Universidad Michoacana San Nicolás de Hidalgo

Facultad de Contaduría y Ciencias Administrativas

TESINA:

"Seguridad en el Comercio Electrónico"

QUE PARA OBTENER EL TITULO EN LICENCIADA EN INFORMÁTICA ADMINISTRATIVA

Presenta:
ANEL GÓMEZ ESTRADA

ASESOR
M.A. MA. HILDA RODALES TRUJILLO

Morelia, Mich.
Octubre de 2009

Índice

Resumen

Cada vez es más frecuente encontrarnos con portales virtuales que nos ofrecen productos y servicios a través del Internet. Y es por ello que los usuarios que hacen uso de esta servicio, aunque el miedo que existe de aun es muy grande, no es sencillo encontrar personas que den sus datos muy fácilmente, por el miedo que no saber lo que puede pasar con sus cuentas bancarias, que es principal medio de pago en estos portales.

Esto puede deberse a la falta de seguridad que en unos casos está presente y en otros no sabemos hasta que punto es fiable. De ahí se deriva el miedo de los usuarios para usar la compra en línea.

La seguridad hasta ahora, nunca ha sido uno de los principales puntos a la hora de tener en cuenta el desarrollo y la evolución del Internet.

Parece que este detalle tiende a cambiar, y que la seguridad enfocada al comercio electrónico busca la seguridad de los datos de sus usuarios. La incorporación de mecanismos, técnicas y algoritmos adecuados para realizar transacciones electrónicas que lo hace necesario para evitar los riesgos a los que se exponen los usuarios.

Se puede hablar en este sentido de cuatro aspectos básicos de seguridad: autentificación, confidencialidad, integridad y el no-repudio.

Conocer y aplicar conceptos, técnicas y algoritmos para implementar un sistema de seguridad es imprescindible para minimizar riesgos y así poder asegurar al usuario que el comercio electrónico es un mecanismo seguro en el cual puede confiar siempre que se trate con la delicadeza que requiere.

Introducción

En lo que hoy día conocemos como informática confluyen muchas de las técnicas, procesos y máquinas que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar su capacidad de memoria, de pensamiento y de comunicación. De ahí se desglosa la carrera de la licenciatura de informática administrativa, donde el egresado de esta carrera se caracteriza por comprender un ámbito social y laboral. Así mismo se desarrolla como un facilitador de tareas de investigación y en aplicación de la informática a diversos problemas como por ejemplo los de tipo administrativo aplicando el uso adecuado de las tecnologías de información.

Por lo tanto el Licenciado en Informática es un profesional capacitado para relacionarse con profesionales de otras áreas, y su trabajo facilita el proceso de grandes cantidades de información que es utilizada para la toma de decisiones, asegurando un aprovechamiento adecuado de los recursos y tecnologías de información, puede desarrollarse cubriendo necesidades tanto en el sector público como en el privado y en cualquier giro que tenga la organización. Analizar, diseñar e implementar sistemas de información administrativos para cualquier tipo de entidad. Optimizar los procesos, tomando como base la teoría general de sistemas y apoyándose en las áreas de administración, contabilidad, economía y las ciencias sociales. Es así que este se encarga de desarrollar, crear, definir, administrar planes de trabajo que el mismo plantea y crea, como es el desarrollo de las páginas web donde el licenciado aplicada cada una de las técnicas adquiridas durante la carrera.

La complejidad de la seguridad en el comercio electrónico requiere del desarrollo de estrategias que permitan la libre realización del comercio electrónico en el mercado único garantizando al mismo tiempo la seguridad de este.

La utilización creciente de la tecnología de la información en virtualmente todos los ámbitos de la actividad económica publica o privada, parece mostrar que

es merecedora de confianza. Basta la experiencia común para percibir la dependencia de las organizaciones de una tecnología que se ha desarrollado en cinco décadas, en la historia de las invenciones.

Los profesionistas de la informática que se ocupan de la seguridad alertan de los riesgos que pudieran no estar controlados, el objetivo es garantizar la seguridad.

Debido a que el Internet se ha convertido en el medio de interconexión mas utilizada de recursos informáticos, no se puede aceptar la afirmación de que el computador más seguro es aquel que ésta apagado, y por tanto, desconectado a la red.

Ahora bien el principal problema que presenta le comercio electrónico en el Internet es la falta de confianza que tenemos es que todo resulte como se desea.

El primer capitulo se aborda la problemática de la seguridad, desde un ámbito general a un particular. En los primeros días de Internet, el correo electrónico era uno de de usos más populares. Aun así, la gente tenía sería reocupaciones acerca de que un rival comercial interceptarlos mensajes de correo electrónico con objeto de tener información que le pudiera dar una ventaja competitiva. Otro temor era que los supervisores o jefes pudieran leer la correspondencia no comercial de los empleados, con repercusiones negativas.

El segundo capitulo, se enfoca en los conceptos generales de lo que se trata el comercio electrónico, como se usa y como compre los servicios de la compra y venta en el comercio electrónico.

Objetivo

El objetivo principal de este trabajo es brindar y dar a conocer las herramientas necesarias, para que los diseñadores de portales puedan ser brindar un nivel se seguridad sea aceptable hacia el usuario.

Identificar los términos de comercio electrónico y seguridad del comercio electrónico. Conocer las posibles Amenazas, a las que se enfrenta el comercio electrónico.

Hipótesis

Al utilizar las herramientas propuestas de la seguridad en comercio electrónico éste mejorara en:

- El aumento de compras en línea.
- Crear escenarios aceptables para el usuario.
- Información restringida para los persona ajenas al portal.
- Apego a los parámetros legales que el usuario requiere.

Capitulo 1

Seguridad

1. SEGURIDAD

1. 1Seguridad Lógica.

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la seguridad Lógica, podemos pensar en la Seguridad Lógica como la manera de aplicar procedimientos que aseguran que sólo podrán tener acceso a los datos las personas a sistemas de información autorizados para hacerlos.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Los operadores deben trabajar sin supervisión minuciosa y no podrán modificar ni programas archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Asegurar que la información transmitida sea recibida sólo por el destinatario al cual ha sido dirigida y por ningún otro.
5. Asegurar que la información que el destinatario ha recibido sea la misma que ha transmitida.
6. Se debe disponer de sistemas alternativos de transmisión de información entre diferentes puntos.

Los controles de acceso pueden implementar a nivel de sistema Operativo, de sistemas de información, en base de datos en un paquete específico de seguridad o en cualquier otro utilitario.

Estos controles contribuyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional; de que puedan ser utilizados o modificados sin autorización; también para mantener la integridad de la información y para resguardar la información confidencial de accesos no autorizados.

Las consideraciones relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso solicitado por un usuario a un determinado recurso.

1.1 Seguridad Física

Se argumenta que la seguridad perfecta sólo existe en una habitación sin puertas, pero eso naturalmente no es posible, en la actualidad el objeto es prevenir, detectar y detener la ruptura de seguridad informática y de las organizaciones. ISO 17799 ofrece un marco para la definición de la seguridad informática en la organización y ofrece mecanismos para administrar el proceso de seguridad.

Controles de seguridad Física y de Entorno. ISO 17799

Este estándar proporciona a las organizaciones los siguientes beneficios, entre otros:

- Una metodología estructurada reconocida internacionalmente.
- Un proceso definitivo para evaluar, implementar mantener y administrar seguridad informática.
- Una certificación que permite a una organización demostrar su status en seguridad.

ISO 17799 contiene 10 controles de seguridad, los cuales se usan como base para la evaluación de riesgos. Los controles de Seguridad Física manejan los riesgos inherentes a las instalaciones de las empresas:

- Ubicación
- Seguridad en perímetro físico.
- Control de Acceso
- Equipamiento
- Transporte de bienes.

- Políticas y estándares.

Según el planteamiento de Controles de Seguridad Física y de entorno los controles de seguridad física y del entorno se implementan par proteger los ambientes en que se encuentran los recursos del sistema, los recursos del sistemas en sí y los elementos adicionales que permiten su operación, los beneficios que proporcionan las medidas relacionadas a la seguridad física y del entorno incluyen entre otros, la protección de empleados.

Los controles de seguridad física y del entorno, buscan proteger los sistemas informáticos de que se concreten amenazas como:

- Interrupción en la prestación de servicios.
- Daño físico.
- Divulgación no autorizada de información.
- Pérdida de control de la integridad del sistema.
- Robo físico.

Los controles de acceso físico restringen el riesgo el ingreso y salida de personal. Equipos o medios de almacenamiento de un área determinada, su enfoque no es sólo a las áreas en las que se encuentran el hardware del sistema, sino también a la zonas del cableado necesario para conectar los elementos del sistema, de energía eléctrica, aire acondicionado o calefacción, líneas telefónicas, dispositivos, documentos fuente, y otros elementos necesarios para la operación del sistema, eso significa que es necesario identificar todas las zonas de las instalaciones que contengan elementos del sistema.

Es importante revisar los controles de acceso físico a cada área, en horario de trabajo y fuera de él, para determinar si los intrusos pueden evadir los controles y evaluar la efectividad de los procedimientos.

1.2 Seguridad Organizacional.

La mayoría de los sistemas de información no son inherentemente seguros y las soluciones técnicas son sólo una parte de la solución total del problema de seguridad.

La recuperación de desastres es esencial para asegurar, que los recursos informáticos críticos para la operación del negocio. Por eso en esta parte veremos aspectos de seguridad que van mas allá del hardware y del software.

Las principales amenazas que se prevén son:

- Desastres naturales.
- Desastres causados por el hombre.

Los sistemas son vulnerables a una serie de amenazas que pueden ocasionar daños que resulten en pér4didasd significativas. Los daños pueden ser de diversos tipos, como alterar la integridad de la Base de Datos o un incendio que destruya todo el centro de cómputo, por otro lado las pérdidas pueden ser consecuencia de acciones de empleados supuestamente confiables o de hackers externos, la precisión para calcular las pérdidas no siempre es posible, algunas de ellas nunca son descubiertas y otras son barridas bajo la alfombra a fin de evitar publicar desfavorablemente para la organización, los efectos de las amenazas varían desde afectar la confidencialidad e integridad de los datos hasta afectar la disponibilidad del sistema.

Una gran parte de las empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra esta amenaza es uno de los retos mas duros, el saboteador pueden ser un empleado o un sujeto ajeno a la empresa y su motivos pueden ser de los variados.

Desde que la información es procesada y almacenada en computadoras, a la seguridad informática puede ayudar a proteger este recurso, sin embargo es muy poco lo que puede hacer para evitar que un empleado con autorización de acceso de información pueda entregarla o venderla.

El término hacker, se refiere a los atacantes que se introducen en un sistema sin autorización y pueden ser internos o externos a la organización, existen diferencias entre estos atacantes, el hacker tiene por finalidad introducirse en el sistema y hacer notar que lo logró, el que además de introducirse sin autorización destruye sistemas e información es el 'cracker', y los que hacen uso de sus conocimientos de hardware, software y telefonía.

1.3 Criptología

El cifrado o encriptado es el proceso de transformación del texto original en texto cifrado o criptograma, este proceso es llamado encriptación. El contenido de información de texto cifrado es igual al del texto original pero sólo es inteligible para personas autorizadas. El proceso de transformación del criptograma en le texto original se llama des encriptado o descifrado.

La criptografía es la rama del conocimiento que se encarga de la escritura secreta, también se puede definir como la ciencia y arte de describir para que sea indescifrable el contenido del texto original para el que no posea la clave.

El criptoanálisis es la ciencia, o de inserción de textos cifrados falsos, válidos para el receptor. La Criptología es le conocimiento que engloba la criptología y el criptoanálisis y se define la ciencia de la creación y ruptura de cifrados y códigos.

A la técnica de transformación de datos de forma de hacerlos inútiles frente a intrusos se le denomina "criptografía", al arte de desbaratar estas técnicas se le llama "criptoanálisis" y conjuntamente se les conoce como "criptología". Aunque el término "criptología" no está recogido todavía en el Diccionario de la Real

Academia (siendo una traducción directa de la palabra inglesa *Cryptology*) lo cierto es que es de uso común entre los expertos en seguridad de comunicaciones.

Coloquialmente, se consideran erróneamente los términos encriptar y cifrar como sinónimos, al igual que sus respectivas contrapartes, desencriptar y descifrar, pero no ocurre lo mismo con el término codificar. No obstante, se debe utilizar el término cifrar en vez de encriptar, ya que se trata de un anglicismo de los términos ingleses *encrypt* y *decrypt*. Por definición codificar significa expresar un mensaje utilizando algún código, pero no necesariamente de forma oculta, secreta; escribir en idioma español implica el uso de un código, que será comprensible para los hispanohablantes pero no tanto para quienes no dominan el idioma; la matemática y la lógica tienen sus propios códigos, y en general existen tantos códigos como ideas.

El procedimiento utilizado para cifrar datos se realiza por medio de un algoritmo al cual se le puede considerar como una función matemática. Por lo tanto, un algoritmo de cifrado es una fórmula para desordenar una información de manera que ésta se transforme en incomprensible, usando un código o clave (en ocasiones, más de una). Los mensajes que se tienen que proteger, denominados texto en claro, se transforman mediante esta función, y a la salida del proceso de puesta en clave se obtiene el texto cifrado, o cifrograma. En muchos casos, existe un algoritmo de descifrado encargado de reordenar la información y volverla inteligible, pero no siempre es así. Cuando existen ambas funciones, una para cifrar y otra para descifrar, se dice que el sistema criptográfico es de dos vías o reversible (a partir de un mensaje en claro se puede obtener uno cifrado y a partir de éste se puede obtener el mensaje original), mientras que cuando no existe una función para descifrar se dice que el sistema es de una sola vía (a partir de un mensaje cifrado no es posible obtener el mensaje en claro que lo generó; la aplicación de esto es, por ejemplo, para el almacenamiento de contraseñas).

La transformación de datos provee una posible solución a dos de los problemas de la seguridad en el manejo de datos. El problema de la privacidad y

el de la autenticación, evitando que personas no autorizadas puedan extraer información del canal de comunicación o modificar estos mensajes.

Desde el punto de vista histórico los métodos de cifrado se han dividido en dos categorías: cifradores de sustitución y cifradores de transposición. En un cifrador de sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para disfrazarlas. Los cifradores de sustitución preservan el orden de los símbolos del texto en claro, pero los disfrazan. El cifrador de sustitución más antiguo que se conoce es el cifrador de César, atribuido a Julio César. En este método, A se representa por D, B por E, C por F, y así cada letra se sustituye por la que se encuentra tres lugares delante de ella, considerando que luego de la Z vuelve a comenzar por la A. Una variante del cifrador de César es permitir que el alfabeto cifrado se pueda desplazar k letras (no sólo 3), convirtiéndose k en la clave.

1.3.1 Firma digital

La firma digital es, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

La firma electrónica, como la manuscrita, puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

La Ley 59/2003 de Firma digital que puede ser diferente en cada país, define tres tipos de firma:

- **Simple**. Incluye un método de identificar al firmante

- **Avanzada**. Además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI
- **Reconocida**. Es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante)

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente, funciona en una sola dirección, es decir, no es posible a partir del valor resumen calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades para el usuario, para ello se usan software que automatizan tanto la función de calcular el valor hash como su verificación posterior.

Para que sea de utilidad, la función hash debe satisfacer dos importantes requisitos. Primero, debe ser difícil encontrar dos documentos cuyo valor para la función "hash" sea idéntico. Segundo, dado uno de estos valores, debería ser difícil recuperar el documento que lo produjo.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla.

Existen funciones "hash" específicamente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos. Para usarlos un documento se firma con una función "hash", cuyo resultado es la firma. Otra persona puede comprobar la firma aplicando la misma función a su copia del documento y comparando el resultado con el del documento original. Si concuerdan, es casi seguro que los documentos son idénticos.

Claro que el problema está en usar una función "hash" para firmas digitales que no permita que un "atacante" interfiera en la comprobación de la firma. Si el documento y la firma se enviaran descifrados, este individuo podría modificar el documento y generar una firma correspondiente sin que lo supiera el destinatario. Si sólo se cifrara el documento, un atacante podría manipular la firma y hacer que la comprobación de ésta fallara. Una tercera opción es usar un sistema de cifrado híbrido para cifrar tanto la firma como el documento. El firmante usa su clave privada, y cualquiera puede usar su clave pública para comprobar la firma y el documento. Esto suena bien, pero en realidad no tiene sentido. Si este algoritmo hiciera el documento seguro también lo aseguraría de manipulaciones, y no habría necesidad de firmarlo. El problema más serio es que esto no protege de manipulaciones ni a la firma, ni al documento. Con este método, sólo la clave de sesión del sistema de cifrado simétrico es cifrada usando la clave privada del firmante. Cualquiera puede usar la clave pública y recuperar la clave de sesión. Por lo tanto, resulta obvio usarla para cifrar documentos substitutos y firmas para enviarlas a terceros en nombre del remitente.

Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir.

El Digital Signature Algorithm es un algoritmo de firmado de clave pública que funciona como hemos descrito. DSA es el algoritmo principal de firmado que se usa en GnuPG.

1.3.2 Certificados Digitales

Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente el nombre de la entidad certificada, un número serial, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital), y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

Emisores de certificados

Cualquier individuo o institución puede generar un certificado digital pero si éste *emisor* no es reconocido por quienes interactuaran con el propietario del certificado, es casi igual a que si no hubiese sido firmado. Por ello los emisores deben acreditarse para así ser reconocidos por otras personas, comunidades, empresas o países y que su firma tenga validez.

La gran mayoría de los emisores tiene fines comerciales, y otros, gracias al sistema de Anillo de confianza pueden otorgar gratuitamente certificados en todo el mundo, como:

- CAcert.org, emisor administrado por la comunidad con base legal en Australia.
- Thawte, sólo para certificados personales. Emisor propiedad de Verisign.

Pero para que un certificado digital tenga validez legal, el prestador de Servicios de Certificación debe acreditarse en cada país de acuerdo a la normativa que cada uno defina.

Encargados de autorizar la creación de una Autoridad de certificación o Prestador de Servicios de Certificación de algunos países son:

- En México, la Secretaría de Economía.
- En Chile, el Ministerio de Economía.
- En España: el Ministerio de Industria, Turismo y Comercio y Agencia Catalana de Certificación.
- En Venezuela, la SUSCERTE - MCT (Superintendencia de Servicios de Certificación Electrónica)
- En Perú, el INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual)

- En la República Dominicana el Indotel (Instituto Dominicano de las Telecomunicaciones)
- En Colombia, Certicámara (La Sociedad Cameral de Certificación Digital Certicámara S.A.)

1.4 Seguridad en Infraestructura

Los retos, expectativas y oportunidades del entorno empresarial actual han llevado a muchas empresas a moverse hacia el modelo de empresa sin perímetro. Aunque mejora la capacidad de competir y de adaptarse a las condiciones cambiantes, esta transformación también aumenta ciertos riesgos y vulnerabilidades. El aumento del acceso de clientes, por ejemplo, aumenta la importancia y la complejidad de establecer una protección contra amenazas como la manipulación de la identidad de los clientes. Esto requiere una estrategia para gestionar identidades, proteger datos y asegurar las redes y transacciones y una infraestructura que pueda ayudar a protegerse a sí misma. Cada nueva oportunidad y ventaja de IT incorpora su propio riesgo potencial en cuanto a seguridad; riesgo que se debe gestionar de forma continuada, se debe supervisar y se debe auditar, sin perder de vista los costos.

Lo que se necesita es un enfoque completo a la gestión de riesgos de seguridad; uno que incluya políticas gubernamentales de seguridad de IT, procesos de seguridad y gestión de controles y sistemas que ayuden a protegerse a sí mismos. Está en juego no sólo la seguridad de los datos y de la red, sino también la pérdida potencial de beneficios de la empresa, de reputación y de ventaja competitiva. Su seguridad es un problema de IT y un problema de confianza en la marca. Para proteger su infraestructura vital frente a daños deliberados o accidentales, el enfoque debe integrar funciones de seguridad en la infraestructura, no solucionar los retos después de materializarse el riesgo.

Infraestructura Extendida de Seguridad (IES)

- Autoridad Central
- Agencia Registradora
- Agencia Certificadora
- Agentes Certificadores
- Aplicaciones de Usuarios
- Base de Datos Registradora Aplicativa
- Aplicaciones

1.5 Niveles de seguridad Informática

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book(**), desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos. Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1 y el D.

Nivel D: Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.
Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

Nivel C1: Protección Discrecional Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "súper usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

Nivel C2: Protección de Acceso Controlado Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a

usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoría requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.
Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Nivel B1: Seguridad Etiquetada Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

Nivel B2: Protección Estructurada Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior.

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

Nivel B3: Dominios de Seguridad Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y test ante posibles violaciones.

Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.
Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Nivel A: Protección Verificada Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

Capitulo 2

Comercio Electrónico

2.1 Introducción al Comercio electrónico.

Actualmente el comercio electrónico no es lo que fue ayer o lo que habrá de ser mañana. El comercio electrónico de bienes, servicios e información por medio de sitios electrónicos, tal y como lo conocemos hoy en día, se origino en 1991 cuando internet entró de lleno al uso comercial. Ahora existen miles de sitios electrónicos y cientos de compañías que realizan diariamente transacciones multimillonarias por la red.

Esta revolución en al comunicación tuvo un inicio bastante interesante. Internet es la versión más reciente de una combinación de redes entre universidades, dependencias gubernamentales, grandes corporaciones y organismos de investigación. En 1969, el Departamento de la Defensa de los Estados Unidos creó una red llamada ARPANET (*Advanced Research Projects Agenncy*, *Dirección de Proyectos de Investigación avanzad)*.

El comercio electrónico es una fuerza dinámica dentro de la economía de los Estados Unidos y del mundo entero. El uso de Internet en la actividad comercial está revolucionando la forma de la que el mundo corporativo realiza negocios, además está aumentando el poder de la economía, ya que este medio logra comunicar a las grandes empresas con los nuevos líderes comerciales. Las pequeñas empresas tienen acceso a los clientes mediante el uso de Internet. Hoy en día, millones de clientes en todo el mundo pueden solicitar bienes y servicios durante las 24 horas del día, los siete días de al semana.

Diariamente los individuos, las pequeñas empresas, las grandes corporaciones y los gobiernos realizan negocios por Internet. La mayor parte de las transacciones se llevan a cabo por medio de computadoras personales. Sin embargo cambiando rápidamente, pues el auge del comercio electrónico genera una demanda de movilidad. (** Gary P. Schneider)

El término "comercio electrónico" se refiere a la venta de productos y servicios por Internet. Actualmente, este segmento presenta el crecimiento más acelerado de la economía. Gracias al costo mínimo que implica, hasta la empresa más pequeña puede llegar a clientes de todo el mundo con sus productos y mensajes. En la actualidad, más de 250 millones de personas en todo el mundo utilizan Internet habitualmente. (***Brian Kerns)*

El 69% de la población conectada a la red ha realizado al menos una compra en los últimos 90 días. Teniendo en cuenta estos datos, los analistas estiman que este sistema generará ventas por un valor de USD 3,2 mil millones de dólares hasta el año 2004. Si se calcula que el ingreso promedio familiar de los usuarios de Internet asciende a USD 59.000, captar a este público objetivo de gran atractivo sería muy beneficioso para su negocio.

El comercio electrónico en México beneficia no solo al proveedor que es quien anuncia su producto, sino también al consumidor; otra de las ventajas de la utilización del mismo es que se puede pagar sin tener dinero en efectivo, que es en la mayoría de las ocasiones, siendo a través de tarjeta de crédito, actualizándose y utilizándose no solo el comercio y mercadotecnia, sino también la banca.

2.2 Requisitos del Comercio Electrónico

El principal requisito en una transacción de comercio electrónico es la seguridad como en todas las transacciones que implica el manejo de dinero. (** Oelkers)

Pero hay dos requisitos aconsejables apara que los sistemas de comercio electrónico sean comparables a los de monedas y billetes, sino no se aplican pueden que el comercio electrónico no se atractivo para los usuarios. Estas son:

- **Anonimato.** Con monedas o billetes la identidad del comprador no es conocida por el vendedor. Para poder mantener también en el comercio electrónico el derecho propio de los humanos a la intimidad, nadie excepto el banco propio deberían conocer l identidad del comprador y éste no debería conocer la naturaleza de la compra.
- **Flexibilidad.** Poder aceptar diferentes medios de pago para todas las situaciones posibles de usuarios de Internet.
- **Convertibilidad.** Poder transformar los diferentes sistemas de pago sin necesidad de realizar una compra, como pasa con las divisas y las cuentas de los bancos.
- **Eficiencia.** El coste del sistema de comercio no debe ser mayor que el precio del producto o servicio.
- **Ser divisible.** Como las monedas o billetes poder dividir la posibilidad de compra en fracciones más pequeñas.
- **Transferible.** Poder pasar el poder de compra de una persona a otra sin necesidad de realizar una transacción, igual que se puede prestar a regalar el dinero tradicional.

El único sistema de pago que cumple todos los requisitos es el dinero electrónico.

2.3 Dinero Electrónico

Estos sistemas deben cumplir todos los requisitos comentados anteriormente, por lo tanto tienen exactamente las mimas funciones que las monedas y los billetes.

Se utilizan diversas tecnologías para implementarlos.

- **Números Firmados.** La entidad financiera emite unos números aleatorios y los firma con su clave privada. Estos números están registrados en la base

de datos de la entidad. Su valúa depende de la longitud del número y se pueden fraccionar cambiándolos en la entidad. Los usuarios los piden por la entidad a cambio de un cargo a su cuenta o tarjeta y los utilizan o dan cuando creen conveniente. El sistema DigiCash trabaja con este tipo de dinero electrónico.

- **Monederos Electrónicos.** Son tarjetas con un chip donde se almacenan cantidades de dinero que previamente se han desconectado de una cuenta. El poseedor de la tarjeta posee el dinero de forma anónima y los puede gastar cuando y de la forma que quiera, así como prestar. Estos sistemas ya se utilizan en las compras físicas, pero para Internet se debería construir ordenadores con lectores adecuados.

Capitulo 3

Sistemas de Seguridad en el Comercio Electrónico

3.1 SSL (Secure Sockets Layer)

3.1.1 Características

EL SSL es un protocolo seguro de Internet inventado por la empresa Netscape. No es exclusivo del comercio electrónico sino que sirve para cualquier comunicación vía Internet y, por lo tanto, también para transacciones económicas. Esta implementado para el protocolo HTTP.

Sustituye los sockets del sistema operativo. Los sockets son el interface entre las aplicaciones y el protocolo TCP/IP del sistema operativo (Figura 3.1.1.1). Así puede servir para cualquier aplicación que utilice TCP/IP: Mail, Webs, FTP, News, etc.

Aunque las aplicaciones de los programas actuales sólo permiten HTTP (Webs).

Aplicación
SSL
TCP
IP
…….

Situación del SSL en la pila TCP/IP
**Manuel Pons Martorell

Para diferenciar las páginas dentro de una zona de servidor SSL, Netscape utiliza la denominación http y se conecta mediante e puesto 443.

El SSL puede realizar las funciones:

- **Fragmentación.** En el emisor se fragmentan los bloques mayores que 2_{14} octetos y el receptor se vuelven a re ensamblar.
- **Compresión**. Se puede aplicar algoritmo de compresión a los mensajes.
- **Autenticación.** Permite autenticar el cliente y el servidor mediante certificados. Este proceso se realiza durante la fase de Handshake. Durante la transmisión los mensajes autentican al emisor mediante un resumen con clave, llamado MAC, en cada mensaje.
- **Integridad.** En todos los mensajes se protege la integridad mediante el Mac
- **Confidencialidad.** Todos los mensajes se envían encriptados.

Se utilizan certificados X.509v3 para la transmisión de las claves públicas.

3.1.2 Protocolo SSL

El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA 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 reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 se usa como algoritmo de hash.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

Cuando el cliente pide al servidor seguro una comunicación segura, el servidor abre un puerto cifrado, gestionado por un software llamado Protocolo SSL Record, situado encima de TCP. Será el software de alto nivel, Protocolo SSL Handshake, quien utilice el Protocolo SSL Record y el puerto abierto para comunicarse de forma segura con el cliente.

El Protocolo SSL Handshake

Durante el protocolo SSL Handshake, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad. Este protocolo sigue las siguientes seis fases:

- La fase **Hola**, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la intimidad y para la autenticación.
- La fase de **intercambio de claves**, en la que intercambia información sobre las claves, de modo que al final ambas partes comparten una clave maestra.
- La fase de **producción de clave de sesión**, que será la usada para cifrar los datos intercambiados.
- La fase de **verificación del servidor**, presente sólo cuando se usa RSA como algoritmo de intercambio de claves, y sirve para que el cliente autentique al servidor.
- La fase de **autenticación del cliente**, en la que el servidor solicita al cliente un certificado X.509 (si es necesaria la autenticación de cliente).
- Por último, la fase de **fin**, que indica que ya se puede comenzar la sesión segura.

El Protocolo SSL Record

El Protocolo SSL Record especifica la forma de encapsular los datos transmitidos y recibidos. La porción de datos del protocolo tiene tres componentes:

- MAC-DATA, el código de autenticación del mensaje.
- ACTUAL-DATA, los datos de aplicación a transmitir.
- PADDING-DATA, los datos requeridos para rellenar el mensaje cuando se usa cifrado en bloque.

3.2 TLS (Transport layer security)

3.2.1 Protocolo TLS

El TLS es un protocolo estandarizado por el IETF, por lo tanto, es un estándar de facto de Internet. Su origen es el SSL pero se parte de éste para mejorar algunas cosas y, sobre todo, porque SSL es propiedad de una empresa privada: Netscape. Así el TLS puede ser le estándar mundial para todo el software de cliente y servidor. El TLS permite compatibilidad con SSLv3, el cliente y el servidor definen el protocolo utilizando el Handshake. (**Manuel Pons Martorell)

Las diferencias más importantes son sobre los siguientes aspectos:

- **Alerta de certificado.** En respuesta al mensaje CertificateRequest los clientes que no tienen que no tienen certificado sólo contestan con un menaje de alerta si son SSL.
- **Claves de Sesión.** Se calculan de forma diferente.
- **Algoritmos de intercambio de claves.** El TLS no soporta al algoritmo Fortaleza Kea del SSl, un algoritmo secreto y de propiedad privada muy similar al Diffie Hellman.
- **Campos incluidos en le Mac** En TLS se utilizan dos campos más del mensaje que en SSL para el cálculo del MAC. Es mas seguro.

3.3 SET (Secure Electronic Transaction)

3.3.1 Características

El SET es un protocolo inventado exclusivamente para realizar comercio electrónico con tarjetas de crédito. Fue impulsado por las empresas de tarjetas de crédito Visa y MasterCard, las más extendidas e importantes del mundo. Han colaborado en su desarrollo las empresas más significativas del mundo de la telemática: GTE, IBM, Microsoft, SAIC, Terisa, Verisign, etc. La participación de estas empresas tan importantes y especialmente el impulso de las marcas de tarjetas Visa y MasterCard hacen que este protocolo tenga muchas posibilidades de convertirse en el futuro sistema de comercio electrónico seguro.

Es un sistema abierto y multiplataforma, donde se especifican protocolos, formatos de mensajes, certificados, etc. Sin limitación de lenguaje de programación sistema operativo o máquina. El formato de mensaje está basado en el estándar definido por la empresa RSA Data Security Inc. PKCS-7, como los protocolos S-MINE y SSL. (**Manuel Pons Martorell)

3.3.2 Agentes del comercio Electrónico SET

En SET se definen 5 agentes que pueden intervenir en transacciones comerciales:

- **Comprador.** Adquiere un producto utilizando la tarjeta de crédito de su propiedad.
- **Banco o entidad financiera.** Emite la tarjeta de crédito de 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 no actúan directamente en las transacciones son:

- **Propietario de la marca de la tarjeta.** Avalan las tarjetas.
- **Autoridad de certificación.** Crea los certificados que se utilizan en las transacciones de la pasarela, el velador y el comprador. Pueden ser los bancos, los propietarios de la marca de la tarjeta o entidades independientes.

Comercio Electrónico

2.1 Introducción al Comercio electrónico.

Actualmente el comercio electrónico no es lo que fue ayer o lo que habrá de ser mañana. El comercio electrónico de bienes, servicios e información por medio de sitios electrónicos, tal y como lo conocemos hoy en día, se origino en 1991 cuando internet entró de lleno al uso comercial. Ahora existen miles de sitios electrónicos y cientos de compañías que realizan diariamente transacciones multimillonarias por la red.

Esta revolución en al comunicación tuvo un inicio bastante interesante. Internet es la versión más reciente de una combinación de redes entre universidades, dependencias gubernamentales, grandes corporaciones y organismos de investigación. En 1969, el Departamento de la Defensa de los Estados Unidos creó una red llamada ARPANET (*Advanced Research Projects Agenncy*, *Dirección de Proyectos de Investigación avanzad)*.

El comercio electrónico es una fuerza dinámica dentro de la economía de los Estados Unidos y del mundo entero. El uso de Internet en la actividad comercial está revolucionando la forma de la que el mundo corporativo realiza negocios, además está aumentando el poder de la economía, ya que este medio logra comunicar a las grandes empresas con los nuevos líderes comerciales. Las pequeñas empresas tienen acceso a los clientes mediante el uso de Internet. Hoy en día, millones de clientes en todo el mundo pueden solicitar bienes y servicios durante las 24 horas del día, los siete días de al semana.

Diariamente los individuos, las pequeñas empresas, las grandes corporaciones y los gobiernos realizan negocios por Internet. La mayor parte de las transacciones se llevan a cabo por medio de computadoras personales. Sin embargo cambiando rápidamente, pues el auge del comercio electrónico genera una demanda de movilidad.

El término "comercio electrónico" se refiere a la venta de productos y servicios por Internet. Actualmente, este segmento presenta el crecimiento más acelerado de la economía. Gracias al costo mínimo que implica, hasta la empresa más pequeña puede llegar a clientes de todo el mundo con sus productos y mensajes. En la actualidad, más de 250 millones de personas en todo el mundo utilizan Internet habitualmente. (**Brian Kerns)*

El 69% de la población conectada a la red ha realizado al menos una compra en los últimos 90 días. Teniendo en cuenta estos datos, los analistas estiman que este sistema generará ventas por un valor de USD 3,2 mil millones de dólares hasta el año 2004. Si se calcula que el ingreso promedio familiar de los usuarios de Internet asciende a USD 59.000, captar a este público objetivo de gran atractivo sería muy beneficioso para su negocio.

El comercio electrónico en México beneficia no solo al proveedor que es quien anuncia su producto, sino también al consumidor; otra de las ventajas de la utilización del mismo es que se puede pagar sin tener dinero en efectivo, que es en la mayoría de las ocasiones, siendo a través de tarjeta de crédito, actualizándose y utilizándose no solo el comercio y mercadotecnia, sino también la banca.

2.2 Requisitos del Comercio Electrónico

El principal requisito en una transacción de comercio electrónico es la seguridad como en todas las transacciones que implica el manejo de dinero.

Pero hay dos requisitos aconsejables apara que los sistemas de comercio electrónico sean comparables a los de monedas y billetes, sino no se aplican pueden que el comercio electrónico no se atractivo para los usuarios. Estas son:

- **Anonimato.** Con monedas o billetes la identidad del comprador no es conocida por el vendedor. Para poder mantener también en el comercio electrónico el derecho propio de los humanos a la intimidad, nadie excepto el banco propio deberían conocer l identidad del comprador y éste no debería conocer la naturaleza de la compra.
- **Flexibilidad.** Poder aceptar diferentes medios de pago para todas las situaciones posibles de usuarios de Internet.
- **Convertibilidad.** Poder transformar los diferentes sistemas de pago sin necesidad de realizar una compra, como pasa con las divisas y las cuentas de los bancos.
- **Eficiencia.** El coste del sistema de comercio no debe ser mayor que el precio del producto o servicio.
- **Ser divisible.** Como las monedas o billetes poder dividir la posibilidad de compra en fracciones más pequeñas.
- **Transferible.** Poder pasar el poder de compra de una persona a otra sin necesidad de realizar una transacción, igual que se puede prestar a regalar el dinero tradicional.

El único sistema de pago que cumple todos los requisitos es el dinero electrónico.

2.3 Dinero Electrónico

Estos sistemas deben cumplir todos los requisitos comentados anteriormente, por lo tanto tienen exactamente las mimas funciones que las monedas y los billetes.

Se utilizan diversas tecnologías para implementarlos.

- **Números Firmados.** La entidad financiera emite unos números aleatorios y los firma con su clave privada. Estos números están registrados en la base de datos de la entidad. Su valúa depende de la longitud del número y se pueden fraccionar cambiándolos en la entidad. Los usuarios los piden por la entidad a cambio de un cargo a su cuenta o tarjeta y los utilizan o dan cuando creen conveniente. El sistema DigiCash trabaja con este tipo de dinero electrónico.
- **Monederos Electrónicos.** Son tarjetas con un chip donde se almacenan cantidades de dinero que previamente se han desconectado de una cuenta. El poseedor de la tarjeta posee el dinero de forma anónima y los puede gastar cuando y de la forma que quiera, así como prestar. Estos sistemas ya se utilizan en las compras físicas, pero para Internet se debería construir ordenadores con lectores adecuados.

Capitulo 4

Marco Legal

Legislación Nacional - México

1) Esta Dictaminadora reconoce que a partir del primero de enero de 1999, las modificaciones que el Congreso de la Unión realice al Código Civil producirán efectos exclusivamente en el ámbito federal, en virtud de ello se considera procedente la propuesta del Grupo Parlamentario del Partido Revolucionario Institucional de modificar la denominación actual de este cuerpo normativo, por la de Código Civil Federal, así como modificar el artículo 1°, con el fin de precisar su ámbito material de validez.

2) La que dictamina también considera acertado reformar el artículo 1803 del Código Civil, para incorporar la posibilidad de que las partes puedan manifestar su voluntad u ofertar algún bien o servicio mediante el uso de medios electrónicos. Sin embargo, en esta parte aún cuando en el concepto coinciden las iniciativas que ahora se dictaminan, la presentada por el Grupo Parlamentario del Partido Acción Nacional introduce la definición de "Mensaje de datos", entendiendo como tal la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o a través de cualquiera otra tecnología, término que es utilizado a lo largo del todo el texto de su iniciativa. En tanto que la iniciativa del Grupo Parlamentario del Partido Revolucionario Institucional, hace referencia a lo largo de su propuesta precisamente a la utilización de medios electrónicos, ópticos o de cualquier otra tecnología. Al respecto, esta Dictaminadora considera más acertada la segunda de las propuestas mencionadas, dado que en el artículo 1803 se hace referencia a los medios para expresar el consentimiento, más que a la información generada, enviada, recibida, archivada o comunicada por dichos medios.

3) En cuanto a la propuesta de adición al artículo 1811 del Código Civil, presentada por el Partido Acción Nacional, referente a la validez de la propuesta y aceptación de la misma hecha por medios electrónicos, esta Dictaminadora considera necesario precisar la redacción de la adición para precisar que tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos, como lo señala al día de hoy dicho artículo tratándose de la propuesta y aceptación hechas por telégrafo. La redacción quedaría de la manera siguiente:

"Artículo 1811.-...

Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos."

4) Por lo que hace a la reforma al artículo 1834 del Código Civil propuesta por el Grupo Parlamentario del Partido Acción Nacional, esta Dictaminadora considera necesario también establecer las disposiciones que regularán la exigencia de la forma escrita, cuando se utilicen los medios electrónicos; sin embargo, coincide con el Grupo Parlamentario del Partido Revolucionario Institucional, de que se requiere actualizar los alcances de la legislación civil vigente en lo relativo a los actos que requieren de la forma escrita otorgada ante un fedatario público, y que bien pueden conservar e incluso fortalecer la seguridad jurídica en beneficio de los obligados, si se utilizan medios electrónicos, ópticos o cualquier otra tecnología, conforme a un procedimiento claro y particularmente descriptivo que acredite la atribución de información a una persona, y asegure que ésta será susceptible de consulta posterior. Por lo que se considera certera la adición del artículo 1834 bis, con algunas precisiones en la redacción como a continuación se señala:

"Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión integra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.**"**

5) Se considera innecesaria la propuesta de adición al artículo 217 del Código Federal de Procedimientos Civiles, hecha por el Grupo Parlamentario del Partido Acción Nacional, pues sólo reitera que tratándose de "mensaje de datos" (información generada o comunicada por medios electrónicos, ópticos o por

cualquier otra tecnología), se regirá por los artículos específicos: 210-A y 210-B de ese mismo Código.

6) En cuanto a la adición de los artículos 210-A y 210-B al Código Federal de Procedimientos Civiles, hecha por el Grupo Parlamentario del Partido Acción Nacional, que se refieren respectivamente al reconocimiento jurídico y a la valoración probatoria de los "mensajes de datos", esta Dictaminadora considera oportuno prever fusionar tales disposiciones en un solo artículo, como sigue:

"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea presentado y conservado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.**"**

7) Por lo que hace a la propuesta de reforma a los artículos 47, 48 y 49 del Código de Comercio, hecha por el Grupo Parlamentario del Partido Acción Nacional, relacionados con la obligación de los comerciantes de conservar todo tipo de documentos, incluyendo los "mensajes de datos", con el objeto de que dicha obligación no represente una carga innecesaria de conservación de documentos para los comerciantes, la que dictamina considera adecuado acotarla a aquellos documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones. Asimismo, esta Comisión considera importante señalar los requisitos mínimos de conservación de originales, así como la autoridad facultada para emitir los requisitos para dicha conservación.

8) Respecto de la propuesta de artículo 641 de la iniciativa hecha por el Grupo Parlamentario del Partido Acción Nacional, de las definiciones ahí señaladas sólo se considera importante la de mensaje de datos y sistema de información, ya que los términos de emisor y destinatario se explican por si mismos. Asimismo, el

contenido del artículo 642 de dicha iniciativa sobre los contratos mercantiles celebrados mediante el uso de medios electrónicos, se considera más adecuado incorporarlo en el artículo 80 del Código de Comercio, que es el precepto que al día de hoy regula los medios para la celebración de los contratos, el mismo criterio se aplica respecto del contenido del artículo 643 que habla de la conservación de información, pues la regulación para tal efecto es más adecuada incorporarla en el artículo 49 del Código de Comercio, en la que sólo habrá que agregar el supuesto de conservación, por lo que dichos artículos quedarían de la manera siguiente:

"Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.

Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos**".**

"Artículo 641.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos**."**

"Artículo 642.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor sí ha sido enviado:

I.- Usando medios de identificación, tales como claves o contraseñas de él, o;

II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.

9) Además, en este mismo sentido esta Comisión considera que el contenido de los nuevos artículos 644 y 645 que propone el Grupo Parlamentario del Partido

Acción Nacional debe homologarse a la propuesta de contenido del artículo 1834 bis del Código Civil, para quedar como sigue:

"Artículo 645.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.

En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión integra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.**"**

10) Por lo que hace al artículo 646, que refiere a las reglas de conservación, dicha disposición la que dictamina la considera más adecuada incorporarla en el artículo 49 del Código de Comercio, ya que la acota, como se ha señalado, a aquellos documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.

11) En cuanto al contenido del artículo 647 iniciativa hecha por el Grupo Parlamentario del Partido Acción Nacional, que se refiere a la validez y fuerza obligatoria a la manifestación de la voluntad hecha por "mensaje de datos", se considera oportuna, pero debe incorporarse en la parte adjetiva del Código de Comercio, como lo propone el Partido Revolucionario Institucional mediante la adición del artículo 1298-A.

12) Esta Dictaminadora considera importante establecer en el Código de Comercio, como lo propone el Grupo Parlamentario del Partido Acción Nacional, las disposiciones que regulen lo relativo a mensajes de datos que requieran de un acuse de recibo y del lugar en que se tendrá pro expedido un mensaje de datos, por lo que deben preverse en los artículos 644 y 646, lo siguiente:

"Artículo 644.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo.

Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente."

"Artículo 646.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo."

13) Esta Dictaminadora, en atención al contenido del Libro Tercero y de su único Título que se propone denominado "Del Comercio Electrónico", y a que el Libro Segundo del Código de Comercio se refiere al comercio terrestre, considera que la ubicación del nuevo Titulo es más apropiada en el contexto de este Libro Segundo, para lo cual se modificaría la denominación del mismo por la de "Comercio en general", y se incorporaría en su Título II que se llamaría "Del Comercio Electrónico", a partir del artículo 89, actualmente derogados, de tal forma que los artículos 641 a 646 antes mencionados pasarían a ser los numerales 89 a 94 del Código de Comercio.

14) Por otra parte, a esta Comisión le fue turnada también para su dictamen una iniciativa presentada el pasado 9 de diciembre de 1999 por los Diputados integrantes de los Grupos Parlamentarios del Partido Acción Nacional, del Partido Revolucionario Institucional y del Partido Verde Ecologista de México, entre las propuestas de reforma y adición contenidas en la misma se encuentra una modificación al Código de Comercio en la parte que regula el Registro Público de Comercio operado por medios electrónicos.

Dicha modificación propone reformar el artículo 18 del Código de Comercio para señalar que la operación del Registro Público de Comercio estará a cargo de la Secretaría de Comercio y Fomento Industrial, y de las autoridades responsables del registro público de la propiedad de los Estados y en el Distrito Federal, en términos del propio Código, y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la Constitución Política de los Estados Unidos Mexicanos. Asimismo, se propone que para tal efecto, existan en cada entidad federativa, las oficinas del Registro Público de Comercio que demande el tráfico mercantil, con el objeto de mejorar la administración y operación del mismo, y hacerlo uniforme, eficiente y seguro para la sociedad.

De igual forma, se propone reformar el artículo 20, para señalar que el Registro Público de Comercio operará con un programa informático y con una base de datos central, la cual estará interconectada mediante medios electrónicos con las bases de datos que sobre este Registro se integren en las oficinas estatales.

Con dicho programa informático, se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral. Con ello se automatizará la inscripción y la consulta de los actos registrales, y se sustituirá al tradicional esquema de libros y folios mercantiles previstos en la normatividad vigente a nivel de reglamento.

Las bases de datos estatales del Registro Público de Comercio, se integrarán con la información incorporada por medio del programa informático, respecto de cada inscripción o anotación de los actos mercantiles inscribibles, y la base central con la información que los responsables del Registro incorporen en las bases de datos estatales. Dicha base central tendrá por objeto resguardar a nivel nacional los asientos registrales en materia mercantil. Además, para garantizar la seguridad sobre el resguardo de la información registral, se dispone que las bases de datos cuenten con, al menos, un respaldo electrónico.

El programa informático será establecido por la Secretaría de Comercio y Fomento Industrial. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal.

En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en alguna base de datos estatal, o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario.

**** Gaceta Parlamentaria, año III, número 500, miércoles 26 de abril de 2000**

Capitulo 5

RECOMENDACIONES DE SEGURIDAD

Con el objetivo de comprender claramente la importancia de la seguridad en un sistema de información de las paginas web, se hizo la recopilación de información presentada en los capítulos anteriores acerca de cuáles son los elementos que podrían constituir fallas o posiciones que no otorgan o comprenden un nivel aceptable de seguridad informática para las distintas aplicaciones que se manejan hoy en día, así como las principales vulnerabilidades que afectan a los distintos sistemas operativos con mayor cantidad de usuarios, y las leyes que rigen estos elementos.

Este capitulo muestra los resultados de la investigación en herramientas de seguridad.

VULNERABILIDADES Y RECOMENDACIONES DE SEGURIDAD

El éxito en los ataques a los sistemas operativos se debe en su mayor parte al aprovechamiento de unas pocas vulnerabilidades del software utilizado. Los atacantes son siempre oportunistas y por lo general explotan las fallas más conocidas con las herramientas que estén disponibles. Muchos de los ataques en la web, como se ha mencionado en capítulos anteriores, se basan en aprovechar que las organizaciones no reparan las vulnerabilidades con parches informáticos ya existentes.

La reparación de vulnerabilidades no se lleva a cabo por diversas razones, como el no saber cuales son las más riesgosas, la cantidad de trabajo no permite su solución, o no hay conocimiento de cómo arreglarlas de una manera segura. Además que si se aplica un scanner de riesgos a un sistema web el número de vulnerabilidades puede alcanzar cantidades de dos mil, y eso impresiona a cualquiera. Sin embargo, muchas de estas fallas pueden repararse al actualizar el sistema o descargar los parches necesarios. Por ello, la finalidad es que este documento sea de utilidad para todo aquel que desee iniciarse en la seguridad informática A continuación se describen a detalle las principales vulnerabilidades de cada sistema operativo, y se proponen soluciones para estos problemas de seguridad.

1. **Servicios de Información de Internet en Internet Explorer (IIS)**. IIS presenta vulnerabilidades de tres clases principales: incapacidad para manejar peticiones no anticipadas, desbordamientos de buffer y aplicaciones de muestra.

- Incapacidad de Manejar Peticiones no Anticipadas. Muchas de las vulnerabilidades de IIS están relacionadas con la incapacidad de manejar peticiones HTTP formadas impropiamente. Un buen ejemplo es la vulnerabilidad Unicode directory traversal explotada por el gusano (worm) Code Blue. Si se arma una petición que explote una de estas vulnerabilidades, un atacante remoto puede hacer lo siguiente: Ver el código fuente de las aplicaciones utilizadas, ver los archivos fuera de la raíz de documentos Web, ver los archivos que el servidor de Internet ha sido instruido para no servir, ejecutar comandos arbitrarios en el servidor para borrar archivos o instalar una puerta trasera.
- Desbordamientos del Buffer. Muchas extensiones ISAPI; tales como ASP, HTR, IDQ, PRINTER, SSI; son vulnerables a desbordamientos de buffer. Un ejemplo es la vulnerabilidad de la extensión ISAPI **.idq**, la cual fue aprovechada por los gusanos Code Red y Code Red II. Una petición cuidadosamente creada de un atacante remoto puede resultar en lo siguiente: Negación de servicio, ejecución arbitraria de código o comandos en el contexto del usuario de servidor de Internet.
- Aplicaciones de Muestra. Las aplicaciones de muestra son generalmente diseñadas para demostrar la funcionalidad del ambiente de un servidor, no para resistir ataques, y no están planeadas para que sirvan como aplicaciones de producción. El problema es que su localización por default es conocida y su código fuente disponible a escrutinio, esto las hace blancos de intentos de explotación. Las consecuencias pueden ser severas: Una aplicación de muestra, tal como **newdsn.exe**, le permite a un atacante remoto crear o sobrescribir archivos en el servidor.

Para estar protegido contra esta vulnerabilidad se recomienda:

- Aplicar los parches informáticos más actuales. Para el caso de usar IIS 4 sobre NT4 con Service Pack 6, hay que aplicar un paquete de actualización de seguridad acumulada e individualmente un parche.
- Seguir estando pendiente de nuevas vulnerabilidades que aparezcan y de los correspondientes parches. HFNetChk (Network Security Hotfix Checker) es un programa que asiste al administrador del sistema y revisa sistemas locales y remotos para encontrar parches nuevos.

- Eliminar las aplicaciones de muestra. Las aplicaciones de muestra, incluyendo la herramienta **iisadmin** pueden ser usada para revisar que la instalación del servidor fue correcta, pero debe ser eliminada inmediatamente.
- Deshacer el mapa de extensiones ISAPI no necesarias. La mayoría de los desplegados IIS no tienen necesidad para la mayoría de las extensiones ISAPI que son mapeadas por default como **.htr, .idq, .ism** y **.printer**.

- Filtrar las peticiones http. Muchas explotaciones de IIS, incluyendo las de la familia de Code Blue y Code Red, utilizan peticiones http maliciosamente formadas en ataques de sobre flujo de buffer. El filtro URLScan puede ser configurado para rechazar tales peticiones antes de que el servidor intente procesarlas. Esta herramienta puede ser descargada del sitio de Microsoft.

Acceso de Usuarios Anónimo. Una conexión de sesión nula, también conocida como Acceso de Usuario Anónimo, es un mecanismo que permite a un usuario anónimo extraer información (como nombres de usuario y compartidos) por medio de la red, o conectarse sin autenticación. Es utilizado por aplicaciones como el Explorador de Windows.

La cuenta del sistema tiene privilegios virtualmente ilimitados y sin password, de manera que no puedes acceder haciéndote pasar por usuario. Pero el sistema a veces necesita acceder información en otras máquinas, tales como compartidos disponibles, nombres de usuarios, etc. Es decir las clásicas funcionalidades ofrecidas por el entorno de red. El problema en sí, es que la web no accesa a otros sistemas usando una cuenta de usuario y password, sino que usa una sesión nula. Desafortunadamente los atacantes pueden también ingresar en forma de una sesión nula.

Se puede modificar el registro, pero puede causar que el sistema deje de trabajar correctamente, pero ello puede afectar la sincronización del dominio u otros servicios, por ello mismo se recomienda que solo aquellos con acceso a la web tengan configurado este valor. Todas las otras máquinas deben ser protegidas con un firewall configurado para bloquear el acceso de otras redes que desean accesar a esta para vaciar los datos que ahí se contengan

CONCLUSIONES

La seguridad en Internet siempre ha sido una de las principales preocupaciones para todos aquellos que están conscientes de los peligros que puede ocasionar una intrusión de alguien no deseado en nuestra propia computadora o en los archivos más secretos. Como hemos visto no solo debemos de cuidarnos de aquellos quienes están fuera de nuestra casa u oficina sino también de quienes son compañeros de trabajo. La información es una posesión muy valiosa, no debemos de dejar que alguien husmee sin consentimiento.

Esta no es una acción fácil ya que siempre habrá gente que tome como reto el acceder de manera ilegal a cualquier sistema o archivo que esta conectado a Internet. Muchas de estas personas tienen la firme creencia de que están haciendo algo bueno al mostrar las fallas en los sistemas de seguridad, ya que ellos no hacen ningún daño a los archivos personales. Sin embargo hay quienes no tienen buenas intenciones y se la pasan explorando las posibilidades de observar o modificar información ajena. Se podría decir que esta es una característica típica del hombre ya que siempre le gusta tomar lo que esta prohibido y aun en el ambiente electrónico esto se aplica porque siempre se están buscando maneras de romper las modernas protecciones a la información.

Los clásicos sistemas de seguridad como la encripción, antivirus y firewalls son los mas útiles para tener una buena privacidad en la transferencia de los datos, sin embargo no son perfectos, los piratas siempre encuentran puertas traseras y formas de entrar. Aun existe mucha investigación para mantener la información segura, algunos trabajos se orientan en que se puedan hacer cada vez mas modificaciones a los algoritmos de encripción y a las funciones para que resistan los ataques más usuales, evitando así, que haya incursiones y protegiéndonos de robos de archivos.

Con la realización de este proyecto se presento una visión sobre los protocolos de seguridad en Internet y los niveles o capas en que trabajan ellos.

Glosario

Exposición: Es una forma de posible pérdida o daño en un sistema computacional, por ejemplo el acceso no autorizado de información, la modificación de información, o la negación de acceso a un servicio.

Vulnerabilidad: Es una debilidad en el sistema que puede ser explotada para causar pérdida o daño. Si una persona explota una vulnerabilidad se está perpetrando un ataque al sistema.

Amenazas: Son circunstancias que tienen el potencial de causar pérdida o daño, los ataques humanos son ejemplos de amenaza, al igual que los desastres naturales, errores inadvertidos, etc.

Control: Es una medida de protección que reduce una vulnerabilidad.

Amenazas contra Hardware: Estos se refieren a ataques físicos contra el equipo de cómputo, tal como prenderles fuego, lanzarles agua, roedores, llaves y desarmadores que causan corto circuitos.

Amenazas contra Software: El software puede ser destruido maliciosamente, modificado, borrado o colocado erróneamente. Estos errores se presentan cuando uno trata de acceder al software.

Amenazas contra Datos: Los datos son especialmente vulnerables a la modificación. Ya que si está es hecha de manera habilidosa no será detectada.

Confidencialidad. Nos asegura que la información en un sistema de computadora y la información transmitida sean accesibles solo por las partes autorizadas para la lectura. Este tipo de acceso incluye la impresión, desplegado, y otras formas de liberación, incluyendo la simple revelación de existencia de un objeto.

Autenticación. Nos asegura que el origen de un mensaje o de un documento electrónico es correctamente identificado, y de que no se trata de una identidad falsa.

Integridad. Nos asegura que solo los equipos o usuarios autorizados serán capaces de modificar las capacidades de los sistemas de computadoras y de la transmisión de información. La modificación incluye escritura, cambios, status del cambio, borrado, y retraso o revisión de los mensajes transmitidos.

No-repudio. Requiere que ni la persona que envía el mensaje ni el receptor sea capaz de negar la transmisión.

Control de acceso. Requiere que el acceso a las fuentes de información sea controlado por el sistema objetivo.

Disponibilidad. Requiere que las capacidades del sistema de computadora estén disponibles a los equipos autorizados cuando se les necesite.

Bibliografía

[1].EMILIO DEL PESO Navarro
Servicios de la sociedad de la información: Comercio electrónico y protección de datos
Editorial. Días de Santos - Social Science – 2003 - 422 páginas

*[2].*SCHNEIDER Gary P.
Comercio ELECTRONICO- 3era: Edición
Editorial. Computers - 2004

[3].OELKERS
Comercio electrónico- Serie Bussines.
Editorial. Computers – 2004

[4].RINCÓN CÁRDENAS Erick
Manual de derecho de comercio electrónico y de Internet
2006 - 500 páginas

[5].ESPAÑA BOQUERA María Carmen
Servicios avanzados de telecomunicación
Ed: Díaz de Santos- Technology – 2003 - 816 páginas

[6].ALONSO Rafael
Confianza y seguridad en comercio electrónico
2001 - 133 páginas

[7].RIVAS PÉREZ Gabriel, RICOTTA Adrien
Seguridad en el comercio electrónico
2007 - 52 páginas

[8].ADAM Olaf
Seguridad en Internet
Computers, 2006

[9].HUIDOBRO MOYA José Manuel, ROLDÁN MARTÍNEZ David
La tecnología e-business
2005

[10]. HUIDOBRO MOYA José Manuel -
Redes Y Servicios de Comunicaciones
Technology - 2006