrónico y la seguridad en la Web y se observó la aplicación de los mismos en empresas mediante entrevistas de campo.

Durante el desarrollo de la presente tesis se realizó un relevamiento de la utilización de las tecnologías del comercio electrónico en el mercado y se observó las medidas de seguridad aplicadas. Se presentaron los conceptos que permiten al usuario de Internet detectar sitios seguros y confiar en ellos; se analizaron las técnicas existentes de certificación de sitios seguros y los mecanismos de certificación y seguridad para encontrar las formas de persuasión que, basadas en la tecnología, le permitan a las empresas que sus clientes confíen en el comercio electrónico.

Hemos mencionado los problemas de la seguridad en la Web que, si bien dependen del caso particular, suelen orbitar alrededor de los siguientes puntos:

- Aseguramiento del servidor Web de forma física y lógica.
- Aseguramiento de la información en tránsito.
- Aseguramiento de la computadora del usuario.

También se comentaron las diferentes herramientas de protección, las prácticas y arquitecturas que aumentan la seguridad. Las técnicas de identificación digital mediante certificados y firmas. Se habló de la criptografía como base para la protección de los datos, aunque no es sinónimo de seguridad.

Se hizo hincapié en los principales problemas de seguridad de las máquinas en la actualidad y se encontró que su solución estaba disponible desde hacía mucho tiempo y se basa en los siguientes puntos:

- Definir políticas en tiempo de diseño.
- Prevenir la intercepción de claves de acceso.
- Utilizar las herramientas de seguridad disponibles.
- Evitar fallas y errores de programación.
- Utilizar Firewalls
- Utilizar bitácoras
- Utilizar respaldos
- Minimizar servicios
- Restringir el acceso
- Utilizar seguridad física
- Auditar la seguridad

Utilizando medidas de seguridad, buenas prácticas y arquitecturas que pueden asegurar al cliente la integridad y fiabilidad de sus datos se logra la tan anhelada confianza y satisfacción que es el objetivo primordial de cualquier empresa para subsistir en un mercado competitivo.

Las posibilidades que los clientes tienen de protegerse de ataques son muchas. Las responsabilidades en caso de fraude, recaen sobre el prestador del servicio, por negligencia, ya que las herramientas de seguridad existen y son eficientes si se usan con buenas prácticas.

Existen desvíos entre la teoría sobre la aplicación de la tecnología disponible y la práctica, los cuales se deben en su mayoría al poco apoyo de los empresarios a la seguridad, esto se debe a tomar, erróneamente, a la seguridad como un costo y no como una inversión.

El usuario debe estar al tanto de los riesgos y cómo defenderse ya sea de las formas de prevención como de las posibilidades de reaccionar ante ataques. Somos nosotros, los profesionales de sistemas, los que tenemos que mostrarles los peligros verdaderos y los mecanismos de defensa que existen en su favor.

Las empresas tendrán que cambiar su cultura respecto a la seguridad de la información, así como lo hicieron con la seguridad física de los empleados en las últimas décadas. Pero aquí también jugamos nosotros un papel fundamental ya que debemos mostrar a las empresas los beneficios de tener políticas de seguridad de datos y que este cambio significa evolución y subsistencia.

Tenemos que transmitir la idea de seguridad al cliente, sino simplemente huirá de nuestro sitio. De esto dependerá el éxito o el fracaso del comercio electrónico.

Bibliografía

Libros:

[L-1] Manual de referencia HTML
Autor: Thomas A. Powel
Editorial: Mc Graw Hill
Edición: 1998, España

[L-2] El Libro de la Webmaster
Autor: John Merlin Fisher
Editorial: Anaya Multimedia
Edición: 1997, España

[L-3] Reingeniería y Seguridad en el Ciberespacio
Autor: J. A. Calle Guglieri
Editorial: Diaz de Santos
Edición: 1997, España

[L-4] Técnicas de Criptografía y de Protección de Datos
Autor: Amparo Fúster Sabater, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Mosqué
Editorial: Ra Ma
Edición: 1997, España

[L-5] Firewalls and Internet Security
Autor: Willam R. Cheswick
Editorial: Addison – Wesley Publishing Company
Edición: 1994, Estados Unidos

[L-6] Strategic Data Planning Methodologies
Autor: James Martin
Editorial: Prentice – Hall inc
Edición: 1982, Estados Unidos

[L-7] Apuntes de la cátedra Comercio Electrónico
Edición: 2000, Argentina

[L-8] Construya firewalls para Internet
Autor: Brent Chapman, Elizabeth D Zwicky
Editorial: Mc Graw Hill
Edición: 1999, México

[L-9] Seguridad y comercio en el Web
Autor: Simson Garfinkel, Gene Spafford
Editorial: Mc Graw Hill

Edición: 1999, México

[L-10] Java, Programación en Internet
Autor: Americo Damasceno Jr.
Editorial: Métodos S.A.
Edición: 1996, Argentina

[L-11] Como Se Hace Una Tesis
Autor: Umberto Eco
Editorial: Gedisa Editorial
Edición: 1993, España

Sitios Web:

[W-1] Powel Internet Consulting
URL: www.pint.com

[W-2] Información sobre SSL
URL: http://www.psy.uq.oz.au/~ftp/Crypto

[W-3] Información sobre SSL
URL: ftp://ftp.ox.ac.uk/pub/crypto/SSL/

[W-4] Transacciones electrónicas seguras
URL: www.mastercard.com/set/set.htm

[W-5] Centro de coordinación CERT
URL: www.cert.org

[W-6] Información encriptación
URL: www.red21.com/cursos/area.htm

[W-7] Portal de compras de Páginas Doradas
URL: http://www.paginasdoradas.com.ar/PDPortal/compras/

[W-8] Trabajos sobre seguridad en Internet
URL: http://www.monografias.com/

[W-9] El protocolo SSL
URL: http://home.netscape.com/newsref/std/sslref.html

[W-10] Conferencia internacional de desarrollo de Comercio y Seguridad
URL: http://developer.netscape.com/

[W-11] Seguridad en Internet
URL: http://home.netscape.com/newsref/ref/Internet-security.html

[W-12] Uso de RSA por SSL
URL: http://home.netscape.com/newsref/ref/rsa.html

[W-13] Estudios de comercio en la Web
URL: http://www.global-concepts.com/

[W-14] Generación de Números Pseudoaleatorios usados en Sistemas Criptográficos
URL: http://www.seguridata.com/nf/generacion.doc

[W-15] El ABC de los documentos electrónicos seguros
URL: http://www.seguridata.com/nf/abc.pdf

[W-16] El sistema RCA
URL: http://www.seguridata.com/nf/rsa/rsa1.htm

[W-17] Portal de Internet Terra
URL: http://www.terra.com.ar

[W-18] Revista digital de cityeconomika
URL: http://www.cityeconomika.com/ar/6/notes,6775.asp

[W-19] Sitio de seguridad informática
URL: http://www.virusprot.com

[W-20] Publicación Internet en Argentina: Cuantificación y Perfil de usuario de la consultora Carrier y Asoc. Información y análisis de mercado.
URL:
http://banners.noticiasdot.com/termometro/boletines/autor/boletines-autor-carrieryasoc.htm

[W-21] ISACA (Information Systems Audit and Control Association)
URL: http://www.isaca.org/

[W-22] Constitución de la Nación Argentina
Sancionada: 15 de diciembre de 1994 Promulgada: 30 de enero de 1995
URL: http://infoleg.mecon.gov.ar/txtnorma/ConstitucionNacional.htm

[W-23] Automotive Industry Action Group
URL: www.aiag.org

[W-24] Electronic Commerce Innovation Centre
URL: http://www.ecommerce.ac.uk/

[W-24] Alfa - Redi: Revista de Derecho Informático
URL: http://www.alfa-redi.org/revista/data/14-5.asp

[W-25] Consultora D'Alessio IROL
URL: http://www.dalessio.com.ar/

Entrevistas y observaciones del campo:

[E-1] Rodríguez, Walter Alfredo Líder de Proyectos de **AVANSIS SA de CV**
Entrevistas realizadas desde 09 de mayo de 2002 hasta fines de agosto de 2002 realizadas vía mail.

AVANSIS SA de CV es una consultora de sistemas de México DF. que desarrolla programas Java que resuelven transacciones ON-LINE de todo tipo
Y entre sus clientes se encuentran:

?? **BANCRECER** (www.bancrecer.com.mx)
Rubro: Banco
Lenguaje de programación: Java 1.1.8 (JavaBeans, Servlets, JSPs, XML y XSL con Translets)
WebServer: IBM WebSphere para MainFrame y NT

?? **PROSA** (www.prosa.com.mx)
Rubro: Tarjetas de crédito.
Esta empresa es la encargada de controlar las compras realizadas con tarjetas de crédito. Es el similar a "postnet" en Argentina.
Trabaja con los bancos de México para coordinar los gastos de los usuarios.
Lenguaje de programación: Java 1.2
WebServer: IPlanet (de SUN)

?? **BITAL** (www.bital.com.mx)
Rubro: Banco
Sistema desarrollado en: Java 1.1.8 (Servlets y JSPs)
WebServer: IBM WebSphere para AIX y NT

?? **INVERLAT** (www.inverlat.com.mx)
Rubro: Banco
Sistema desarrollado en: Java 1.1.8 (Servlets y JSPs)
WebServer: IBM WebSphere para AIX y NT

?? **TELMEX** (www.telmex.com.mx)
Rubro: Telefonía
Esta es la empresa numero uno en servicio de llamadas locales, larga distancia e internacionales de México.
Sistema desarrollado en: Java 1.2 (Servlets y JSPs)
WebServer: IBM WebSphere version 3.5 para AS/400

Anexo A. Formulario de encuesta realizada

Datos generales

Nombre:.....
Cargo:.....
Título: .....
¿Desde que año es usuario de Internet? .....

Punto de vista de usuario

¿ha realizado consultas a productos y/o servicios que involucren transacciones de comercio electrónico (compras, remates, home banking)?

? SI

¿La información obtenida es confiable?

? SI

? NO

¿Cuales de los siguientes rubros ha consultado en Internet?

Rubros	
Viajes	
Libros	
Hardware	
Software	
Inscrip. a cursos/ eventos	
Electrodomésticos	
CDs	
Vehículos	
Remates	
Cursos Online	
Transacciones bancarias	

¿concretó la transacción?

? SI

¿Tuvo algún inconveniente con la transacción?

? SI

? NO

¿Cuales de los siguientes rubros ha comprado/utilizado en Internet?

Rubros	
Viajes	
Libros	
Hardware	
Software	
Inscrip. a cursos/ eventos	
Electrodomésticos	
CDs	
Vehículos	
Remates	
Cursos Online	
Transacciones bancarias	

Considera que la experiencia ha sido en general:

? Muy positiva

? Positiva

? Neutra

? Negativa

? Muy negativa

? NO

¿por que?

? Desconfianza en los medios electrónicos de pago

? Prefiere la atención personalizada

? Costos

? Desconfianza en la entrega

? Desconfianza en el tratamiento de los datos

? Otros motivos ¿cuales?.....
.....

? NO

¿por que?

? Desconfianza en los medios electrónicos de pago

? Prefiere la atención personalizada

? Costos

? Desconfianza en la entrega

? Desconfianza en el tratamiento de los datos

? Otros motivos ¿cuales?.....
.....

¿considera que Internet como canal de comercialización reemplaza a los canales tradicionales o sólo los complementa?

? Reemplaza

? Complementa

De la siguiente lista de rubros, ¿ En cuales considera que la publicidad influye positivamente?

Rubros	
Viajes	
Libros	
Hardware	
Software	
Inscrip. a cursos/ eventos	
Electrodomésticos	
CDs	
Vehículos	
Remates	
Cursos Online	
Transacciones bancarias	

¿cambió Internet su forma de comprar?

? SI

? NO

¿accede a más oferta a través de Internet?

? SI

? NO

Considera que Internet como medio de comercialización es principalmente:

? una moda

? una herramienta de venta

? un espacio para crear nuevas estrategias de comercialización online y offline

? un medio de difusión de los productos

¿le recomendaría a un amigo suyo utilizar el e-commerce?

? SI

? NO

¿ha sabido de alguien que tenga una experiencia negativa en la compra o uso de algún servicio de Internet?

? SI

? NO

Punto de vista de profesional de TI

¿Le preocupa la seguridad en las transacciones de datos y su inviolabilidad?

? SI

? NO

¿Intenta que la seguridad sea transmitida al cliente?

? SI

? NO

¿Cómo califica la relación entre la seguridad y el éxito comercial de una transacción de comercio electrónico?

? Muy alta

? Alta

? Neutra

? Baja

? Muy Baja

¿Conoce las posibilidades que tiene el usuario para determinar la seguridad de un sitio Web antes de relacionarse comercialmente con él?

? SI

? NO

¿Conoce los servicios de e-trust?

? SI

? NO

¿Conoce los servicios de las autoridades certificadoras de e-commerce?

? SI

? NO

Considera a la encriptación como factor de la seguridad en las transacciones condición:

? Necesaria

? Suficiente

? Necesaria y suficiente

¿Qué importancia le da a las políticas de seguridad en sus proyectos de TI?

? Mucha

? Bastante

? Alguna

? Ninguna

¿Sigue buenas prácticas relacionadas con la seguridad (Auditar, utilizar seguridad física, restringir acceso)?

? SI

? NO

¿Le recomendaría a un cliente utilizar el e-commerce?

? SI

? NO