UNIVERSIDAD DE SOTAVENTO A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

“EVOLUCIÓN DE LAS TELECOMUNICACIONES VÍA I.P. COMO UN MEDIO ECONÓMICO DE COMUNICACIÓN EN LAS EMPRESAS.”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

JOSÉ ANTONIO FORTUNA MORALES

ASESOR DE TESIS:
LIC. EMILIO DE JESÚS ESPRONCEDA GONZÁLEZ

COATZACOALCOS, VER. **FEBRERO 2008**

ÍNDICE DE CONTENIDO

INTRODUCCION

La utilización creciente de la tecnología de la información en virtualmente todos los ámbitos de la actividad económica, pública o privada, parece mostrar que es merecedora de confianza.

Basta la experiencia común para percibir la dependencia de las organizaciones (y la sociedad en su conjunto) de una tecnología que se ha desarrollado en cinco décadas a un ritmo desconocido en la historia de las invenciones. A su vez ha influido en la innovación de los campos del saber a los que se ha aplicado.

Desde el principio la información debía tener las siguientes características:

- Privacidad
- Autenticidad
- Disponibilidad
- Integridad

No mucho tiempo atrás (los ‘60s), el control de acceso a los datos, era satisfactoriamente llevado a cabo por el Mainframe, que centralizaba las invocaciones y el control de acceso, garantizando así la seguridad necesaria para que los datos tuvieran las características deseadas. Los computadores y la seguridad de datos han evolucionado con la tecnología, pero el objetivo es básicamente el mismo.

En los ‘70s, surge ARPAnet, que interconectaba departamentos de investigación de varias universidades y diversas oficinas gubernamentales de defensa de los EE.UU., hasta ese momento los usuarios conectados tanto a los mainframes como a esta red, eran una audiencia selecta cuyos límites eran bien conocidos.

En los ‘80s, junto con la era de las PC’s, los sistemas distribuídos y las redes, aparecen los virus. Luego con el uso de Internet, las redes corporativas y los servidores son susceptibles de ser víctimas de diferentes amenazas.

Siguiendo a Castells, la infraestructura de la vida cotidiana se ha vuelto tan compleja y está tan entrelazada que su vulnerabilidad ha aumentado de forma exponencial.

Aunque las nuevas tecnologías mejoran los sistemas de seguridad, también hacen la vida diaria más vulnerable. El precio por aumentar la protección será vivir en un sistema de cerrojos electrónicos, sistemas de alarma y patrullas de policía en línea telefónica1.

Tampoco es infrecuente encontrar recelos; por ejemplo cuando al público se le plantea la cuestión de si es sensato confiar en las computadoras; ciertamente fundados, a juzgar por las noticias que con creciente asiduidad aparecen en los medios de comunicación.

La dependencia respecto de la Tecnología de la Información, y la necesidad de un desarrollo sostenido de la Sociedad de la Información reclaman establecer fundamentos sólidos de confianza. Lo que significa aplicar salvaguardas o defensas (técnicas y administrativas) para controlar el riesgo; así como disponer de legislación que sirva para marcar las reglas de juego, dirimir las discrepancias y castigar el delito. Se trata de actuaciones complejas en sí mismas y en sus relaciones, pero ya no es admisible demora en su establecimiento. Solo así se pueden aprovechar con tranquilidad los recursos y las oportunidades que la Sociedad de la información ofrece a las relaciones económicas o personales.

Los profesionales de la informática que se ocupan de la seguridad alertan acerca de riesgos que pudieran no estar controlados; y también desde el ámbito político,

el objetivo es garantizar la seguridad, esto es la seguridad como medio de ganar la confianza.

Es cierto que la generación y la permanencia de la confianza es un fenómeno complejo, que tiene que ver mas con la percepción del usuario de la seguridad que con la protección rigurosamente demostrable.

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

Actualmente existe mayor facilidad para realizar un ataque al disponer de tecnología mas sofisticada, asimismo la tecnología nos brinda herramientas para hacer frente a estas amenazas, controlar los riesgos y conseguir que la información, el activo más valioso de la Sociedad de la Información posea lo que se buscó desde el principio:

- Privacidad
- Autenticidad
- Disponibilidad
- Integridad

CAPÍTULO 1

1. DEFINICIÓN DEL PROBLEMA

1.1 Presentación Del Problema

Internet ha iniciado una revolución tanto o más grande que la industrial y no podemos sustraernos a los cambios que ha originado, sobre todo en la forma de hacer negocios. Sin embargo, en nuestro medio, los usuarios finales no disponen de información clara de como involucrarse en esta revolución de manera segura.

No se dispone de una guía para la selección de una solución de seguridad.

El usuario final en nuestro medio no dispone de información del entorno que gira alrededor del tema de comercio electrónico, ni tampoco de criterios para decidir cuando debe aplicar seguridad del tipo de firmas digitales, u otros tipos de seguridad.

1.2 Propósito Del Estudio

Establecer los pasos necesarios para la implementación de un sitio seguro de e-commerce, todo ello bajo el marco legislativo de nuestro país y las normas y recomendaciones internacionales en las que se basa dicha legislación.

Asimismo, presentar los elementos involucrados en el tema de comercio electrónico.

CAPITULO 2

2.1 SEGURIDAD

2.1.1 Seguridad 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 aseguren que sólo podrán tener acceso a los datos las personas o sistemas de información autorizados para hacerlo.

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 sido transmitida.
6. Se debe disponer de sistemas alternativos de transmisión de información entre diferentes puntos.

2.1.1.1 Controles de Acceso

Los controles de acceso pueden implementarse a nivel de Sistema Operativo, de sistemas de información, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Estos controles constituyen una ayuda importante para proteger al sistema operativo de la red, a los sistemas de información y software adicional; de que puedan ser utilizadas(os) o modificadas(os) sin autorización; también para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con autorización de acceso) 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 son planteadas por el National Institute for Standards and Technology (NIST) en el NIST Handbook1; donde se encuentran resumidos los siguientes esquemas para dotar de seguridad a cualquier sistema:

Identificación y Autentificación

Se constituye en la primera línea de defensa para la mayoría de los sistemas computarizados, al prevenir el ingreso de personas no autorizadas y es la base para casi todos los controles de acceso, además permite efectuar un seguimiento de las actividades de los usuarios. **Identificación** es cuando el usuario se da a conocer en el sistema; y **Autentificación** es la verificación que realiza el sistema de la identificación.

Roles

El acceso a la información puede ser controlado también, considerando la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes:

- Líder de proyecto,
- Programador
- Operador
- Jefe de un área usuaria
- Etc.

Los derechos de acceso se agrupan de acuerdo con un rol determinado y el uso de los recursos se restringe a las personas autorizadas a asumir dicho rol, cambiar de rol implicaría salir del sistema y reingresar.

El uso de roles es una manera bastante efectiva de implementar el control de accesos, siempre que el proceso de definición de roles esté basado en un profundo análisis de cómo la organización opera. Es importante aclarar que el uso de roles ***no*** es lo mismo que el uso compartido de cuentas.

Transacciones

Otro planteamiento para implementar controles de acceso en una organización son las transacciones, sería del modo siguiente: el computador conoce de antemano el número de cuenta que proporciona a un usuario el acceso a la cuenta respectiva, este acceso tiene la duración de una transacción, cuando esta es completada entonces la autorización de acceso termina, esto significa que el usuario no tiene mas oportunidad de operar.

Limitaciones a los Servicios

Las Limitaciones a los Servicios son controles que se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o que han sido preestablecidos por el administrador del sistema. Un ejemplo se este tipo de control es: cuando en un cajero automático establece un límite para la cantidad de dinero que se puede transferir de una cuenta a otra, y también para los retiros.

Otro ejemplo podría ser cuando los usuarios de una red, tienen permitido intercambiar e-mails entre sí, pero no tienen permitido conectarse para intercambiar e-mails con usuarios de redes externas.

Modalidad de Acceso

Adicionalmente a considerar *cuando* un acceso puede permitirse, se debe tener en cuenta también *que tipo de acceso* o *modo de acceso* se permitirá. El concepto de modo de acceso es fundamental para el control respectivo, los modos de acceso que pueden ser usados son:

- Lectura
- Escritura
- Ejecución
- Borrado

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación
- Búsqueda

Estos criterios pueden ser usados de manera conjunta con otros, por ejemplo, una organización puede proporcionar a un grupo de usuarios acceso de Escritura en una aplicación en cualquier momento dentro del horario de oficina, y acceso sólo de Lectura fuera de él.

Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto al horario, el uso de parámetros como *horario de oficina* o *día de semana* son comunes cuando se implementan este tipo de controles, que permiten limitar el acceso de los usuarios a determinadas horas.

Control de Acceso Interno

Los controles de acceso interno determinan lo que un usuario (o grupo de usuarios) puede o no hacer con los recursos del sistema. Se detallarán cinco métodos de control de acceso interno:

Palabras Clave (Passwords)

Las palabras clave o passwords, están comúnmente asociadas con la autentificación del usuario, pero también son usadas para proteger datos, aplicaciones e incluso PC's. Por ejemplo, una aplicación de contabilidad puede solicitar al usuario un password, en caso de que aquel desee acceder a cierta información financiera.

Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo e incluyen una gran variedad de aplicaciones.

Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La criptología es un tema cuya amplitud será tratada en un subcapítulo aparte.

Listas de Control de Accesos

Estas listas se refieren a un registro de:

- Usuarios (incluye grupos de usuarios, computadoras, procesos), a quienes se les ha proporcionado autorización para usar un recurso del sistema.
- Los tipos de acceso que han sido proporcionados.

Hay una gran flexibilidad para el manejo de estas listas, pueden definir también a que usuario o grupos de usuarios se les niega específicamente el acceso a un recurso. Se pueden implementar Listas de Control de Accesos Elementales y Avanzadas.

Límites sobre la Interfase de Usuario

Comúnmente utilizados en conjunto con listas de control de accesos, estos límites restringen a los usuarios a funciones específicas. Pueden ser de tres tipos:

- Menús
- Vistas sobre la Base de Datos
- Límites físicos sobre la interfase de usuario.

Los límites sobre la interfase de usuario pueden proporcionar una forma de control de acceso muy parecida a la forma en que la organización opera, es decir, el

Administrador del Sistema restringe al usuario a ciertos comandos, generalmente a través de un menú.

Las vistas sobre la Base de datos, limitan el acceso de los usuarios a los datos contenidos en la BD, de tal forma que los usuarios dispongan sólo de aquellos que puedan requerir para cumplir con sus funciones en la organización.

Un ejemplo de los límites físicos sobre la interfase de usuario se da en un cajero automático, que proporciona un número determinado de botones para seleccionar opciones.

Etiquetas de Seguridad

Las Etiquetas de Seguridad son denominaciones que se dan a los recursos (puede ser un archivo), las etiquetas pueden utilizarse para varios propósitos, por ejemplo: control de accesos, especificación de pruebas de protección, etc.

En muchas implementaciones, una vez que la denominación ha sido hecha, ya no puede ser cambiada, excepto, quizás, bajo cuidadosas condiciones de control, que están sujetas a auditoría. Las etiquetas de seguridad son una forma muy efectiva de control de acceso, pero a veces resultan inflexibles y pueden ser costosas de administrar, y estos factores pueden desanimar en su uso.

Control de Acceso Externo

Los controles de acceso externo son una protección contra la interacción de nuestro sistema con los sistemas, servicios y gente externa a la organización.

Dispositivos de control de puertos

Estos dispositivos autorizan el acceso a un puerto determinado del computador host y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem. Los dispositivos de control de puertos actúan de manera previa e independiente de las funciones de control de acceso propias del computador y comúnmente son usados en comunicaciones seriales.

Se verá mas detalles sobre este punto en el sub capítulo sobre Seguridad en Infraestructura.

Firewalls o Puertas de Seguridad

Los firewalls permiten bloquear o filtrar el acceso entre 2 redes, generalmente una privada y otra externa (por ejemplo Internet), entendiendo como red privada una 'separada' de otras.

Las puertas de seguridad permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización, adicionalmente a estos beneficios los firewalls reducen la carga del sistema en procesos de seguridad y facilitan la centralización de servicios.

Este tema será abordado en el sub capítulo sobre Seguridad en Infraestructura.

Autenticación Basada en el Host

La autenticación basada en Host, proporciona el acceso según la identificación del Host en el que se origina el requerimiento de acceso, en lugar de hacerlo según la identificación del usuario solicitante.

2.1.2 Seguridad Organizacional/Operacional

Actualmente es claro que las organizaciones son cada vez mas dependientes de sus recursos informáticos, y vemos también que a la par de ello las organizaciones diariamente enfrentan una serie de amenazas que de concretarse afectarían dichos recursos. 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.

En este capítulo revisaremos las siguientes áreas de interés:

- Recuperación de Desastres
- Seguridad Física
- Forénsica
- Educación y Documentación

2.1.2.1 Recuperación de Desastres

La recuperación de desastres es esencial para asegurar, que los recursos informáticos críticos para la operación del negocio, estén disponibles cuando se necesiten, pues esto garantiza la continuidad del negocio. Es muy importante ser conscientes de que independientemente de que nuestra empresa esté altamente asegurada contra ataques de hackers, o infección de virus, etc.; la seguridad de la misma será prácticamente nula si no se ha previsto como combatir un incendio, o si no se ha previsto la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo en la misma.

Por eso en esta parte veremos aspectos de seguridad que van mas allá del hardware y del software.

Tipos de Desastre

Las principales amenazas que se prevén son:

- Desastres naturales
- Desastres causados por el hombre

Desastres naturales

Son eventos generados por procesos dinámicos en el interior de la tierra, estos eventos son de manifestación espectacular y constituyen muestras de la energía interna de la tierra. Los desastres naturales que se pueden producir en nuestro país son:

- Sismos
- Maremoto
- Inundaciones
- Actividad volcánica

Para los fines del presente estudio analizaremos los tres primeros.

Sismos

Este fenómeno se manifiesta como el repentino movimiento o vibración de una parte de la corteza terrestre, causado por la presencia de ciertas fuerzas, como las producidas por la tectónica de placas, o la ruptura gradual de la corteza ocasionada por el plegamiento o desplazamiento de materiales (fallas geológicas), o por el proceso de erupción volcánica. Un sismo es la liberación de energía de la corteza terrestre, acumulada por tensiones internas.

En el caso de los desastres naturales la prevención es la mejor norma, y de las precauciones tomadas depende el porcentaje de recuperación que se pueda obtener. Las medidas de protección, para el caso de sismos, recomendadas por el INDECI, son:

- Verificar si el inmueble donde se instalarán los equipos, cumple con normas de diseño y construcción sismo resistente propios de la zona, en suelo y lugar adecuados.
- Los suelos de peor calidad son los de sedimentos, como lodo, arena o saturados de humedad, siendo los mejores los de roca buena o poco deteriorada.
- Organizarse y delegar responsabilidades para la evacuación, prepare y/o conozca su plan de protección y aplíquelo.
- Identificar las áreas que ofrecen mayor seguridad para ubicar los equipos (intersección de columnas con vigas, por ejemplo), zonas de peligro y rutas de evacuación directas y seguras.
- Las puertas y ventanas deben abrirse fácilmente (es preferible que las puertas se abran hacia afuera) para evitar que se traben.
- Las ventanas grandes de vidrio deben tener cintas adhesivas en forma de aspa, para evitar esquirlas en la ruptura.
- Los ambientes y rutas de evacuación deben estar libres de objetos que retarden la evacuación. No colocar objetos pesados o frágiles en lugares altos, sin la máxima seguridad.
- Conocer la ubicación y saber desactivar las llaves generales de luz, agua y gas.
- Realizar simulacros frecuentes de evacuación

Maremotos

Son fenómenos marítimos que consisten en una sucesión de olas que pueden alcanzar grandes alturas: unos 30 metros en litorales con contornos y batimetría desfavorables, este fenómeno es causado por sismos de origen tectónico, por grandes erupciones de Islas Volcánicas o por derrumbes marinos o superficiales.

En alta mar la altura de ola es apenas de unos decímetros y la separación entre cresta y cresta, llamada longitud de onda, puede tener varias decenas de kilómetros hasta aproximadamente 200 Km., y pasa sin ser percibida por los navegantes.

En alta mar, el maremoto es como un acordeón extendido, y se acerca a las costas como un acordeón cerrado.

Las medidas de Protección son dirigidas al personal, pues en una situación de esta naturaleza no hay mucho que hacer por los equipos:

- Conozca las zonas de seguridad establecidas y las rutas de evacuación, para lo cual debe hacer las consultas necesarias en la Oficina de Defensa Civil de su Municipalidad.
- Si el inmueble se encuentra cerca de la playa, evacúe hacia las zonas de seguridad después de que haya ocurrido un sismo de gran intensidad llevando su equipo de emergencia. Evacúe siguiendo las rutas de evacuación establecidas, asegúrese de que cada persona lleve únicamente *lo indispensable.*
- Recuerde que la aproximación de un Maremoto es precedida normalmente por un alza o baja (retirada) notable de las aguas en la costa.

Inundación

Invasión de aguas en áreas normalmente secas, debido a precipitaciones abundantes o ruptura de embalses o mareas altas, causando daños considerables. Las inundaciones pueden presentarse en forma lenta y gradual en los llanos y en forma súbita en regiones montañosas.

Medidas de Precaución:

- Ocupar zonas seguras, no riberas de los ríos, quebradas, planicies o valles tradicionalmente inundables.
- Conservar los bosques y vegetación existentes, evitando que se destruyan, ya que las plantas dan firmeza al suelo e impiden la erosión.
- Organizar y participar en trabajos de forestación o reforestación en las orillas de los ríos, incluyendo especies de rápido crecimiento que se extiendan por el suelo y den solidez a las riberas.
- Organizar trabajos de limpieza del cauce del río.
- Conservar limpio el cauce de los ríos, evitando el arrojo de basura o materiales que puedan generar represamiento.
- Conocer las rutas de evacuación y zonas de seguridad establecidas por el Comité de Defensa Civil de la localidad.

DESASTRES CAUSADOS POR EL HOMBRE

Explosiones

Una explosión es la liberación brusca de una gran cantidad de energía encerrada en un volumen relativamente pequeño que produce un incremento violento y rápido de la función, con desprendimiento de calor, luz y gases, se acompaña de estruendo y rotura violenta del recipiente en que está contenida. El origen de la energía puede ser térmica, química o nuclear.

Medidas de Prevención

- Vigilancia de personas extrañas con actitud sospechosa.
- Vigilar vehículos (carros, carretillas, triciclos, etc.) conducidos por personas con actitud sospechosa.
- Vigilancia de objetos y paquetes abandonados.
- Después de la explosión, si el inmueble ha sufrido serios daños, evacuarlo y no ocuparlo hasta que personal calificado realice una evaluación. Cerrar la llave de luz y de gas.

Inundaciones

Las inundaciones se definen como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, son ocasionadas por falta de drenaje ya sea natural o artificial. Además de las causas naturales de inundaciones vistas en el rubro anterior, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso del agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

Incendios

El uso inadecuado de combustibles, fallas en instalaciones eléctricas, instalaciones eléctricas defectuosas, el inadecuado almacenamiento y traslado de sustancias peligrosas, son las principales causas de los incendios.

El fuego es una de las principales amenazas contra la seguridad, es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información, los programas y los equipos.

Existen varias clases de fuego:

Clase “A”.- El fuego se origina en materiales sólidos como : telas, maderas, basura etc. y se apaga con agua o con un extintor de polvo químico seco ABC, espuma mecánica.
Clase “B”.- Se origina en líquidos inflamables como gasolina, petróleo, aceite, grasas, pinturas etc. y se apaga con espuma de bióxido de carbono (CO_2) o polvo químico seco, arena o tierra. No usar agua.
Clase “C”.- Se origina en equipos eléctricos y para apagarlo debe usarse el extintor de bióxido de carbono (CO_2) o polvo químico seco ABC, BC. No usar extintor de agua u otros que sean conductores de electricidad.
Clase “D”.- Se presenta en metales combustibles como aluminio, titanio y otros productos químicos. Usar extintores de tipo sofocantes, como los que producen espuma.”

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputo son:

- El inmueble en que se encuentren las computadoras, no debe ser combustible ni inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo hasta el techo.
- Debe construirse un 'falso piso' instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles.
- Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo del centro de cómputo y del lugar donde se almacenan los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de cómputo instalándolos en áreas que cuenten con los mecanismos de ventilación y detección de incendios adecuados. Como parte de su protección se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputo deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores)

El personal debe ser entrenado en el uso de los extintores de fuego, si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

Es recomendable implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger de un posible incendio que podría originarse en áreas adyacentes.

Acciones Hostiles

Los sistemas de TI son vulnerables a una serie de amenazas que pueden ocasionar daños que resulten en pérdidas 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 publicidad desfavorable para la organización, los efectos de las amenazas varían desde afectar la confidencialidad e integridad de los datos hasta afectar la disponibilidad del sistema. Algunas de las amenazas ya han sido vistas en rubros anteriores, ahora trataremos las siguientes:

- Robo y Fraude
- Espionaje
- Sabotaje
- Hackers y código maliciosos

Robo y Fraude

Los sistemas de TI pueden ser usados para estas acciones de manera tradicional o usando nuevos métodos, por ejemplo, un individuo puede usar el computador para sustraer pequeños montos de dinero de un gran número de cuentas financieras bajo la suposición de que pequeñas diferencias de saldo no serán investigadas, los sistemas financieros no son los únicos que están bajo riesgo, también lo están los sistemas que controlan el acceso a recursos de diversos tipos, como: sistemas de inventario, sistemas de calificaciones, de control de llamadas telefónicas, etc.

Los robos y fraudes usando sistemas de TI pueden ser cometidos por personas internas o externas a las organizaciones, estadísticamente los responsables de la mayoría de los fraudes son personas internas a la organización.

Adicionalmente al uso de TI para cometer fraudes y robos, el hardware y el software del computador también son vulnerables al robo, de la misma forma que lo son las piezas de stock y el dinero, también es necesario ser consciente de que para hablar de robo no es necesario que una computadora o una parte de ella sea sustraída, es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina, la información también es susceptible de ser sustraída pues puede ser fácilmente copiada, al igual que el software, del mismo modo las cintas y/o discos pueden ser copiados sin dejar rastro.

Cada año millones de dólares son sustraídos de empresas y en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines, ya sea para transferencias ilícitas de dinero, alteración de saldos de cuentas, eliminación de registros de deuda, u otras actividades similares, sin embargo, debido a que las partes implicadas (compañía, empleados, fabricantes,

auditores, etc.), en lugar de ganar, tienen mas que perder, ya sea en imagen o prestigio, no se da publicidad a este tipo de situaciones.

Sabotaje

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 puede ser un empleado o un sujeto ajeno a la empresa y sus motivos pueden ser de lo mas variados.

Al estar mas familiarizados con las aplicaciones, los empleados saben que acciones causarían mas daño, por otra parte el downsizing ha generado grupos de personas con conocimientos sobre diversas organizaciones y con conocimiento de acceso a sus sistemas. Entre las acciones de sabotaje mas comunes tenemos:

- Destrucción de hardware
- 'Bombas lógicas' para destrucción de programas y/o datos
- Ingreso erróneo de datos
- Exposición de medios magnéticos de almacenamiento de información a imanes
- Introducción de suciedad, partículas de metal o gasolina por los conductos de aire acondicionado.
- Corte de las líneas de comunicaciones y/o eléctricas

Espionaje

Se refiere a la acción de recolectar información propiedad de una compañía para ayudar a otra compañía. Desde que la información es procesada y almacenada en computadoras, 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 a información pueda entregarla o venderla.

Hackers y Código Maliciosos

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 para no pagar las llamadas que hacen son los 'phreakers'

El código malicioso se refiere a los virus, worms, caballos de troya, bombas lógicas y otros ejemplos de software 'no deseado' que son introducidos en los sistemas, detallaremos a continuación la definición de algunos de estos términos:

Virus: Segmento de código que se replica adjuntando copias de sí mismo a los ejecutable existentes, la nueva copia del virus se ejecuta cuando un usuario ejecuta el programa host, o cuando ciertas condiciones, especificadas como parte del virus, se presentan.

Caballo de troya (Trojan Horse): Es un programa que ejecuta una tarea deseada, pero que adicionalmente realiza funciones inesperadas e indeseadas.

*Wor*m: Es un programa que se autoreplica y no requiere un ejecutable que le sirva de host, el programa crea una copia de sí mismo y la ejecuta sin intervención del usuario, los worms comúnmente usan los servicios de red para propagarse.

2.1.2.2 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 objetivo es prevenir, detectar y detener las rupturas 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 definido 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, entre los 10 controles mencionados se encuentran aquellos orientados a garantizar la Seguridad Física y del entorno.

Los controles de Seguridad Física manejan los riesgos inherentes a las instalaciones de las empresas, e incluyen:

- ***Ubicación.-*** Se deben analizar las instalaciones de la organización, considerando la posibilidad de un desastre natural.
- ***Seguridad del perímetro físico.-*** El perímetro de seguridad de las instalaciones debe estar claramente definido y físicamente en buen estado,

las instalaciones pueden dividirse en zonas, basándose en niveles de clasificación u otros requerimientos de la organización.

- ***Control de Accesos* –** Las aperturas en el perímetro de seguridad de las instalaciones deben contar con controles de ingreso/salida proporcionales con el nivel de clasificación de la zona a la que afecta.
- ***Equipamiento* –** Los equipos deben estar situados en una zona de las instalaciones que asegure, físicamente y en su entorno, su integridad y disponibilidad.
- ***Transporte de bienes* –** Mecanismos para el ingreso o salida de bienes a través del perímetro de seguridad.
- ***Generales* –** Políticas y estándares, como la utilización de equipos de destrucción de documentos, almacenamiento seguro y regla de 'escritorio limpio', deben existir para administrar la seguridad operacional en el espacio de trabajo.

Controles de Seguridad Física y de entorno. NIST

Según el planteamiento del NIST los controles de seguridad física y del entorno se implementan para proteger los ambientes en que se encuentran los recursos del sistema, los recursos del sistema 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 los 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 de TI
- Daño físico
- Divulgación no autorizada de información
- Pérdida de control de la integridad del sistema
- Robo físico

Analizaremos brevemente los siguientes controles operacionales de seguridad física y del entorno:

- Control de Acceso físico
- Fallas en servicios accesorios
- Interceptación de datos
- Sistemas Móviles y portátiles

Control de Acceso Físico

Los controles de acceso físico restringen 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 encuentra el hardware del sistema, sino también a las zonas del cableado necesario para conectar los elementos del sistema, de energía eléctrica, aire acondicionado o calefacción, líneas telefónicas, dispositivos de backup, 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.

Se debe considerar la posibilidad del ingreso subrepticio de un intruso, por ejemplo por el techo o por una abertura en la pared que puede ser cubierta con el mobiliario, si una puerta es controlada por una cerradura con combinación, el intruso puede observar a una persona autorizada introducir la clave, si las ‘tarjetas llave’ no son controladas cuidadosamente, el intruso puede robar una o usar la de un cómplice, todas estas posibilidades dan paso a medidas correctivas enfocadas.

Fallas en servicios accesorios

Los sistemas de TI y las personas que los operan requieren un ambiente de trabajo razonablemente bajo control, en estos ambientes usualmente se utilizan equipos de servicios accesorios como por ejemplo los de aire acondicionado que cuando fallan ocasionan una interrupción del servicio y pueden dañar el hardware.

Los equipos de servicios accesorios tienen diversos elementos, cada uno de ellos tiene un Tiempo entre fallas *(mean-time-between-failures MTBF)* y un Tiempo de reparación *(mean-time-to-repair MTTR)* , el riesgo de fallas se puede reducir adquiriendo equipos con valores MTBF bajos y el MTTR se puede reducir manteniendo un stock de repuestos y personal entrenado en su mantenimiento, estas y otras estrategias se evaluarán comparando la reducción del riesgo con los costos de conseguirlo.

Interceptación de datos

Existen tres formas en que los datos pueden ser interceptados: observación directa, interceptación de la transmisión de datos e interceptación electromagnética.

- *Observación directa* .- en la mayoría de los casos es relativamente fácil reubicar la pantalla para eliminar la exposición de los datos a un observador no autorizado.
- *Interceptación de la transmisión de datos.*- si un interceptor logra el acceso a las líneas de transmisión, fácilmente tendrá acceso a los datos transmitidos, adicionalmente a ello puede transmitir data falsa con propósitos de fraude u otros.
- *Interceptación electromagnética.*- los sistemas generalmente irradian energía electromagnética que puede ser detectada por receptores de

propósito especial, en estos casos la distancia es determinante para que la intercepción sea exitosa, a menor distancia entre el sistema y el receptor mas posibilidad de éxito.

Sistemas móviles y portátiles

El análisis y el manejo de los riesgos debe ser modificado en sistemas de esta naturaleza, por ejemplo un sistema instalado en un vehículo o una laptop.

Estos sistemas comparten un riesgo mayor de robo y daño físico, inclusive de accidentes vehiculares, y si procesan datos particularmente importantes y/o valiosos, es apropiado almacenar los datos en un medio que pueda ser removido del sistema cuando éste se encuentra desatendido o encriptar los datos.

Control de Accesos

El control de acceso se refiere no solamente a la capacidad de identificación de la persona que solicita el acceso, sino también está asociado a la apertura o cierre de puertas, y también a conceder o negar acceso basándose en horarios, en áreas o sectores dentro de una empresa o institución.

Las formas de control de accesos que veremos a continuación son:

- Utilización de sistemas biométricos
- Verificación Automática de Firmas
- Protección Electrónica

Utilización de Sistemas Biométricos

La biometría se define como “la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos, utilizando métodos estadísticos”.

Los factores que son necesarios para que un sistema biométrico sea efectivo son:

- *Precisión*.- es la característica mas crítica de un sistema de identificación biométrica, el sistema debe ser capaz de separar de manera precisa a los impostores.
- *Velocidad*.- esta es una característica básica de los sistemas biométricos y está referida a la capacidad de proceso del sistema, es decir, a que tan rápido puede el sistema anunciar si acepta o rechaza el requerimiento de acceso, y esto debe ser el procedimiento de autenticación completo, que incluye la presentación del solicitante de acceso al sistema, el ingreso del dato físico, el procesamiento del dato, el anuncio de aceptación o rechazo de la solicitud y si el sistema es para una puerta, también se incluye el atravesar y cerrar la misma.
- *Aceptación de los usuarios*.- la aceptación de un sistema biométrico se da cuando aquellos que deben usar el sistema, administradores y personal, están todos de acuerdo en que hay recursos que necesitan protección, que los sistemas biométricos controlan efectivamente el acceso a estos recursos y que el sistema no producirá demoras en la producción ni impedirá el normal movimiento del personal.
- *Unicidad del órgano*.- puesto que el propósito de los sistemas biométricos es la identificación de personas, se espera que la característica física en la que se basan sea única, que no haya posibilidad de que se duplique en el mundo. Sólo 3 características de órganos humanos que se usan para identificación biométrica, son únicas: la huella digital, la retina del ojo y el iris del ojo.

- *Resistencia a los impostores*.- la habilidad del sistema para rechazar datos de impostores es vital, esto incluye el reconocimiento de elementos plásticos, o de goma o inclusive manos o dedos de personas fallecidas que puedan ser utilizados para lograr el acceso a los recursos protegidos.
- *Confiabilidad*.- se basa en la operación continua, rápida y precisa del sistema biométrico.
- *Requerimientos para almacenamiento de datos*.- no es un factor muy significativo, puesto que los medios de almacenamiento ya no son costosos.
- *Tiempo de ingreso.-* no es un factor muy significativo pero el estándar aceptado para la mayoría de sistemas en el mercado es de 2 minutos por persona.

Los diferentes tipos de sistemas biométricos y sus características se mencionarán a continuación.

Huella digital

Se basa en el principio de que no existen en el mundo dos huellas digitales iguales, cada huella posee arcos, ángulos, bucles, remolinos, etc., y cada una de estos rasgos (llamados minucias) tiene una posición relativa, todo ello es analizado para establecer la identificación de una persona. Cada persona posee más de 30 minucias y entre dos personas no hay más de 8 minucias iguales.

Geometría de la mano

Los datos geométricos de la mano constituyen un record tridimensional que incluye: la longitud, el ancho y el peso de la mano y de los dedos, estos datos son captados por la toma simultánea de cámaras verticales y horizontales.

Patrones de Voz

Hasta 7 parámetros de tonos nasales, vibraciones en la laringe y garganta, y presión de aire en la voz son capturadas por sensores de audio. Este sistema es muy sensible a factores externos como: ruido, estado de ánimo y/o de salud de la persona, envejecimiento, etc.

Patrones de Retina

El sistema trabaja en base a patrones de los vasos sanguíneos de la retina, en el área de la retina que se encuentra detrás del globo ocular.

Patrones de Iris

El iris, que es la porción alrededor de la pupila que da color al ojo, tiene un patrón único de estrías, puntos, filamentos, aros, vasos, etc. que permite la identificación efectiva de una persona.

Dinámica de firma

La velocidad de la firma, la dirección y la presión son captados por sensores, el proceso de escribir genera una secuencia sonora de emisión acústica, esto constituye un patrón que es único en cada individuo.

Emisión de Calor

Se basa en el termograma, que es la medición del calor que emana el cuerpo, realizando un mapa de valores sobre la forma de cada persona.

Protección Electrónica

Este tipo de protección hace uso de elementos sensores que detectan una situación de riesgo, la transmiten a una central de alarmas, ésta procesa la información que ha recibido y en respuesta emite señales alertando sobre la situación.

Barreras Infrarrojas y de microondas

Están compuestas por un transmisor y un receptor de haces de luces infrarrojas y de microondas respectivamente, la alarma se activa cuando el haz es interrumpido. Estas barreras pueden cubrir áreas de hasta 150 metros.

Los rayos se pueden reflejar usando espejos infrarrojos y así cubrir diferentes zonas con una misma barrera.

Como estos detectores no utilizan el aire como medio de propagación, no son afectados por sonidos fuertes o turbulencias de aire, también son inmunes a fenómenos aleatorios como movimientos de masas de aire, calefacción, luz ambiental etc.; otra ventaja es la capacidad de atravesar ciertos materiales como el vidrio, plástico, hormigón, mampostería, madera.

Detector de Ultrasonido

Este equipo crea un campo de ondas sobre el campo protegido utilizando ultrasonido, si un cuerpo cualquiera realiza un movimiento dentro de este campo generará una perturbación que activará la alarma. La cobertura de este sistema puede llegar a los 40 metros cuadrados.

Detectores pasivos sin alimentación

Estos detectores van conectados a la central de alarmas para enviar la información de control y no requieren alimentación extra de ninguna clase, dentro de este tipo de detectores tenemos:

- Detector de aberturas
- Detector de roturas de vidrios
- Detector de vibraciones

Circuito cerrado de televisión

Estos sistemas permiten controlar lo que ocurre en las instalaciones de la organización, según lo captado por las cámaras estratégicamente ubicadas, puede ser como elemento disuasivo, cuando se colocan a la vista o para evitar que un intruso se dé cuenta que está siendo captado por un elemento de seguridad, cuando se colocan ocultas.

Los monitores de estos circuitos deberán ubicarse en una zona de alta seguridad, y todos estos elementos deberán incluir algún control contra sabotaje, de tal forma que si se produce algún incidente contra algunos de sus componentes, éste enviará una señal a la central de alarma para tomar las medidas correspondientes.

Edificios inteligentes

Un edificio inteligente se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación, esto a través de la integración de la totalidad de los sistemas existentes en el inmueble, como por ejemplo teléfonos, seguridad, comunicaciones por computador, control de subsistemas (calefacción, aire acondicionado, entre otros) y todas las formas de administración de energía.

2.1.2.3 Forénsica

El término forénsica se refiere al examen sistemático o científico de evidencia durante la investigación de un crimen.

La computación forénsica involucra el examen metódico de todos y cada uno de los datos relevantes que pueden ser encontrados en un computador, en un intento de descubrir evidencia o recrear eventos; los datos son todo lo que está almacenado en dicho computador, como: cartas, e-mails, documentos, archivos de imágenes, logs de los firewalls, o routers, de los Sistemas de Detección de Intrusos, etc.

Las técnicas de la forénsica son empleadas frecuentemente en casos de delito informático, un caso típico es cuando la red ha sufrido un ataque y el equipo forense trata de determinar en que punto el hacker rompió la seguridad del sistema, si uno o mas computadores han sido comprometidos en el ataque y cual o cuales son; otro punto a determinar por el equipo forense es la actividad del hacker en el sistema, es básico identificar como ingresó y eliminar los Caballos de Troya (‘Trojan horses’), puertas traseras (‘Back doors’) u otros elementos que el hacker haya dejado. Todos los hallazgos del equipo forense deberán ser documentados de manera muy cuidadosa y precisa.

La documentación de los sucesos cobra mayor importancia, toda vez que, dependiendo de la legislación del país, ésta puede ser usada como evidencia para enjuiciar al hacker. Como un ejemplo de lo que un equipo forense puede hacer: durante la investigación al Presidente Clinton que realizó un Consejo Independiente, algunos de los e-mails que Mónica Lewinsky dirigió al presidente, fueron recuperados de su computadora, aún cuando habían sido eliminados.

La computación forénsica se aplica también para otros casos, por ejemplo cuando las organizaciones desean controlar el uso excesivo de internet, con los recursos de la empresa, por parte de los empleados, o el mal uso del mismo, como cuando visitan páginas pornográficas.

Cualquiera que sea el hecho que se investiga, la recolección de evidencia es fundamental para determinar la amplitud del hecho y al(los) culpable(s), las reglas básicas para esta recolección son: documentar todo lo que el investigador hace y asegurar que la evidencia en sí no se vea comprometida en ninguna forma, los pasos a seguir para la recolección de evidencia son:

- *Asegurar el área física.*- tomar fotografías de toda el área, equipos y conexiones e inventariar los documentos, discos y otros medios de almacenamiento de información.
- *Desactivar el sistema*.- **no** usar el teclado, y no efectuar un shut down del sistema operativo, pues esto puede ocasionar la activación de triggers o bombas lógicas que pueden destruir evidencia.
- *Asegurar el sistema.*- deberá ser sellada y etiquetada, en especial los floppy drive, el botón de encendido y todos los cables.
- *Preparar el sistema.*- desconectar los cables, previa toma de fotografías, retirar los cables de alimentación de los discos, iniciar el sistema e ingresar al menú de configuración.
- *Examinar el sistema.*- en el menú de configuración chequear y tomar nota de la fecha y hora del sistema.
- *Preparar el sistema para la recolección.*- cambiar la secuencia de inicialización, para cargar el sistema desde floppy, si es posible dejar esta opción de inicialización como única, si no lo es anteponer el floppy al disco duro.
- *Conectar un medio de almacenamiento*.- instalar un disco de destino que será configurado como Disco 1, el original será el Disco 2, asegurarse que el sistema los reconozca y que se siga inicializando el sistema desde floppy

con un diskette preparado por el equipo forense, apagar el sistema y reconectar los cables.

- *Copiar información.-* inicializar el sistema usando el diskette forense, copiar la información del disco original (Disco 2) al disco de destino (Disco 1), si es posible efectuar dos copias del disco original.
- *Asegurar la evidencia.-* retirar los discos del sistema y colocarlos en contenedores antiestáticos, sellarlos colocando en la etiqueta la fecha y firmando.
- *Examinar la evidencia.-* La forénsica es un herramienta vital para la respuesta a incidentes, provee evidencia concluyente y puede corroborar otras evidencias, pero es necesario tener en cuenta que es una disciplina a ser ejercida sólo por profesionales entrenados, pues aficionados o amateurs pueden causar daños irreparables a la evidencia.

2.1.2.4 Educación y Documentación

Educación

Los seres humanos somos falibles y somos probablemente el punto más débil en la seguridad de los sistemas, por ello el personal de una organización debe tener el conocimiento necesario para comprender el significado de sus acciones y evitar brechas en la seguridad, un programa que brinde este conocimiento tiene por objetivo:

- Dejar claro el porqué la seguridad es importante y los controles necesarios
- Definir claramente las responsabilidades de los empleados en la seguridad
- Servir como foro de discusión sobre las medidas de seguridad y las dudas al respecto

Respecto a los programas de este tipo, se pueden implementar en tres niveles.

Conocimiento

Entendemos este nivel como ‘dar a conocer’ la importancia de las prácticas de seguridad y las políticas de la organización al respecto. Es necesario que se tenga conciencia que actualmente en el ambiente de sistemas de TI, casi todos en la organización tienen acceso a estos recursos y por lo tanto pueden causar daño en ellos.

Este ‘dar a conocer’ enfatiza el hecho de que la seguridad da soporte a la misión de la organización al proteger los recursos valiosos y motiva a los empleados respecto a las políticas de seguridad, es común encontrar que éstos piensan que la seguridad es un obstáculo para la productividad y que su función es producir y no proteger, por eso esta motivación busca cambiar la actitud en las organizaciones dando a conocer a los empleados la importancia de la seguridad y las consecuencias de su falta.

Entrenamiento

El propósito del entrenamiento es enseñar al personal las habilidades necesarias para desarrollar sus labores de manera más segura, esto incluye el ***que*** hacer y ***como*** hacerlo. El entrenamiento es más efectivo cuando está enfocado a una audiencia específica, pues es distinto lo que se imparte a los usuarios en general de lo que es necesario dar a los ejecutivos o al personal técnico.

Educación

La educación en seguridad es algo mas profundo y está dirigido a profesionales del área o personas cuyo trabajo requiere especialización en seguridad.

La Educación en seguridad está más allá de los alcances de los programas de Conocimiento o Entrenamiento de las organizaciones.

Documentación

La documentación de todos los aspectos de operación y soporte de los computadores es importante para asegurar continuidad y consistencia. La seguridad de un sistema también debe ser documentada, esto incluye varios tipos de documentación, como:

- Planes de seguridad
- Planes de contingencia
- Análisis de riesgos
- Políticas y procedimientos de seguridad

La mayor parte de esta información, en especial el Análisis de riesgos debe estar protegido de acceso y difusión no autorizados.

La documentación de seguridad requiere estar actualizada y ser accesible, esta accesibilidad debe tener factores en cuenta, como por ejemplo: la necesidad de hallar fácilmente un Plan de Contingencia durante una situación de desastre, también es necesario que esta documentación esté diseñada para satisfacer las necesidades de los diferentes tipos de personas que van a utilizarla, por esta razón algunas organizaciones separan la documentación en:

- Políticas
- Procedimientos

Un manual de procedimientos de seguridad informa a los usuarios de diversos sistemas como realizar sus tareas de manera segura y un manual de procedimientos para operación de sistemas o personal de soporte proporciona directivas con un considerable detalle técnico.

2.1.3 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 del texto cifrado es igual al del texto original pero sólo es inteligible para las personas autorizadas. El proceso de transformación del criptograma en el texto original se llama desencriptado o descifrado.

El término Criptografía consta de los vocablos griegos *Cryto* : secreto y *grafos*: escritura. La criptografía es la rama del conocimiento que se encarga de la escritura secreta, también se puede definir como la ciencia y arte de escribir para que sea indescifrable el contenido del texto original para el que no posea la clave.

El Criptoanálisis es la ciencia que estudia los métodos para descubrir la clave, a partir de textos cifrados, o de inserción de textos cifrados falsos, válidos para el receptor.

La Criptología es el conocimiento que engloba la criptografía y el criptoanálisis y se define como la ciencia de la creación y ruptura de cifrados y códigos.

2.1.3.1 Cifrado Simétrico

La criptografía convencional es también llamada de clave secreta o privada, o sistema de cifrado simétrico. Su característica fundamental es que la misma clave que se utiliza para encriptar se usa también para desencriptar.

La mayoría de los algoritmos simétricos se apoyan en los conceptos de **Confusión y Difusión** vertidos por Claude Shannon sobre la Teoría de la Información a finales de los años cuarenta.

Estos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave (Confusión); y repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado (Difusión).

La criptografía simétrica se clasifica en dos familias:

- Criptografía simétrica de bloques
- Criptografía simétrica de lluvia o flujo

Criptografía simétrica por Bloques

En este tipo de criptografía, el mensaje se agrupa en bloques, antes de aplicar el algoritmo de cifra a cada bloque de forma independiente, con la misma clave.

Hay algunos algoritmos muy conocidos por su uso en aplicaciones bancarias (DES), correo electrónico (IDEA, CAST) y comercio electrónico (Triple DES).

No obstante, tienen tres puntos débiles:

a) Mala distribución de claves.- No existe posibilidad de enviar, de forma segura, una clave a través de un medio inseguro.
b) Mala gestión de claves.- Crece el número de claves secretas en un orden igual a n^2 para un valor 'n' grande de usuarios.
c) No tiene firma digital.- Aunque sí será posible autenticar el mensaje mediante una marca, no es posible firmar digitalmente el mensaje.

La gran ventaja del cifrado simétrico en bloque es que la velocidad de encriptación es muy alta y por ello se usará para realizar la función de cifrado de la información. Además, con claves de sólo unas centenas de bits obtendremos una alta

seguridad pues su no linealidad y algoritmo hace que el único ataque que puede prosperar es de el de la fuerza bruta, es decir, probando todas las claves posibles.

Respecto a los algoritmos de bloque disponibles tenemos lo siguiente.

A comienzos de los años 70, Horst Feistel creó el algoritmo LUCIFER, el mismo que fue utilizado por el Reino Unido, en 1974 se propone este algoritmo a la NSA como estándar y en ese mismo año dará origen al DES.

El DES (Data Encryption Standard) es el paradigma de los algoritmos de cifrado simétrico, estándar desde 1976, tiene como entrada un bloque de 64 bits del mensaje y lo somete a 16 interacciones, una clave de 56 bits, que en la práctica es de 64 bits (8 de paridad), el desencriptado se realiza mediante la misma clave que la de la codificación, pero invirtiendo el esquema de proceso.

Hoy es vulnerable por su longitud de clave.

Este algoritmo pasa la certificación de la NBS (National Bureau of Standards) en 1987 y en 1993, pero en 1997 el NIST (National Institute of Standards and Technology, antigua NBS) no certifica al DES y llama a concurso público para establecer un nuevo estándar, el AES (Advanced Encryption Standard).

En octubre del año 2000 el NIST elige el algoritmo belga RIJNDAEL como el nuevo estándar de algoritmos de cifra del siglo XXI, es decir el RIJNDAEL es el AES que el gobierno estadounidense a través de la convocatoria del NIST estuvo buscando. Es software de libre distribución y está disponible desde finales del año 2001.

Otros algoritmos de cifrado en bloque son:

Loki: algoritmo australiano similar al DES, tipo Feistel

RCX (X=2,4,5): algoritmo propuesto por Ron Rivest, el método no es público ni está patentado, es un secreto industrial. Cifra bloques de 64 bits con claves de longitud variable. El RC2 se usa es SMIME con longitudes de clave de 40, 64 y 128 bits. El RC4 está incorporado al Netscape Navigator.

CAST: algoritmo tipo Feistel que se ofrece como cifrador por defecto en últimas versiones de PGP, propuesto Por C. Adams y S. Tavares. Cifra bloques de texto de 64 bits con claves de 40 hasta 128 bits en incremento de octetos, 16 vueltas, usa 8 cajas S de 8 bits de entrada y 32 bits de salida con funciones no lineales óptimas (funciones Bent), 4 cajas en procesos de cifra y las otras 4 para generación de claves. Cada caja es un array de 32 columnas y 256 filas. Los 8 bits de entrada seleccionan una fila y los 32 bits de ésta son la salida. Operaciones básicas: suma y resta módulo 2^{32}, or exclusivo y rotaciones circulares hacia la izquierda.

Blowfish: algoritmo tipo Feistel propuesto por Bruce Schneier, cifra bloques de texto de 64 bits, tamaño de clave de 32 hasta 448 bits. Se generan 18 subclaves de 32 bits y cuatro cajas S de 8x32 bits, en total 4.168 bytes, 16 vueltas en cada una de las cuales hay cuatro cajas S con 256 entradas cada una, en cada vuelta se realiza un permutación y una sustitución que es función de la clave y los datos. Operaciones básicas: or exclusivo y suma módulo 2^{32}. Es bastante compacto, requiere sólo 5K de memoria y es 5 veces mas veloz que el DES, su fortaleza puede variar según la longitud de la clave.

IDEA: algoritmo europeo usado en el correo electrónico PGP, aunque ahora ya no es el que PGP usa por defecto puesto que requiere de licencia para ser usado comercialmente. Opera con bloques de 64 bits y claves de 128 bits. El cifrado

consiste en 8 vueltas elementales seguidas de una transformación de salida, es resistente al criptoanálisis y actualmente sólo se puede romper el algoritmo usando el método de fuerza bruta.

Skipjack: propuesta de nuevo estándar en USA a finales de los 90 para comunicaciones oficiales (tiene puerta trasera), ha sido desarrollado por la NSA (National Security Agency), está contenido en los chip Clipper y Capstone y su implementación está permitida sólo en hardware. Cifra bloques de 64 bits con una clave de 80 bits y usa 32 vueltas en cada bloque de cifra, pero los detalles del algoritmo no son públicos, los usuarios depositan sus claves secretas en diversas agencias de gobierno.

RIJNDAEL: algoritmo belga, nuevo estándar mundial desde finales de 2001. Sus autores son Vincent Rijmen y Joan Daemen. Usa tamaño de clave variable 128,192 y 256 bits (estándar) o bien múltiplo de 4 bytes, tamaño de bloque de texto 128 bits o múltiplo de 4 bytes, realiza operaciones modulares a nivel de byte y de palabra de 4 bytes.

TDES o Triple DES: Está basado en la utilización del DES en tres tiempos (encriptar-desencriptar-encriptar) con 3 claves diferentes.

Twofish: Propuesto por Bruce Schneier después de Blowfish, de tipo Feistel, diseño simple, sin claves débiles y multiplataforma, candidato a AES, lo encontraremos en últimas versiones del PGP.

Khufu: algoritmo propuesto por Ralph Merkle con una clave generada con un sistema de cajas S.

Khafre: algoritmo propuesto por Ralph Merkle en el que la clave ya no depende de las cajas S.

Gost: algoritmo similar al DES con cajas S secretas propuesto en la Unión Soviética. Cifra bloques de 64 bits con claves de 256 bits y tiene 32 vueltas.

SAFER (Secure and Fast Encryption Routine): algoritmo propuesto por James Massey. Existen dos variantes una utiliza una llave de 64 bits y la otra usa una de 128 bits, cada bloque de texto a cifrar se divide en 8 bytes, de 0 a 10 vueltas, el mínimo recomendable es 6; en cada vuelta hay operaciones or y sumas normales, potencias y logaritmos discretos. Al final del algoritmo hay tres niveles de operaciones lineales conocidas como Pseudo Transformaciones de Hadamard, cuyo objetivo es aumentar la difusión de los bits.

Akelarre: algoritmo español propuesto en 1996 por el CSIC, Consejo Superior de Investigaciones Científicas.

FEAL: algoritmo propuesto en Japón. En la figura II.1 se presenta un cuadro resumen de las características de los algoritmos enumerados.

Algoritmo	Bloque (bits)	Clave (bits)	Vueltas
Lucifer	128	128	16
DES	64	56	16
Loki	64	64	16
RC2	64	Variable	--
CAST	64	64	8
Blowfish	64	Variable	16
IDEA	64	128	8
Skipjack	64	80	32
RIJNDAEL	128	128 o más	Flexible
Twofish	128	Variable	Variable
Khufu	64	512	16, 24, 32
Khafre	64	128	
Gost	64	256	32
RC5	Variable	Variable	Variable
SAFER 64	64	64	8
Akelarre	Variable	Variable	Variable
FEAL	64	64	32

DES

DES (Data Encryption Standard) ha sido el estándar utilizado mundialmente durante 25 años, generalmente en la banca. Hoy presenta signos de envejecimiento y ha sucumbido a los diversos criptoanálisis que contra él se viene realizando hace ya años. Las especificaciones técnicas de DES son:

- Bloque a cifrar: 64 bits
- Clave: 8 bytes (con paridad, no caracteres ASCII)
- Normas ANSI:
  - –X3.92: Descripción del algoritmo.
  - –X3.108: Descripción de los modos de operación (ECB, CBC, OFB).

- Fácil implementación en un circuito integrado.
- La clave en sí son sólo 56 bits efectivos, puesto que al ser datos de 8 bits, se conoce el bit de paridad; por lo tanto el espacio de claves es: 256 = 7.2 · 1016, tan sólo 72 mil billones de valores.

Criptografía simétrica de Lluvia o Flujo

La criptografía simétrica de Flujo usa el concepto de cifra propuesto por Vernam, este concepto se basa e incluye las ideas que Shannon propone sobre sistemas de cifrado con clave secreta y que son:

- El espacio de claves es igual o mayor que el espacio de los mensajes
- Las claves deben ser equiprobables
- La secuencia de clave se usa una sola vez y luego se destruye (sistema *one-time pad*)

La pregunta es ¿se puede satisfacer la primera de las condiciones?, para ello se debería enviar al destinatario la secuencia de bits de la clave, a través de un canal probablemente inseguro, esta secuencia lo suficientemente larga para asegurar un espacio de claves mayor, 'desbordaría' el canal de comunicaciones.

La solución para evitar el 'desborde' es generar una secuencia pseudoaleatoria a partir de una "semilla" de sólo unas centenas de bits, esta semilla es la que se envía al receptor mediante un sistema de cifra de clave pública y un algoritmo de intercambio de clave, de esta manera no sobrecargamos el canal.

La técnica de cifrado de flujo determina que:

- El mensaje en claro se leerá bit a bit
- La función de cifra se basa normalmente en la función XOR
- La secuencia 'cifrante' se obtiene de una clave secreta K compartida por el emisor y el receptor.
- La función de descifrado se basa igualmente en la función XOR

Los sistemas mas conocidos de cifrado de Flujo son:

- *A5.*- Algoritmo no publicado propuesto en 1994. Usado en el cifrado del enlace entre el abonado y la central de un teléfono móvil (celular) tipo GSM.
- RC4.- Algoritmo de RSA Corp. (Rivest Cipher #4) desarrollado en el año 1987, usado en Lotus Notes y luego en el navegador de Netscape desde 1999. No es público.
- SEAL.- Algoritmo propuesto por IBM en 1994.

2.1.3.2 Cifrado Asimétrico

Ideado por los matemáticos Whitfiel Diffie y Martin Hellman (DH) con el informático Ralph Merkle a mediados de los 70, estos algoritmos han demostrado su seguridad en comunicaciones inseguras como Internet; su principal característica es que no se basa en una única clave sino en un par de ellas: una conocida o Pública y otra Privada, y busca resolver el problema de distribución de claves planteado en los criptosistemas simétricos.

Este tipo de cifrado utiliza una pareja de claves, tal como se ha mencionado líneas arriba, una de ellas para el cifrado y la otra para descifrado, en muchos casos estas claves son intercambiables y la condición es que el conocimiento de la clave pública no permita calcular la clave privada.

Los algoritmos de criptografía asimétrica están basados en un problema matemático denominado NP, este problema se basa en la imposibilidad computacional de factorizar un número que se ha obtenido del producto de dos números primos, cuando éstos últimos tienen una longitud superior a los cien dígitos.

Se enumera a continuación las características de un criptosistema de clave pública:

- Conocer Ek no revela ningún dato acerca de Dk o viceversa
- La clave pública no permite que la otra pueda ser deducida
- Cada usuario dispone del par (Ek, Dk), donde Ek es pública y Dk es privada
- El mensaje cifrado se obtiene de la siguiente manera : cA= {EB (mA)}, donde A es el emisor y B el receptor.
- El mensaje original se obtiene o descifra : mA= DB{ EB (mA)}
- Se verifica además: mA= EB{ DB (mA)}

Como se puede ver el hecho de usar parejas de claves permite que para enviar un mensaje confidencial a un destinatario, basta cifrar dicho mensaje con la clave pública de ese destinatario, de esa forma sólo él podrá descifrarlo haciendo uso de su clave privada, no es necesario un intercambio previo de claves entre emisor y destinatario, el emisor sólo requiere la clave pública del destinatario. Asimismo cada usuario puede cifrar un mensaje con su clave privada de tal forma que otro pueda descifrarlo con su clave pública, de esta manera se implementa la Firma Digital.

Para evitar suplantaciones de identidad, se requiere contar con una tercera parte de confianza que acredite cual es la clave pública de una persona o entidad, esta es la función de las Autoridades de Certificación.

Los algoritmos de cifrado asimétrico son:

- *RSA*.- Creado por *Ron Rives, Adi Shamir y Leonard Adleman*., su característica principal es que sus claves pública y privada se calculan en base a un número obtenido como producto de 2 números primos grandes. Podemos ver el algoritmo en http://rsasecurity.com
- *El Gamal*.- Basado en el problema del Logaritmo discreto, es mas lento para encriptar y verificar que el RSA. Fue creado por Taher ElGamal en 1985.
- *DSA*.- *(Digital Signature Algorithm)*, creado por David Kravitz.
- Existen criptosistemas basados en operaciones matemáticas sobre curvas elípticas y otros basados en la exponenciación discreta en los campos finitos de Galois
- Existen también algunos métodos de encriptación probabilística que tienen la ventaja de ser resistentes al criptoanálisis pero tienen el coste de la expansión de los datos

2.1.3.3 Criptografía de Resumen

En los sistemas de cómputo no siempre es posible 'rastrear' la información para determinar si ha sido modificada, borrada o añadida, en caso de ser posible este rastreo no siempre se puede saber si la información es la correcta, por ejemplo 1,000 puede ser cambiado a 10,000, es pues deseable poder detectar los cambios, intencionales o no, de los datos.

La criptografía puede detectar las modificaciones intencionales o no, pero no puede proteger los datos de ser modificados.

Tanto la criptografía de clave pública como la de clave privada pueden ser usadas para asegurar integridad, aunque algunos métodos de clave pública pueden ofrecer mayor flexibilidad que los de clave privada, los sistemas de verificación de

integridad de clave privada han sido integrados a diversas aplicaciones de manera satisfactoria.

Cuando se usa criptografía de clave privada, se calcula un código de autenticación de mensaje, (***MAC,*** *Message Authentication Code)* a partir de los datos y se anexa a ellos, luego se puede verificar que los datos no han sido cambiados cuando alguien con acceso a la clave puede recalcular el MAC y compararlo con el original, si son idénticos entonces la confidencialidad e integridad no han sido alteradas.

Adicionalmente a las protecciones expuestas, la criptografía proporciona una manera de asociar un documento a una persona determinada, tal como se logra con la firma manuscrita, en este caso a través de la firma digital (se detallará mas adelante), la firma digital puede hacer uso de criptografía de clave pública o privada, generalmente los métodos de clave pública son mas fáciles de usar.

La criptografía de clave pública verifica la integridad haciendo uso de una firma de clave pública y una función hash de seguridad.

Una función hash es un algoritmo que se usa para crear un mensaje 'digerido' al que llamaremos 'hash', éste es una forma corta del mensaje original que cambiará si el mensaje es modificado.

El hash es entonces firmado con una clave privada. Después se puede recalcular el hash usando la clave pública correspondiente y así verificar la integridad del mensaje.

➔Función Hash

Mensaje = M ➔ Función Resumen = H(M)

Firma: $f = E_{dE}\{H(M)\}$

Donde:

dE es la clave privada del emisor que firmará H(M)
eE es la clave pública del emisor

Problema: ¿Cómo se comprueba la identidad en destino?

Solución: Se descifra la firma 'f' con eE. Al mensaje en claro recibido M' (se descifra si viene cifrado) se le aplica la misma función resumen (hash) usada con el mensaje M original, si los valores son iguales, la firma es auténtica y el mensaje íntegro:

Calcula: $E_{eE}(r) = H(M)$
Compara: ¿H(M') = H(M)?

Las funciones hash deben cumplir las siguientes propiedades para garantizar seguridad:

1. *Unidireccionalidad*.- Conocido un resumen H(M), debe ser imposible computacionalmente, hallar M a partir de dicho resumen.
2. *Compresión*.- A partir de un mensaje M de cualquier longitud, el resumen H(M) debe tener una longitud fija, y la longitud de H(M) será menor que la de M.
3. *Facilidad de cálculo*.- A partir de un mensaje M debe ser fácil calcular H(M).
4. *Difusión*.- El resumen H(M) debe ser una función compleja de todos los bits del mensaje M, por lo tanto si un bit del mensaje M es modificado, entonces el hash H(M) debería cambiar la mitad de sus bits aproximadamente.
5. *Colisión simple*.- Conocido M, será computacionalmente imposible hallar un M' tal que H(M) = H(M'), esto se denomina Resistencia débil a las Colisiones.
6. *Colisión fuerte*.- Será computacionalmente difícil encontrar un par (M, M') tal que H(M) = H(M'), esto se denomina Resistencia fuerte a las Colisiones.

A continuación se enumeran los algoritmos de resumen en criptografía:

- *MD5*: Creado por Ron Rivest en 1992 proporciona mejoras al MD4 y MD2 (1990), es más lento pero con mayor nivel de seguridad. Resumen de 128 bits.
- *SHA-1*: Del NIST, National Institute of Standards and Technology, 1994. Es similar a MD5 pero con resumen de 160 bits, otras nuevas propuestas conocidas son SHA-256 y SHA-512.
- *RIPEMD*: De la Comunidad Europea, RACE, 1992. Resumen de 160 bits.
- *N-Hash*: De la Nippon Telephone and Telegraph, 1990. Resumen: 128 bits.
- *Snefru*: Autor Ralph Merkle, 1990. Resúmenes entre 128 y 256 bits. Ha sido criptoanalizado y es lento.
- *Tiger*: Creado por Ross Anderson y Eli Biham en 1996. Resúmenes de hasta 192 bits. Optimizado para máquinas de 64 bits (Alpha).
- *Panama*: Propuesto por John Daemen y Craig Clapp en 1998. Resúmenes de 256 bits de longitud. Trabaja en modo función hash o como cifrador de flujo.
- *Haval*: Autores: Yuliang Zheng, Josef Pieprzyk y Jennifer Seberry, 1992. Admite 15 configuraciones diferentes. Hasta 256 bits.

Las funciones hash vistas (MD5, SHA-1, etc.) pueden usarse además para autenticar a dos usuarios. Como carecen de una clave privada no pueden usarse de forma directa para estos propósitos. No obstante, existen algoritmos que permiten incluirles esta función, entre ellos está HMAC, una función que usando los hash vistos y una clave secreta, autentica a dos usuarios mediante sistemas de clave secreta. HMAC se usa en plataformas IP seguras como por ejemplo en Secure Socket Layer, SSL.

2.1.3.4 Firma Digital

En los sistemas computacionales de la actualidad se almacena y procesa un número creciente de información basada en documentos en papel, disponer de estos documentos electrónicamente permite un procesamiento y transmisión rápidos que ayudan a mejorar la eficiencia en general. Sin embargo, la aceptación de estos documentos en papel ha sido tradicionalmente determinada por la firma escrita que contienen, por lo tanto es necesario refrendar estos documentos en su forma electrónica con un instrumento que tenga el mismo peso legal y aceptación que la firma escrita.

El instrumento en mención es la Firma Digital, esta firma es un mecanismo criptográfico con una función similar a la de la firma escrita, que es de verificar el origen y contenido de un mensaje, y evitar que el originador del mensaje o dato pueda repudiarlo falsamente.

Una firma digital se logra mediante una Función Hash de Resumen. Esta función se encarga de obtener una “muestra única” del mensaje original. Dicha muestra es más pequeña y es muy difícil encontrar otro mensaje que tenga la misma firma. Suponiendo que B envía un mensaje M firmado a A, el procedimiento es:

- B genera un resumen del mensaje R(M) y lo cifra con su clave privada
- B envía el criptograma
- A genera su propia copia de R(M) usando la clave pública de B asociada a la privada
- A compara su criptograma con el recibido y si coinciden el mensaje es auténtico.

Cabe destacar que:

1. Cualquiera que posea la clave pública de B puede constatar que el mensaje proviene realmente de B.
2. La firma digital es distinta en todos los documentos: si A firma dos documentos produce dos criptogramas distintos y; si A y B firman el mismo documento M también se producen dos criptogramas diferentes.

Las funciones Hash están basadas en que un mensaje de longitud arbitraria se transforma en un mensaje de longitud constante dividiendo el mensaje en partes iguales y luego aplicando la función de transformación a cada parte y sumando todos los resultados obtenidos.

Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor más utilizado.

La Firma Digital debe cumplir los siguientes requisitos:

- Debe ser fácil de generar.
- Será irrevocable, no repudiable por su propietario.
- Será única, sólo posible de generar por su propietario.
- Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
- Debe depender del mensaje y del autor.

Esta última propiedad es muy importante.

Si bien en ciertos escenarios es muy importante mantener el secreto de la información, si es que ésta lo requiere, en la mayoría de los casos tiene quizás más trascendencia el poder certificar la autenticidad entre cliente y servidor como ocurre con el comercio electrónico, y garantizar la integridad y confidencialidad de la información que con este fin circula a través de Internet.

Las funciones de la Firma Digital son garantizar:

- Autenticidad del emisor
- Integridad del mensaje
- Actualidad del mensaje
- No repudio del emisor
- No repudio del receptor
- No usurpación de identidad del emisor / receptor

A continuación se enumeran los estándares de Firma Digital:

- 1991: El NIST *(National Institute of Standards and Technology),* propone el DSA, (*Digital Signature Algorithm)*, una variante de los algoritmos de ElGamal y Schnoor.
- 1994: Se establece como estándar el DSA y se conoce como DSS, (*Digital Signature Standard)*
- 1996: La administración de los Estados Unidos permite la exportación de Clipper 3.11, en donde se encuentra incluido el DSS, el mismo que usa una función SHS, (*Secure Hash Standard).*

The Global Trust Register, es un directorio que contiene las principales claves públicas a nivel mundial, esto permite verificar la validez de certificados X.509 y claves públicas PGP

2.1.3.5 Certificados Digitales

Un Certificado Digital, también llamado Certificado de Autenticidad o ID Digital, es un desarrollo de última tecnología que usa criptografía de clave pública para identificar personas, sus privilegios y relaciones; estos certificados son el equivalente de documentos de identidad como los DNI, licencias de conducir, pasaportes u otros.

El Certificado digital enlaza la identidad de una persona a un par de claves que esa persona usa para encriptar un mensaje o firmar digitalmente, asimismo, el Certificado permite a esa persona confirmar que es quien dice ser y que tiene el derecho de usar dichas claves. Un Certificado Digital es emitido por una Autoridad Certificadora y contiene básicamente los siguientes datos:

- Clave Pública del propietario
- Nombre del propietario
- Fecha de expiración
- Identificación del Certificador
- Número de Serie del Certificador
- Firma Digital del Certificador

VeriSign y CyberTrust fueron las primeras firmas comerciales en emitir Certificados Digitales; originalmente el procedimiento de certificación se desarrolló en el MIT, (*Massachussets Institute of Technology)*, en la actualidad las normas para ello están especificadas CCITT mediante el X.509 y se ha implementado en el sistema de seguridad Kerberos.

La versión de Certificados Digitales de SET han sido diseñados exclusivamente para tarjetas de crédito, el SET extiende el uso del estándar X.509 para uso en comercio electrónico.

Una Autoridad de Certificación es un ente u organismo que conforme a ciertas políticas y algoritmos, certificará -por ejemplo- claves públicas de usuarios o servidores

Las Funciones de una Autoridad Certificadora son:

- Emisión de certificados para nuevos usuarios
- Rutinas para modificar o dar de baja un certificado
- Generar listas de revocación
- Comunicarse con otros centros de certificación (estructuras jerárquicas)

PGP (Pretty Good Privacy), es un criptosistema de alta seguridad que combina algunas de las características de los criptosistemas de clave pública y los criptosistemas de clave privada, es decir es híbrido, en la actualidad es probablemente el programa de cifrado mas conocido en el ciberespacio. PGP reconoce dos formatos de certificados diferentes:

- PGP Certificados
- X.509, es uno de los formatos de certificado mas extendido.

2.1.3.6 PKI (Public Key Infraestructure)

Como toda compañía que desea hacer negocios en Internet, debemos tener en cuenta la seguridad de la aplicación que utilizaremos para hacer negocios. Gran parte del comercio hoy es transado a través de tarjetas de débito, tarjetas de crédito y ordenes de compra. Internet es uno de los medios más hostiles en el mundo, ya que existen más de 10 millones de usuarios alrededor de el, interactuando e intercambiando información con todo tipo de contenido, esto ha originado que el movimiento de agentes hostiles en Internet esté virtualmente asegurado, el mundo del ciber-crimen está generalmente libre de la posibilidad de captura o persecución. Ante este panorama, muchos se preguntan ¿Cómo es que yo realmente puedo saber quien está al otro lado de la transacción? Ante todo, tener en cuenta que la confidencialidad e integridad de datos, el control de los accesos, la autenticación de la persona con la que hacemos negocios, y la no repudiación de la información que nos sea enviada o que nosotros enviemos es sumamente importante.

La Infraestructura de Clave Pública (PKI por sus siglas en inglés) es la combinación de software, tecnología de encriptación y servicios que permiten a la empresa proteger la seguridad de sus comunicaciones y negocios en la Internet.
Integra certificados digitales, llaves criptográficas y autoridades de certificación en toda una arquitectura de seguridad de la red de nuestra empresa.

El sistema de autenticación debe tener:

- Una política de certificación
- Un certificado de la CA
- Los certificados de los usuarios (X.509)
- Los protocolos de autenticación, gestión y obtención de certificados:

o Se obtienen de bases de datos (directorio X.500) O bien directamente del usuario en tiempo de conexión (WWW con SSL).

Algunas características de diseño de la AC

- Deberá definirse una política de certificación
  - Ámbito de actuación y estructura
  - Relaciones con otras ACs
- Deberá definirse el procedimiento de certificación para la emisión de certificados:
  - Verificación on-line
  - Verificación presencial
- Deberá generarse una Lista de Certificados Revocados

Funcionamiento de una AC

- Puesta en marcha de la AC:
  - Generará su par de claves
  - Protegerá la clave privada con una passphrase
  - Generará el certificado de la propia AC
- Distribución del certificado de la AC:
  - A través del directorio X.500
  - Por medio de páginas Web
- Podrá certificar a servidores y a clientes

2.1.4 Seguridad en Comunicaciones

Internet, sin lugar a dudas ha revolucionado el mundo de la informática y el de las comunicaciones, es al mismo tiempo un canal de transmisión mundial un mecanismo para distribución de información y un medio para la interacción y colaboración entre individuos, organizaciones y computadores sin importar la ubicación geográfica de éstos. En cualquier caso la interacción y colaboración entre dos entidades se desarrolla en base a la comunicación entre ellas y tiene como pre-requisito la confianza, que se construye y genera en base a seguridad.

2.1.4.1 OSI Vs. TCP/IP

Internet constituye una infraestructura extendida de información formada por un conjunto de miles de redes interconectadas; esta infraestructura está basada en un protocolo de red y transporte abierto: TCP/IP, que prácticamente tiene un alcance universal.

Las redes en la actualidad, que son las que conforman Internet, se caracterizan por basarse en arquitecturas por niveles, con protocolos por niveles, la base reconocida para ello es el modelo OSI, que establece un modelo y define protocolos específicos para el mismo. Los estándares de seguridad han sido añadidos a la arquitectura OSI para proporcionar una funcionalidad de seguridad, amplia, coherente y coordinada; visualizaremos esto en la Figura II.2

EQUIVALENCIA ENTRE LOS MODELOS
OSI Y TCP/IP

Figura **2.2** Niveles del Modelo OSI Niveles TCP/IP

2.1.4.2 Seguridad en Nivel de Aplicación

La ubicación de la seguridad en el nivel de Aplicación, Fig. II.3 es la solución adecuada cuando:

- El servicio de seguridad es específico de la aplicación
- El servicio de seguridad pasa a través de aplicaciones intermedias

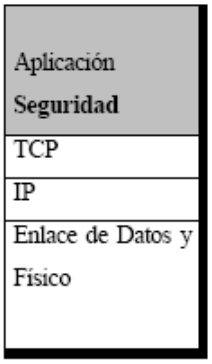


Figura 2.3

En este nivel la seguridad está dirigida a tres rubros que son de particular preocupación: Mensajes electrónicos, transacciones en la Web y pagos en línea; todos estos rubros están sujetos a riesgos potenciales tanto de pérdidas financieras como de imagen y relaciones públicas y aspectos legales y requieren una seguridad mayor que la que proporcionan protocolos de seguridad de niveles inferiores.

Cuando la seguridad está ubicada en este nivel tenemos las siguientes ventajas:

- Menos datos a procesar
- Interfaz sencilla con la aplicación
- Compatibilidad con sistemas conectados a otro tipo de redes

Y la desventaja de tener que considerar la implementación para cada aplicación en cada sistema extremo.

2.1.4.3 Seguridad en Nivel de Transporte

Cuando la seguridad se ubica en el nivel de Transporte, Fig. II.4, los datos procedentes de la aplicación se cifran en el terminal origen antes de ser transmitidos.

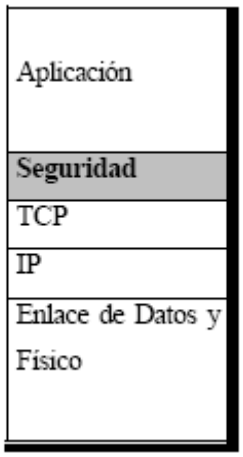


Figura 2.4

Ejemplo de protocolos en este nivel: SSL, TLSP, WTLS entre otros.

La ventaja de ubicar la seguridad en este nivel es que sólo es necesario diseñar dos interfaces entre el nivel de seguridad y el de transporte, por otro lado tenemos como desventaja que no permite ofrecer servicios a campos específicos de la aplicación.

2.1.4.4 Seguridad en Nivel de Red

La seguridad se ubica en el nivel de Red, Fig. II.5, cuando se supone que los sistemas extremos son fiables y las redes subyacentes no lo son, un ejemplo de protocolo en este nivel es IPSEC.

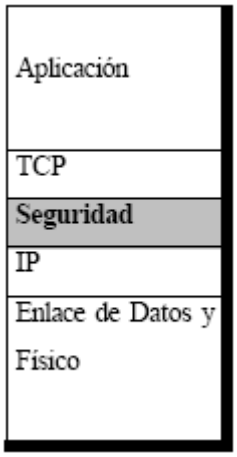


Figura 2.5

Cuando la seguridad está ubicada en este nivel la desventaja es la no compatibilidad con sistemas conectados a otro tipo de redes, pero tenemos las siguientes ventajas:

- Servicios de seguridad transparentes a las aplicaciones
- La capa TCP cifrada oculta detalles de la red.

2.1.5 Seguridad en Infraestructura

La progresiva descentralización de las arquitecturas informáticas implica la necesidad de una mayor atención a los accesos, en el doble sentido de facilitar los accesos autorizados e impedir los no autorizados, éstos últimos calificados como **intrusiones,** los mecanismos para controlar estos accesos se basan en la comparación de algún contenido del mensaje o elemento que pretende pasar al

dominio controlado con una información de referencia, dicho contenido puede ser una información explícita, por ejemplo una contraseña, o bien información que exija un análisis estructural del mensaje para descubrir un patrón catalogado, sea de infección (virus, worms, etc.) o de modificación (intrusión). En todos los casos, el resultado de la comparación conlleva a decisiones de 'apertura' o 'cierre' de puertas, seguidas de otras posibles medidas de salvaguarda.

2.1.5.1 Filtros

Los mecanismos de filtro que se instalan en los nodos-conectores de las redes tienen como función controlar el acceso de terceros a los flujos de información.

Los nodos pueden ser de tres tipos según su nivel OSI y función:

- *Repetidor. Nivel 1, Físico.-* se emplea en un mismo edificio para enlazar equipos comunicados directamente.
- *Puente (Bridge). Nivel 2, Enlace.-* enlaza dos subredes y copia el tráfico de una a otra cuando su origen y destino están en cada orilla. El puente aprende de manera dinámica que equipos se encuentran en cada subred y distribuye tráfico y evita saturaciones en el mismo edificio.
- *Encaminador (Router). Nivel 3-4, Enlace-Red.-* enlaza dos redes unidas por canales externos al edificio atendiendo direcciones de red; por lo tanto suele clasificar los paquetes por protocolo y exigir mecanismos de filtrado específicos.

Un Firewall es un mecanismo de filtro avanzado que protege la confidencialidad e integridad de la información que lo atraviesa, protege una red de otra en la que no se tiene confianza, su función es básicamente separar la red interna de una organización de Internet. Funcionalmente el firewall es un dispositivo lógico que tiene funciones de separación, limitación y análisis del flujo de la información que

circula entre sus dos puertas, como ejerce un control de acceso centralizado, su efectividad exige que lo atraviese todo usuario interno/externo/remoto para acceder desde/a las redes internas protegidas. Los firewalls pueden trabajar en tres niveles:

- *A nivel de Red*.- también llamado filtrado de paquetes o 'apantallado'. Suele ser un router con filtros que usa reglas para conceder o denegar el paso de los paquetes basándose en sus direcciones (fuente, destino y puerto). Su coste es bajo, es rápido, seguro, flexible y transparente, pero poco seguro, pierde el control tras dar el acceso no protege de direcciones enmascaradas ('spoofing'), no da información de registro (logging).
- *A nivel de Aplicación.*- se suele llamar sistema proxy, funciona como 'apoderado' de los usuarios internos que solicitan servicios a los servidores externos de Internet., si se le configura, controla el acceso a servicios individuales simulando ser el origen de todo el tráfico entrante e incluso puede hacerse cargo del tráfico interno. Su mayor costo se compensa con ciertas ventajas: puede configurarse como la única dirección de computador visible para la red externa, proporciona un registro (logging) detallado, y como requiere un módulo proxy específico para cada tipo de servicio, protege incluso contra los computadores internos no seguros o mal configurados. Soporta autentificación 'fuerte' del usuario en dos niveles:
  - El clásico de Identificador + contraseña., poco robusto contra ataques de husmeadores o sniffers.
  - Uno más sofisticado, con técnicas de retrollamada (call-back), claves de un solo uso (one time passwords OTP) o claves públicas certificadas.
- *A nivel de agente activo.*- puede controlar el contenido de los accesos a los servicios, por ejemplo: evitando virus, impidiendo el acceso a servicios de carácter no profesional, imponiendo límites al volumen de información en tránsito, etc. Se apoya en arquitecturas híbridas de los dos niveles citados.

Los firewalls presentan las siguientes limitaciones:

- No protege frente a desastres
- No protege frente a los virus
- No autentifica el origen de los datos
- No garantiza confidencialidad de los datos

2.1.5.2 Sistemas de Detección de Intrusos. IDS

Existen dos tipos básicos de Sistemas de Detección de Intrusos (IDS):

- Basado en Host
- Basado en Red

El IDS basado en Host debe ser instalado en todo sistema en que la capacidad de detectar intrusos es deseada; y aún cuando puede ser mas apropiado para esta función incluso de un atacante interno, su costo puede ser alto y puede limitar la performance del sistema de manera sustancial.

La alternativa son los IDS basados en Red, éstos recolectan datos de sensores y sistemas y los procesan de manera centralizada. Los IDS basados en Red suelen tener un bajo costo y no afectan de manera importante la performance del sistema, pero no son tan eficaces como los IDS basados en host.

2.1.6 Niveles de Seguridad Informática

Lo que importa al usuario o consumidor de un producto, es que dicho producto y/o la organización que lo provee, cumplan los requisitos necesarios para su uso o consumo, la mera existencia de las normas y la declaración del cumplimiento de éstas por parte del proveedor no suelen ser suficientes por sí solas para generar confianza, la generación de confianza requiere la existencia e intervención de esquemas rigurosos y universalmente aceptados, de evaluación, acreditación y certificación, que posibiliten el reconocimiento internacional mas amplio posible, en vista de la ubicuidad de Internet y las TI.

Por ejemplo, el sector educativo tiene esquemas de evaluación (exámenes), acreditación (centros examinadores) y certificación (centros que otorgan títulos), esquemas de este tipo, ampliamente conocidos, aceptados y aplicados son requeridos en el caso de la seguridad informática.

Los Criterios Comunes *(Common Criteria)* representan el resultado de los esfuerzos para desarrollar criterios de evaluación de seguridad informática, que puedan ser ampliamente usados por la comunidad internacional, son una contribución al desarrollo de un estándar internacional y abren el camino a reconocimiento mutuo de los resultados de una evaluación a nivel mundial.

El trabajo de los *Common Criteria (CC)* es una iniciativa de las siguientes organizaciones:

- CSE (Canadá)
- SCSSI (Francia)
- BSI (Alemania)
- NLNCSA (Países Bajos)
- CESG (Reino Unido)
- NIST (EE.UU.)
- NSA (EE.UU.)

El proyecto de los CC se remonta a 1993, y tiene como punto de partida los tres criterios de evaluación de seguridad de las TI existentes en ese momento:

- ITSEC *(Information Technology Security Evaluation Criteria)*.- de la Unión Europea, es el referente principal.
- TCSEC *(Trusted Computer Security Evaluation Criteria)* .- de Estados Unidos.
- CTCPEC de Canadá

Los Criterios Comunes son un esfuerzo multiestatal para armonizar estos criterios, y pese a las diferencias entre unos y otros se pudo comprobar que los resultados de las evaluaciones efectuadas, arrojaban resultados razonablemente equivalentes, lo que permitía la viabilidad de una solución común.

Los CC son lo suficientemente flexibles para permitir su evolución convergente con los numerosos esquemas nacionales existentes sobre seguridad informática en lo concerniente a evaluación, certificación y acreditación. Los CC también proporcionan gran flexibilidad para la especificación de productos de seguridad; los usuarios en general pueden especificar la seguridad funcional de un producto en términos de un perfil estándar de protección, y seleccionar un nivel, previa evaluación, de los 7 niveles de evaluación de aseguramiento definidos en los CC.

Los CC son aplicables a las salvaguardas implementadas por hardware o software, atienden mayoritariamente a las amenazas de personas e incluyen la protección de la confidencialidad, integridad o disponibilidad, los criterios de evaluación que contienen son técnicos, no administrativos y tampoco incluyen orientaciones sobre el marco legal donde se aplican.

La versión 2.0 de los CC, es recogida por la norma ISO 15408, y consta de tres partes, la primera es una descripción del modelo general y establece la estructura y el lenguaje para describir los requisitos de seguridad de los productos y

sistemas, la segunda detalla los requerimientos de seguridad funcional y la tercera los requerimientos para los niveles de aseguramiento. Una descripción de la aplicabilidad de cada una de estas partes a los usuarios de CC interesados, (consumidores, desarrolladores y evaluadores) se describe en la figura II.6

	Consumidores	Desarrolladores	Evaluadores
Parte 1 : Introducción y Modelo General	Como información referencial	Como información referencial para definir requerimientos y formular especificaciones de seguridad para TOE's,	Como información referencial. Como estructura de soporte para ST's y PP's.
Parte 2 : Requerimientos de Seguridad Funcional	Como soporte y referencia en la formulación y declaración de requerimientos de funciones de seguridad.	Como referencia cuando se interpretan las declaraciones de requerimientos y la formulación de especificaciones funcionales de los TOE's	Criterios de evaluación mandatorios para determinar si un TOE presenta efectivamente las funciones de seguridad que declara
Parte 3 : Requerimientos de Aseguramiento	Como soporte para determinar los niveles de aseguramiento requeridos	Como referencia para interpretar requerimientos de aseguramiento y determinar los alcances de aseguramiento de los TOE's	Criterios de evaluación mandatorios para determinar el aseguramiento de los TOE's y para evaluar los PP's y ST's

Figura 2.6Fuente: ***"Common Criteria. Introduction"***

Donde:

TOE (Target of evaluation) es el producto o sistema de TI que se quiere evaluar. *ST (Security Target)* es el objetivo de seguridad, es decir, es una estructura formal que comprende las amenazas al TOE, los requisitos de seguridad y el resumen de las especificaciones de las funciones de seguridad y medidas de aseguramiento implementadas en el TOE. El ST es la base para un acuerdo contractual entre desarrolladores, evaluadores y consumidores.
PP (Protection Profile) es un perfil o estructura formal que especifica, el entorno donde se usará el TOE, los ST y los requisitos de seguridad que el TOE debe satisfacer para alcanzar los ST.

La evaluación parte de la descripción de los requisitos de seguridad de un determinado sistema o componente y puede realizarse de manera genérica o particular para un ST. Una categoría de productos o sistemas de TI tienen una serie de requisitos, objetivos y amenazas respecto a su seguridad, los mismos que se encuentran descritos en el PP, un perfil de protección (PP) responde a las demandas de los consumidores en lo que respecta a la seguridad.

Un cliente o 'consumidor' de TI puede utilizar las evaluaciones como ayuda para decidir si un producto o sistema satisface sus necesidades de seguridad, los CC proporcionan una estructura formal para estas necesidades, es decir el PP.

Paralelamente un desarrollador usa un ST, estructura formal aplicable a un producto específico con el que identifica los requisitos satisfechos por su TOE.

Los CC describen el conjunto de acciones generales que el evaluador debe llevar a cabo y los procedimientos a seguir se encuentran especificados en el Common Evaluation Methodology (CEM).

Los CC definen conjuntos de elementos que se clasifican según sus requerimientos de seguridad y se agrupan en entidades denominadas 'Componentes'. Los Componentes se agrupan en 'Familias' que comparten objetivos de seguridad que pueden diferir en énfasis o rigor, y las Familias se agrupan en 'Clases' que comparten un objetivo funcional.

Como ya se ha mencionado los CC definen 7 niveles de evaluación de aseguramiento *(EAL, Evaluation Assurance Level)*, para cuya evaluación se exige un rigor y formalismo progresivos en el diseño y la construcción del TOE, se tiene en cuenta además la fortaleza de los mecanismos de seguridad del TOE, según el tipo de ataque que se espere contra él.

Los EAL son los siguientes:

EAL1 - *functionally tested* - Este nivel proporciona una evaluación del TOE, en las condiciones en que éste se encuentra disponible al cliente, incluye un chequeo de las especificaciones y también de la documentación de soporte que entregue el proveedor. Se pretende que la evaluación EAL1 pueda ser llevada a cabo de manera satisfactoria sin la asistencia del desarrollador del TOE y con un mínimo presupuesto. Esta evaluación es aplicable cuando se requiere evidencia de si el TOE funciona de una manera consistente con su documentación, pero las amenazas a su seguridad no son vistas como algo serio, el análisis se basa en el chequeo independiente de las funciones de seguridad del TOE. El EAL1 proporciona un incremento significativo de aseguramiento sobre un producto o sistema de TI no evaluado.

EAL2 - *structurally tested* – Este nivel proporciona aseguramiento mediante el análisis de las funciones de seguridad usando las especificaciones, la documentación de soporte y diseño de alto nivel del TOE, para comprender el comportamiento de su seguridad. El EAL2 representa un incremento significativo de aseguramiento comparado con el EAL1, por los requerimientos de chequeo del desarrollador, el análisis de vulnerabilidad y la evaluación de la funcionalidad

basada en especificaciones mas detalladas del TOE. Es aplicable cuando desarrolladores o usuarios requieren un nivel de bajo a moderado de aseguramiento. La inversión de costo y tiempo no se incrementa sustancialmente.

EAL3 - *methodically tested and checked* - Este nivel proporciona aseguramiento a través del uso de controles del ambiente de desarrollo, manejo de la configuración del TOE y evidencia de procedimientos de entrega seguros, el análisis es soportado por el chequeo independiente de las funciones de seguridad del TOE, evidencias de las pruebas del desarrollador basadas en especificaciones funcionales y diseño de alto nivel, análisis de funciones y de vulnerabilidades. El incremento de aseguramiento sobre el EAL2 está dado por los requerimientos de una cobertura mas amplia de chequeo de funciones, mecanismos y procedimientos de seguridad del TOE, que proporcionan confianza en que no habrá interferencias durante el desarrollo.

EAL4 - *methodically designed, tested and reviewed* - Una evaluación EAL4 proporciona un análisis soportado por el diseño de bajo nivel de los módulos del TOE y una parte de la implementación. El test se basa en un análisis de vulnerabilidades, y aunque es riguroso no requiere de manera sustancial conocimientos especiales u otros recursos. Los controles de desarrollo se basan en el modelo de ciclo-de-vida, identificación de herramientas y el manejo automático de configuración. El EAL4 es el más alto nivel en el que es económicamente posible reajustar una línea de productos existente.

EAL5 - *semiformally designed and tested* – Una evaluación EAL5 proporciona un análisis que incluye la implementación completa. El aseguramiento es incrementado por un modelo formal de las políticas de seguridad del TOE, una presentación semiformal de las especificaciones funcionales y del diseño de alto nivel, y una demostración semiformal de la correspondencia entre éstos. En este nivel de evaluación se requiere el diseño modular del TOE y el análisis de covert channels (canales ocultos o canales ilícitos de flujo de información). El análisis de vulnerabilidades debe asegurar resistencia a la penetración de atacantes cuya fortaleza sea moderada.

EAL6 - *semiformally verified design and tested* – El EAL6 es aplicable al desarrollo de TOE's especialmente seguros, para situaciones de alto riesgo en las que el valor de los recursos protegidos justifica los costos adicionales. La evaluación se basa en un análisis modular y por capas del diseño, el análisis de vulnerabilidades debe asegurar resistencia a la penetración de atacantes cuya fortaleza sea alta, la búsqueda de covert channels debe ser sistemática.

EAL7 - *formally verified design and tested* – El EAL7 es aplicable al desarrollo de TOE's para aplicaciones en situaciones de extremado riesgo, y cuando el valor de los recursos a proteger justifica los altos costos. Para una evaluación EAL7 se requiere una presentación formal de las especificaciones funcionales y del diseño de alto nivel, y que exista correspondencia entre ambos, el análisis incluye todo lo necesario para los niveles anteriores y además la validación de un análisis sistemático de covert channels.

Los EAL's de CC han sido desarrollados con el objetivo de preservar los conceptos de aseguramiento bosquejados en los Criterios que los anteceden y que son su base, de esta manera los resultados de evaluaciones previas a los CC continúan siendo relevantes. En la tabla que se presenta a continuación, se establece una equivalencia entre niveles de distintos Criterios, equivalencia que no hay que tomar al pie de la letra pues los niveles de aseguramiento no son tratados de la misma manera en los distintos criterios y por tanto una semejanza exacta no existe.

Common Criteria	**US TCSEC**	**European ITSEC**
-	D: Protección Mínima	EO
EAL1	-	-
EAL2	C1: Seguridad Discrecional	E1
EAL3	C2: Acceso Controlado	E2
EAL4	B1: Seguridad Etiquetada	E3
EAL5	B2: Protección Estructurada	E4
EAL6	B3: Dominios de Seguridad	E5
EAL7	A1: Seguridad Verificada	E6

Fuente: *"Common Criteria. An Introduction"*

Sobre el reconocimiento de los Certificados de Criterios Comunes, además de las mencionadas líneas arriba, los siguientes países ratificaron su adhesión:

- Australia
- España
- Grecia
- Italia
- Noruega
- Nueva Zelanda

Este acuerdo, denominado *Arrangement (Arreglo)* tiene un impacto previsible reflejado en los datos sobre el mercado de TI que proporciona el EITO *(European Information Technology Observatory).* El conjunto de los países miembros del Arreglo representaban más del 65% del mercado mundial, esto en 1999.

Este Arreglo se gestiona por un Comité, cuya primera presidencia corresponde a Alemania y fue firmado en coincidencia con la Primera Conferencia Internacional de Criterios Comunes a la que asistieron expertos de 23 países.

El Arreglo parte de la premisa de que la utilización de productos y sistemas de TI, cuya seguridad ha sido certificada, es una de las salvaguardas principales para proteger la información y los sistemas que la manejan.

Los Organismos de Certificación reconocidos son los encargados de expedir certificados de seguridad a productos o sistemas de TI, o a perfiles de protección, que hayan sido previamente evaluados por Servicios de Evaluación, conforme a los CC, y cuyo resultado haya sido satisfactorio.

El Arreglo consta de 18 artículos, 11 anexos y un apéndice, a lo largo de los cuales especifica con detalle los requisitos que han de cumplir los Certificados de

CC, los Organismos de Certificación y los Servicios de Evaluación, esto entre otros aspectos.

Los CC establecen un conjunto de requisitos que permiten definir las funciones de seguridad de productos y sistemas de TI y de los criterios necesarios para evaluar su seguridad, el proceso de evaluación garantiza que las funciones de seguridad de dichos productos y sistemas reúnen los requisitos que declaran. Los resultados de las evaluaciones realizadas por Servicios de Evaluación independientes entre sí, son equivalentes en su totalidad.

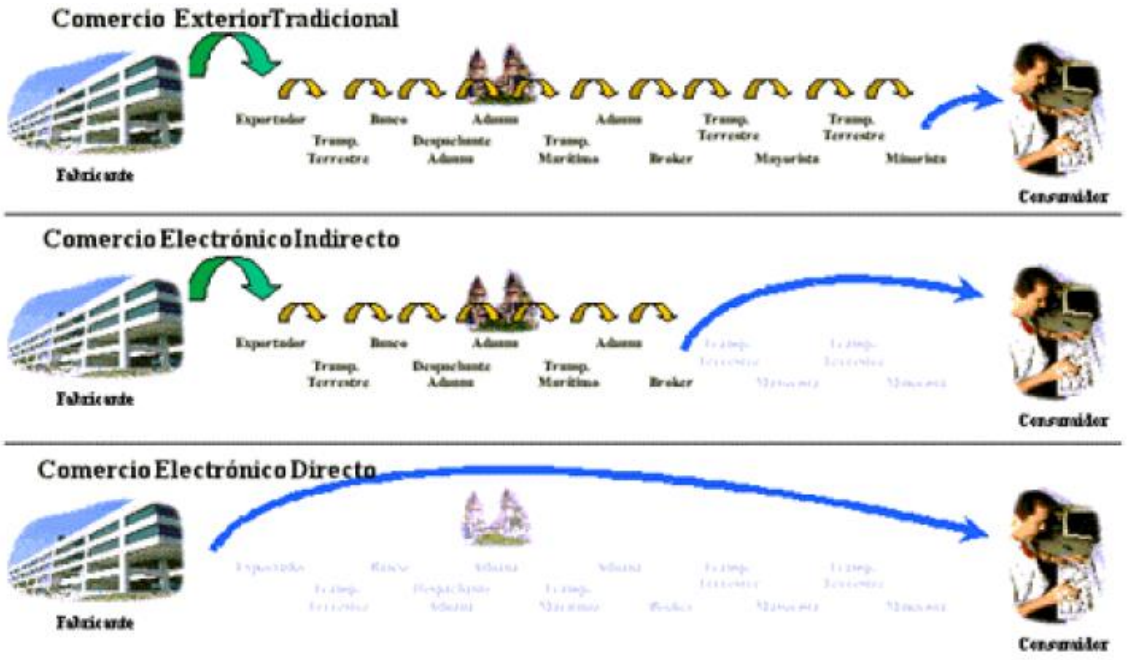
Entre los objetivos del arreglo, figuran:

- Asegurar que las evaluaciones realizadas a productos y/o sistemas de TI, o a perfiles de protección (adecuados a cada caso), hayan sido hechas bajo normas rigurosas y consistentes.
- Propiciar el incremento de los productos y sistemas de TI, y de los perfiles de protección evaluados, con nivel de seguridad en aumento, disponibles en el mercado.
- Que gracias a la aceptación internacional de los certificados, se elimine la carga, en distintos países, que acarrea la duplicación de las evaluaciones de productos y sistemas de TI, y/o perfiles de protección.
- Disminuir los gastos de evaluación y certificación de productos y sistemas de TI, y/o perfiles de protección, en razón de la economía de escala.

2.2 COMERCIO ELECTRÓNICO (E-COMMERCE)

Definición 1: son las actividades comerciales realizadas a través de medios electrónicos de manera "enteramente automática".

Definición 2: Cualquier forma de transacción comercial en la que las partes interactúan electrónicamente en lugar de por intercambio o contacto físico directo.



La venta electrónica es una modalidad del Comercio Electrónico en la que un proveedor suministra bienes o servicios a un cliente a cambio de un pago. Tanto la oferta de los bienes y/o servicios como el pago que realiza el cliente se efectúan por vía electrónica.

La historia del comercio electrónico comenzó hace más de dos décadas por parte de las empresas con la introducción del Intercambio Electrónico de Datos (EDI), que se dio entre firmas comerciales, con el envío y recibo de pedidos, información de reparto y pago, etc).

De igual modo el comercio electrónico, que está orientado al consumidor no tiene pocos años, hace algún tiempo que tenemos conocimiento de lo que es un cajero automático (ATM) o una tarjeta de crédito, y cada vez que se hace uso de una de estas modalidades se está realizando una transacción de comercio electrónico. Estas tecnologías (EDI y ATM), trabajan en un sistema cerrado y es por eso que se ajustan estrictamente a las medidas de la transacción.

En lo que respecta a la parte de Cliente-Servidor, por intermedio de la World Wide Web, se ha establecido una nueva era, tomando y combinando las cualidades de carácter abierto que tiene Internet con una interfaz de usuario sencilla.

La WWW tiene varios años de haber sido creada, y fue en el Laboratorio de Física de Partículas CERN en Ginebra en 1991, con Mosaic, que fue predecesor de Netscape, el ingreso a Internet no fué tan sencillo, le tomó dos años a Mosaic lograrlo, y otros dos años más que las empresas y en general el público se dieran cuenta de su potencial.

El mercado electrónico está referido al mercado económico que se encuentra en crecimiento, en donde los productores, intermediarios y consumidores interactúan de alguna forma electrónica o por intermedio de un contacto digital.

Los mercados físicos son representados de forma virtual en el mercado electrónico y la economía digital se encuentra representada por medio de las actividades económicas a cargo de este mercado electrónico.

Los sitios Internet que se dedican al comercio electrónico manejan una base de datos en las que se especifican uno a uno los productos o servicios ofrecidos, señalando para cada uno su precio, su existencia en inventario, sus especificaciones técnicas y frecuentemente una representación gráfica.

El usuario de Internet, ahora comprador, escoge los productos o servicios que le interesan, define la cantidad a adquirir y sólo a través de un "servidor seguro" proporciona información sobre la tarjeta de crédito mediante la cual se realizará el cargo. Se puede considerar que sólo al cumplir con todos estos requisitos la operación podrá llamarse "comercio electrónico".

Entonces, si queremos definir con mayor amplitud al Comercio Electrónico, lo involucraremos muy estrechamente al mercado electrónico. El comercio electrónico nos hace pensar inmediatamente en los mercados físicos que nosotros conocemos, ya que se dan muchos aspectos que son típicos de éstos. Por ello, al igual que en los mercados físicos, entre los componentes de los mercados de la economía digital se encuentran incluidos:

- Participantes (agentes del mercado como empresas, proveedores, intermediarios, tiendas o galerías y consumidores).
- Productos (artículos, bienes y servicios) y
- Proceso (abastecimiento, producción, marketing, competición, distribución, consumo, etc.)

Si queremos ver la diferencia que existe es que en el mercado electrónico, al menos uno de estos componentes es electrónico, digital, virtual u online, (escoja el término que prefiera). Por ejemplo un participante digital es alguien que posee una dirección de correo electrónico o una página Web.

Los vendedores puramente “físicos” pueden estar vendiendo un producto digital, por ejemplo, un CD-ROM digital.

Alguien que venda productos físicos en una tienda física puede ofrecer información sobre los productos online (permitiendo a los consumidores “buscar online”), mientras que la producción, pedido, pago y distribución, siguen

realizándose de manera convencional. En la actualidad, se pone énfasis sobre el núcleo del mercado electrónico donde toda acción se hace online. Pero si por algún motivo su negocio o consumo se desarrolla por medio de un proceso digital, usted está formando parte del mercado digital. Es decir aunque no nos hayamos dado cuenta, casi todos nosotros ya somos partícipes del mercado electrónico.

Para comenzar participando en el Comercio Electrónico, y realizar transacciones a través del mercado electrónico, se debe cumplir lo siguiente:

Nuestra participación comienza teniendo presencia en el Web. (con una página informativa).

Comercio Business-to-Business (Extranet, Red Compartida, Colaboración).
Comercio Business-to-Consumer (Internet, Seguridad, Certificación).

El comercio electrónico nos ofrece una serie de beneficios que van a hacer que nuestros negocios tengan mayor acogida en todo el contexto global, estos pueden ser algunos de los beneficios que ofrece:

- La mercadotecnia es más barata.
- La respuesta es inmediata.
- El alcance es a nivel mundial.
- Reducción de costos de manejo y procesos de documentos y transacciones.
- Evita la intermediación de funciones.
- Intercambio de información en tiempo real.
- Personalización (mercadotecnia uno a uno).

Entre las oportunidades y beneficios que se ofrecen hay:

- Presencia y Elección Global
- Mayor Competencia y Mejora de la Calidad de Servicio.
- Ajuste Generalizado, Productos y Servicios Personalizados
- Cadenas de Entrega más Cortas o Inexistentes y Respuesta Rápida de Necesidades
- Reducción de Costes y Precios
- Nuevas Oportunidades de Negocios, Nuevos Productos y Servicios.

La característica determinante del comercio electrónico en comparación con otras facilidades que proporciona Internet, es el hecho de que un cliente puede usar la conexión para realizar una transacción comercial con un proveedor. Dicha transacción puede variar desde una compra hasta una rápida verificación de su cuenta con ese proveedor.

Por lo tanto, el comercio electrónico reemplaza muchos de las funciones diarias que pueden consumir una gran cantidad de tiempo para ambas partes, como por ejemplo en los siguientes casos:

- El Banco
- El Distribuidor
- La empresa de logística
- La Fabrica virtual
- La empresa en el hogar

2.3 MARCO LEGAL

2.3.1 Consideraciones Jurídicas en Internet

El comercio electrónico se encuentra en estos momentos creciendo de forma muy rápida, todavía hay temas que están en debate los cuales están en espera de ser resueltos para obtener así todo el potencial que este nos ofrece:

1. **Globalización:** ¿Cómo pueden dos empresas de diferentes continentes saber de su existencia mutua y de los productos o servicios que necesitan u ofrecen?, ¿Cómo puede una empresa conocer y comprender las tradiciones y reglas de negocio de algunos países tan remotos, particularmente cuando estas reglas no suelen ser escritas?, ¿Y cómo puede ser respetada y soportada la diversidad lingüística y cultural de una comunidad de usuarios global?
2. **Apertura Contractual y Financiera:** ¿Cuál es la legalidad que nos ofrece un contrato que hasta cierto punto es oculto y establecido entre empresas? ¿Cuál es el estado legal de ese contrato? ¿Qué cuerpo jurídico lo recoge? ¿Cómo puede ser hecho y confirmado el pago, dadas las diferentes prácticas y regulaciones financieras? ¿Qué tasas de impuestos se aplicaría a estos productos? ¿Cómo se cargan, controlan y recaudan estas tasas? ¿Pueden resolverse los pagos y tasas por el simple procedimiento de mantener una manufacturación electrónica en un tercer país?
3. **Propiedad:** la protección de la propiedad intelectual y de los derechos de copia representan un hito aún por solucionar.
4. **Privacidad y Seguridad:** En el comercio electrónico, el reconocimiento de mecanismos de seguridad y privacidad depende de una tercera parte cualificada (tales como el cuerpo gubernamental), el comercio electrónico requiere del establecimiento de un sistema de certificación global.
5. **Interconectividad e interoperatividad:** Llegar a explotar todo el potencial del comercio electrónico necesita de acceso a nivel mundial, para esto, se debe tener

una estandarización o normalización universal para la interconexión e interoperatividad de redes.

6. **Riesgo:** Cabe la posibilidad de que muchas empresas, sobre todo pequeñas, se encuentren en desventaja, lo que haría que simplemente queden marginadas en este tipo de posibilidades y oportunidades. Es por eso que crece la necesidad de promover iniciativas, realizar campañas publicitarias y dar a conocer ejemplos afortunados promoviendo la formación y el entrenamiento.

En relación a las infracciones que pueden cometer los clientes al realizar acciones prohibidas que no van de acuerdo a las políticas de uso definidas en el contrato de servicios de un sitio web:

1. **Spamming:** Se refiere a enviar correo no solicitado y/o mensajes comerciales no solicitados a través de Internet. No es solamente por el impacto negativo que pueda crear en el consumidor hacia la empresa de servicio de internet, además puede sobrecargar la red haciendo que el servicio que se ofrece al cliente no pueda ofrecerse en condiciones plenas de calidad.

2. **Violaciones de la Propiedad Intelectual:** Se comprende aquí cualquier actividad que infrinja o se apropie de manera fraudulenta de los derechos de propiedad de otros, incluyendo copyrights, marcas, nombres comerciales, secretos comerciales, software o aplicaciones y patentes poseídas por personas físicas o jurídicas o cualquier otro tipo de entidad. También cualquier actividad que infrinja derechos a la privacidad o publicidad o cualquier otro derecho personal de otros. En algunos países, la empresa de servicios está obligada por ley a bloquear el acceso al contenido del cliente que infrinja lo dicho anteriormente.

3. **Lenguaje y Materiales Obscenos:** Al usar la red para emitir, promocionar, guardar, desplegar cualquier tipo de información con pornografía infantil o lenguaje o material obsceno. La empresa de servicios está obligada por ley a notificar a las agencias legales de dicha publicación para que se retire inmediatamente y se tomen acciones legales.

4. **Lenguaje difamatorio o abusivo:** Usar la red para transmitir o descargar lenguaje difamatorio, abusivo o amenazante.

5. Cabeceras de mensajes: Cabeceras de mensajes mal representadas que se utilicen para ocultar el verdadero contenido del mensaje**.**

6. **Acceso no autorizado o ilegal a otros ordenadores o a redes:** Acceder ilegalmente o sin autorización a ordenadores, cuentas, o redes que pertenezcan a otra parte, o atentar contra sistemas de seguridad de otros sistemas (conocido como "hacking"). En general cualquier actividad que pueda ser considerada como una penetración a un sistema.

7. **Distribución de Virus por Internet, Caballos de Troya o cualquier otro tipo de Agente destructivo:** Distribuir información sobre creación de virus, caballos de Troya, mailbombing, pinging o cualquier otro tipo de agente de ataque electrónico. Así como actividades que interfieran en la posibilidad de otros de usar la red o conectarse a la red, sistema, servicio o equipo.

8. Facilitar la violación de la AUP: Promocionar, transmitir o hacer posible cualquier tipo de aplicación, programa, producto, servicio o software que haya sido diseñado para violar esta AUP, incluyendo el facilitar el hacer uso del correo electrónico masivo (spam) en cualquiera de sus formas.

9. **Exportar el Control de Violaciones:** Exportar software encriptado a través de Internet.

10. **Grupos de Red**: La empresa de servicios de internet se reserva el derecho a no aceptar envíos desde grupos de noticias cuando se tenga el conocimiento que dichos mensajes violan la AUP.

11. **Otras actividades ilegales:** Cualquier actividad considerada como ilegal, incluyendo la promoción, transmisión o el hacer posible cualquier tipo de negocio fraudulento.

12. **Otras actividades:** Cualquier otro tipo de actividad que la empresa de servicios de internet pudiera determinar como contraria a sus clientes, reputación, buen hacer o relaciones con terceros.

13. **Privacidad de los correos de los usuarios:** La empresa de servicios de internet, no controlará intencionadamente el correo electrónico privado enviado o

recibido por sus clientes a menos que sea requerido por la ley, autoridades legales o cuando la seguridad pública pueda verse afectada.

Caso de la Casa Amazon.com contra Barnes & Noble

El caso de Amazon.com contra Barnes&Noble nos alerta que el término de "tienda" deberá entrar en un proceso de discusión nuevamente. Los impuestos son un tema que también se toca en esta oportunidad.

Los métodos de distribución de libros es amplia y los vendedores deben dar las facilidades para un conveniente acceso a los clientes. Así mismo la venta de libros por vía correo ha sido un método de distribución llevado a la práctica por muchos años.

Es entonces, que la empresa Amazon.com lleva esta idea a Internet, para convertirse en líder de la venta de libros online, y se anuncia a sí misma como "la mayor librería del mundo" sin la necesidad de contar o abrir tiendas en un local físico, sino vía Internet. La "tienda más grande del mundo", Barnes & Noble con un elevado reparto de beneficios y tiendas físicas, se vio en la obligación de contrarrestar el gran reto de Amazon.com abriendo su propia tienda Web, lo que dio lugar a un pleito contra su competidor.

Entonces, ¿cuáles son los planteamientos estratégicos que estas dos compañías tienen?, acaso ¿pueden haber empresas de productos de competencia similar que se enfrenten?.

El Caso:

Edupage, 8/24/97, Educom Amazon.com acusa a Barnes&Noble en el último asalto a la encalada de ataques entre la pionera en la venta de libros online Amazon.com y Barnes&Noble.

Amazon.com ha presentado un litigio contra Barnes&Noble, alegando que esta entidad debería pagar impuestos por los libros que vende a través de Internet.

El argumento de Amazon se basa en el hecho de que B&N, no como Amazon.com, tiene presencia física en la mayoría de los estados a través de su cadena de más de 1,000 tiendas que constituyen, por lo tanto, el "nexo" de actividad de cada estado.

Uno de los abogados de B&N ha dicho que "no existe fundamento" para las acusaciones de Amazon.

En Mayo, Barnes & Noble interpuso una demanda contra Amazon.com alegando que anunciarse como "la mayor librería del mundo" era publicidad engañosa. (Wall Street Journal 22 de Agosto de 1997)

2.3.2 Avances Legislativos En Otros Países

VENEZUELA:

DECRETO CON RANGO Y FUERZA DE LEY (2.000) SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRONICAS

- Objeto y aplicabilidad de la ley: Reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

- Alcance: Será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente procurando reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.
- La certificación a que se refiere la presente Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la Ley, requieran determinados actos o negocios jurídicos.
- Adaptabilidad de la Ley en los organismos públicos
- Eficacia Probatoria que la ley otorga a los documentos escritos
- Solemnidades y formalidades podrán realizarse utilizando para ello los mecanismos descritos en esta Ley.
- Integridad del Mensaje de Datos.
- Constancia por escrito del Mensaje de Datos quedará satisfecho con relación a un Mensaje de Datos, si la información que éste contiene es accesible para su ulterior consulta.
- Verificación de la emisión del Mensaje de Datos.
- Oportunidad de la emisión, se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario.
- Reglas par la determinación de la recepción.

    1. Si el Destinatario ha designado un sistema de información para la recepción de Mensajes de Datos, la recepción tendrá lugar cuando el Mensaje de Datos ingrese al sistema de información designado.

    2. Si el Destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el Mensaje de Datos en un sistema de información utilizado regularmente por el Destinatario.
- Lugar de emisión y recepción
- Mecanismos y métodos para el acuse de recibo.

1. Toda comunicación del Destinatario, automatizada o no, que señale la recepción del Mensaje de Datos.

2. Todo acto del Destinatario que resulte suficiente a los efectos de evidenciar al Emisor que ha recibido su Mensaje de Datos.

- Oferta y aceptación en los contratos. Las partes podrán acordar que se realicen por medio de Mensajes de Datos.
- Validez y eficacia de la Firma Electrónica. Requisitos:

  La certificación.

  Obligaciones del signatario.
- Creación de la Superintendencia de Servicios de Certificación Electrónica, tendrá por objeto supervisar, en los términos previstos en esta Ley y sus reglamentos, a los Proveedores de Servicios de Certificación públicos o privados.

DE LOS PROVEEDORES DE SERVICIOS DE CERTIFICACION

- De la acreditación.
- Garantía de validez.
- Obligaciones de los Proveedores.
- La contraprestación del servicio.
- Notificación del cese de actividades.

CERTIFICADOS ELECTRONICOS

- Garantía de la autoría de la Firma Electrónica.
- Vigencia del Certificado Electrónico.
- Cancelación.
- Suspensión temporal voluntaria.
- Suspensión o revocatoria forzosa.
- Contenido de los Certificados Electrónicos.

DE LAS SANCIONES a los Proveedores de Servicios de Certificación

Servicios de asesoría especializada en evaluación legal de Páginas Web protección legal de estructuras de negocios en Internet en el área de Internet y desarrollo de e-commerce.

1) **Nombres de Dominio**: asesoría legal en el registro, modificación y transferencia onerosa o gratuita de nombres de dominio, tanto a nivel superior como a nivel nacional o para el extranjero. Asesoría legal y asistencia en procesos de conformidad con los procedimientos alternos de solución de conflictos por el registro de dominios dictado por el ICANN (Internet Corporation for Assigned Names & Numbers)

2) **Propiedad Intelectual**: evaluación y diseño de protección sobre bienes intangibles lo que permite lograr una adecuada protección de todas las figuras objeto de marcas, patentes o derechos de autor o derechos conexos, tales como software, bases de datos, recopilaciones, diseños gráficos, etc. que puedan recaer sobre una pagina Web. Igualmente, protección que debe existir en torno al desarrollo de nuevas modalidades de uso de los derechos intangibles como lo son las modalidades de deeplinking, metatags, y framing, y su evaluación a fin de evitar procesos de competencia desleal, falso patrocinio, usos denigratorios o parasitarios, o en el caso de los derechos de autor, evitar el uso ilegal de citas de terceros, o cualquier otro tipo de bienes intangibles de terceros.

3) **Contratos:** Negociación y desarrollo de contratos relacionados con la Internet, incluyendo contratos de hospedaje, desarrollo de contenido, banners publicitarios, contratos de hipervínculo, licencias sobre derechos intelectuales, con base en ambiente Web.

4) **Condiciones de Uso y Términos Legales**: Diseño y desarrollo de Condiciones de uso de la página web, incluyendo evaluación legal de efectos a terceros en ambientes de comunidad tales como chats, foros, BBS y Newsgroups, así como el desarrollo de términos legales de páginas web.

5) **Política de Privacidad**: Estudio y desarrollo de políticas de privacidad tanto el mundo material como el mundo virtual, basados en normas estándar en la red.
6) **Autenticidad e Integridad en Ambiente Digital:** Asesoría Legal en materia de Entes y Autoridades de Certificación, Firmas Electrónicas y Certificados Digitales, incluyendo políticas de Entes de Certificación.

CHILE:

Según Erwin Fiebig, director de comercio electrónico de Entel Internet, en Chile la conectividad a Internet en empresas no logró penetrar como se esperaba, porque no existía contenido, aplicaciones reales y las compañías no veían un fin práctico en Internet, ahora con el ejemplo del SII, las empresas comienzan a distinguir que Internet es un medio y una herramienta para hacer más eficiente muchas gestiones, reducir costos y a su vez generar mayores ventas. Santiago, Chile. Luego de que por años se pensó que Transbank fue la entidad que limitó el surgimiento de las ventas a través de Internet, ahora Chile ingresa abruptamente hacía el comercio electrónico para personas, una serie de declaraciones están tratado de "desmitificar" este problema y como parte del lanzamiento de su plataforma de comercio electrónico para PYMEs, Edwin Fiebig, director de Comercio Electrónico de Entel Internet, trata de aclarar estos temas.

ESTADOS UNIDOS:

La ley del Senado americano para la tutela de la privacidad en Internet ha suscitado las críticas de las empresas tecnológicas que sostienen que la ley las expone a acciones legales por parte de los clientes y les impone unos requisitos mayores que los requeridos a sus competidores de la “Vieja Economía”.

En una audiencia de la comisión para el comercio del Senado, la ley para la privacidad online presentada por el senador Ernest Hollings ha obtenido el consenso mayoritario de las asociaciones de consumidores por establecer

requisitos diferenciados según el tratamiento que de los datos personales o “sensibles” se haga. Sin embargo las empresas de la Nueva Economía han encontrado varios puntos sobre los que discrepar.

Desde el sitio de e-commerce Amazon.com. han declarado que a dicha empresa no se le puede pedir el tratamiento de los datos personales de los clientes de forma distinta a la que hace cualquier otro competidor "offline”. Desde Hewlett-Packard Co. apuntaban que la ley podría provocar una oleada de acciones legales por parte de los clientes.

Algunos senadores sostienen que precisamente las empresas tecnológicas son las que deberían apoyar la ley para evitar la existencia de un mosaico confuso de leyes diferentes en cada estado para la tutela de la privacidad.

CAPITULO 3

Aplicación:

Construyendo Una Infraestructura Confiable De E-Commerce

Los negocios que pueden administrar y procesar transacciones comerciales a través de Internet pueden ganar en competitividad, debido a la posibilidad de alcanzar audiencia para sus ofertas a nivel mundial a bajo costo, ahora bien, hay que tener en cuenta que los clientes compran bienes y/o servicios a través de la Web sólo cuando confían en que su información personal, número de tarjeta de crédito por ejemplo, está segura; para ello el negocio debe tomar las medidas necesarias con el fin de minimizar los riesgos inherentes a la Web.

Para poder aprovechar las ventajas que proporcionan las oportunidades del e-commerce y evitar dichos riesgos, los negocios deben tener conocimiento y comprender los problemas y dudas que afectan la privacidad, seguridad y confianza en el sistema, algunas de estas preocupaciones son:

- *¿Cómo puedo estar seguro de que los datos sobre las tarjetas de crédito o débito de mis clientes, no serán accedidos por personas no autorizadas, cuando realicen una transacción supuestamente segura en la Web?*
- *¿Cómo puedo garantizar a los clientes que visitan mi site que están realizando negocios conmigo y no con un impostor?*
- *Si me he asegurado de cubrir las dudas anteriores ¿cuál es la mejor manera de hacérselo saber a los clientes para que se sientan seguros de hacer negocios conmigo?*

- *Cuando los clientes se sientan lo suficientemente en confianza para negociar en línea conmigo ¿cómo puedo darles facilidades para que me paguen usando tarjetas de crédito o débito u otros métodos?*
- *¿Cómo puedo verificar la validez de la tarjeta que está usando mi cliente?*
- *¿Qué hago con la información de pago que el cliente me ha enviado?*

Estas preocupaciones apuntan a los objetivos fundamentales de establecer una infraestructura confiable de e-commerce:

- Autentificación
- Confidencialidad
- Integridad
- No repudio

La solución para los objetivos propuestos incluyen 2 componentes esenciales:

- Certificados para servidores
- Sistema de Pago seguro en línea

Además se debe tener en cuenta que la seguridad debe estar en todas las etapas desde el inicio del proyecto.

3.1 Seguridad En El Comercio Electrónico

Internet es una red insegura para todo tipo de operaciones. La única forma de poder hacer transacciones seguras es imponiéndole mecanismos de seguridad a cada una de ellas.

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».

Esto se debe a que darle a un sistema un determinado grado de seguridad, aunque sea mínimo, implica imponer algún tipo de restricción, lo que forzosamente disminuirá la operatividad con respecto al estado anterior en el que no se tenía seguridad.

Internet es una red insegura, porque 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 que cumpliera 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.

No es cierto que, por implantar determinados mecanismos de seguridad automáticos, Internet se vuelve segura.

El parámetro fundamental a tener en cuenta, ya sea uno un usuario final o una corporación, es el siguiente: «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».

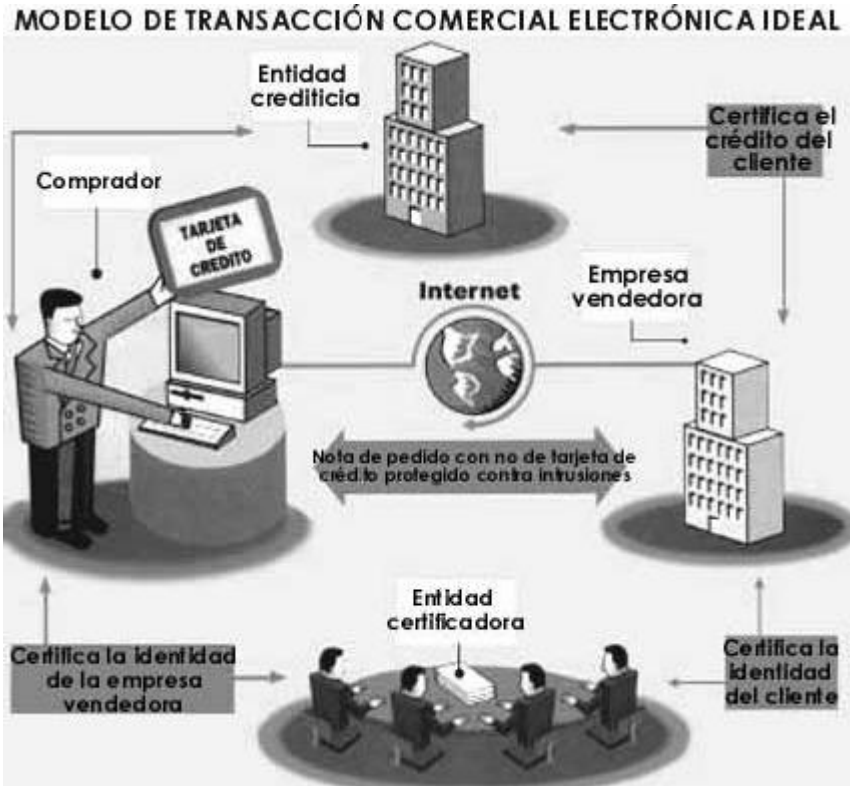
Por lo tanto, a partir de la conexión de un sistema seguro (el suyo propio) con otro inseguro (Internet) se deberá aumentar el grado de seguridad. Dicho de otra manera:

«Cada vez que se agregue algo a un sistema que lo vuelva más abierto (por ejemplo una conexión a Internet) se deberá actualizar la estrategia de seguridad informática del mismo».

Las notas de compra que completa el usuario en su computadora son enviadas por Internet a la empresa vendedora en forma de mensaje. Como estas notas contienen información sensible (número de la tarjeta de crédito del comprador), y como cualquier tipo de mensaje que circula por Internet puede ser interceptado por un intruso con el fin -entre otros- de obtener números de tarjetas de crédito en vigencia, es necesario utilizar algún mecanismo de seguridad que minimice este riesgo.

La posibilidad de que un intruso intercepte un mensaje que circula por Internet no se puede evitar, pues es parte de la inseguridad propia de Internet. Poniéndonos en el caso más desfavorable, que implicaría que todo mensaje que enviemos por Internet será interceptado, lo que tenemos que lograr es que, una vez que sea interceptado, la información que contiene no sea útil para el intruso.

Una forma de lograr esto es por medio de la encriptación de la información del mensaje.



EL APORTE DE LA ENCRIPTACIÓN

La encriptación aplicada a un caso como éste funciona codificando por medio de una clave la información que contiene el mensaje.

De esta manera, el contenido sólo puede ser conocido por quienes tengan la clave para decodificarlo (el comprador y la empresa vendedora).

Aunque un intruso intercepte el mensaje, lo que verá en él le resultará incomprensible, pues no tiene la clave de decodificación para hacerlo legible.

En la práctica, estos mecanismos se implementan con sistemas de doble encriptado o de clave pública, que además de tener un buen nivel de seguridad contra ataques de decodificación, permiten determinar que el mensaje ha sido generado por una determinada persona.

LA IDENTIDAD DEL COMPRADOR Y LA EMPRESA VENDEDORA

En una transacción comercial física, la identidad del emisor puede ser probada por medio de un documento, y la de la empresa vendedora por medio de sus comprobantes de venta.

Pero una de las características más particulares de la comunicación electrónica (como es la comunicación a través de Internet), es la capacidad de anonimato y de presentarse bajo una identidad falsa.

El sistema de doble encriptado garantiza que la orden de compra fue emitida por el propietario de una determinada dirección de correo electrónico, pero la pregunta que surge es:

¿Será el propietario de esa dirección de correo electrónico quien dice ser, y por lo tanto el titular de la tarjeta de crédito?

Con respecto a la empresa vendedora también cabe preguntarse: ¿la página web que estoy viendo en la pantalla de la computadora es auténtica o sólo es una trampa para recolectar números de tarjeta de crédito de incautos?

El mecanismo propuesto para estos casos es el uso de Certificados Digitales emitidos por una Autoridad de Certificación.

La Autoridad Certificadora se encarga de certificar que una determinada dirección de correo electrónico pertenece a una persona específica, y que una determinada dirección de página web pertenece a una empresa específica. De esta manera, por medio de la AC quedarían aseguradas las identidades del comprador y de la empresa vendedora.

El grado de seguridad y el de operatividad de un sistema son inversamente proporcionales, tal como se ha visto líneas arriba; es por esto que el arte del consultor en seguridad informática, consiste en llevar un sistema a una relación de equilibrio entre estos dos factores.

En una transacción electrónica ideal el comprador y la empresa vendedora se comunican a través Internet.

La empresa llega al comprador a través de su página Web, que debería estar certificada en cuanto a su identidad por una AC.

Los pedidos del usuario llegan a la empresa vendedora por medio de un mensaje protegido por encriptación, para que, en caso de ser interceptado, no se conozca el número de tarjeta de crédito. La identidad del usuario también debería estar certificada. La entidad crediticia que emite la tarjeta de crédito seguirá existiendo para avalar el crédito del usuario hasta que se implementen otros mecanismos de pago como el dinero electrónico.

PROTOCOLOS

Determinados protocolos aseguran la confidencialidad e integridad de la información transmitida a través de la Red y garantizan la viabilidad de cualquier orden de pago.

Una de las principales preocupaciones que tiene el consumidor en el uso del comercio electrónico es la seguridad. ¿Qué pasa si doy mi número de tarjeta para comprar en una tienda? ¿Es seguro? ¿Me robarán los datos? ¿Y el dinero? ¿Es Internet un medio de pago seguro?

Para ello se han creado dos protocolos estándar de seguridad: **el protocolo SET y el protocolo SSL**.

Una vez que ingresas a Internet para comprar, los comercios virtuales te avisan de que vas a entrar en un servidor seguro y podrás comprobarlo cuando en la parte superior de tu navegador la dirección empieza por https. Esa "s" indica servidor seguro. A partir de ese momento, has entrado en una página protegida por SSL o por SET. Los protocolos SSL y SET son medios de encriptación de datos. Es decir, una vez entregados tus datos, nadie podrá interceptarlos, copiarlos o modificarlos.

SSL (Secure Sockets Layer): es un protocolo de propósito general para establecer comunicaciones seguras, propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Hoy constituye la solución de seguridad implantada en la mayoría de los servidores web que ofrecen servicios de comercio electrónico. Para pagar, el usuario debe rellenar un formulario con sus datos personales (tanto para el caso del envío de los bienes comprados, como para comprobar la veracidad de la información de pago), y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago y el comerciante ya se ocupará manualmente de gestionar con su banco las compras. El canal seguro lo proporciona SSL. Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura (debido a que los navegadores utilizan 40 bits de longitud de clave, protección muy fácil de romper). SSL deja de lado demasiados aspectos para considerarse la solución definitiva y esto porque:

- Sólo protege transacciones entre dos puntos (el servidor web comercial y el navegador del comprador). Sin embargo, una operación de pago con tarjeta de crédito involucra como mínimo tres partes: el consumidor, el comerciante y el emisor de tarjetas.

- No protege al comprador del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta.
- Los comerciantes corren el riesgo de que el número de tarjeta de un cliente sea fraudulento o que ésta no haya sido aprobada.

El estándar SET (Secure Electronic Transaction): fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de gigantes de la industria del software, como Microsoft, IBM y Netscape, con la finalidad de superar los inconvenientes y limitaciones anteriores.

La gran ventaja de este protocolo es que ofrece autenticación de todas las partes implicadas (el cliente, el comerciante y los bancos, emisor y adquiriente); confidencialidad e integridad, gracias a técnicas criptográficas robustas, que impiden que el comerciante acceda a la información de pago (eliminando así su potencial de fraude) y que el banco acceda a la información de los pedidos (previniendo que confeccione perfiles de compra); y sobre todo la gestión del pago, ya que SET gestiona tareas asociadas a la actividad comercial de gran importancia, como registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

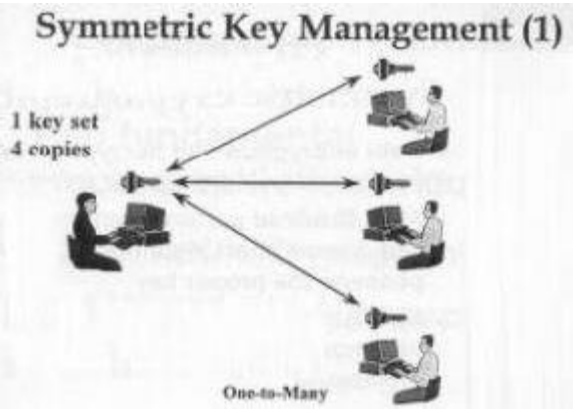
Entonces, si todo son alabanzas, ventajas y puntos fuertes, ¿por qué SET no termina de implantarse? ¿Por qué no goza de la popularidad de SSL, si se supone mejor adaptado? En primer lugar, su despliegue está siendo muy lento. Exige software especial, tanto para el comprador (aplicación de monedero electrónico) como para el comerciante (aplicación POST o terminal de punto de venta), que se está desarrollando con lentitud. En segundo lugar, aunque varios productos cumplan con el estándar SET, esto no significa necesariamente que sean compatibles. Este es un problema que exige mayores esfuerzos de coordinación y más pruebas a escala mundial para asegurar la interoperabilidad. Sus puntos fuertes son también su talón de Aquiles: la autenticación de todas las partes exige rígidas jerarquías de certificación, ya que tanto los clientes como comerciantes

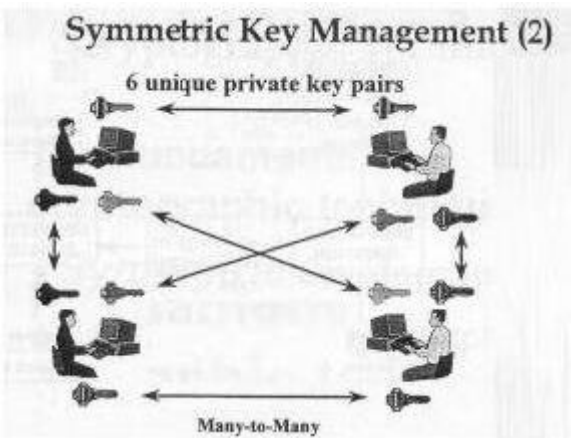
deben adquirir certificados distintos para cada tipo de tarjeta de crédito, trámites que resultan engorrosos, cuando no esotéricos, para la mayoría de los usuarios.

En definitiva, SET es un elefante de gran tamaño y fuerza, pero de movimientos extraordinariamente pesados. SSL es una liebre que le ha tomado la delantera hace años. No es tan perfecto, no ofrece su seguridad ni sus garantías, pero funciona.

TÉCNICAS CRIPTOGRÁFICAS

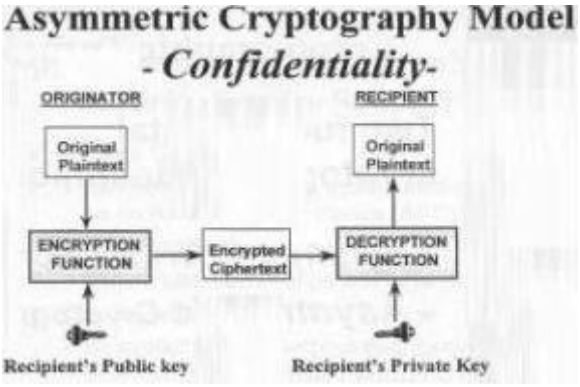
Como hemos visto en un capítulo anterior, existen dos técnicas criptográficas básicas. **La Criptografía *Simétrica* y la Criptografía *Asimétrica*.**

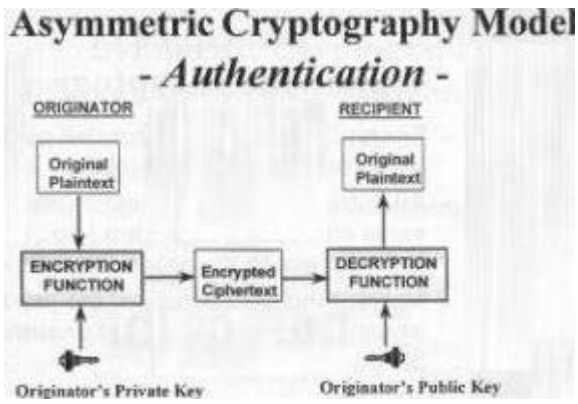




La *Criptografía Simétrica* está basada en la encriptación y decriptación de datos utilizando la misma llave. Todas las partes autorizadas deberán utilizar el mismo algoritmo de encriptación y poseer la misma llave. El control de accesos puede ser garantizado por una tercera parte, que puede ser un Centro de Control de Accesos (ACC por sus siglas en inglés). La ventaja es la de tener un rápido proceso de encriptado/desencriptado, y es una tecnología fácil de comprender y utilizar. La gran desventaja que existe al utilizar este método de encriptación, es la de que mucha gente olvida su password,

haciendo así ilegible todo mensaje cifrado que le llegue. Para evitar la pérdida de esta información, existe una entidad llamada Autoridad de Certificación (CA por sus siglas en inglés), que tendrá la responsabilidad de contar con un mecanismo de recuperación. Este debe contar con altísimas medidas de seguridad, de tal modo que pueda garantizar que las llaves privadas no serán utilizadas por otras personas. Además, debe existir mucha confianza entre esta autoridad y los usuarios, de tal manera que confiemos
plenamente que el usuario que utiliza una llave autorizada por la CA, es quien dice ser.





La *Criptografía Asimétrica* está basada en la encriptación y desencriptación utilizando dos llaves diferentes (pero relacionadas entre sí).

Todas las partes autorizadas deberán utilizar el mismo algoritmo de encriptación, por ejemplo el Rivest, Shamir, Adleman (RSA); y tener acceso a las llaves. Las llaves privadas deben ser distribuidas de manera segura a individuos específicos. Las llaves privadas de autenticación deben ser generadas localmente y nunca ser reveladas a alguien. Las llaves públicas deben ser fácilmente obtenibles. Su integridad debe ser mantenida todo el tiempo. La autenticidad de la llave pública debe ser verificable, y pueden ser revocadas. Sus ventajas son la de ser una tecnología conocida y muy bien comprendida, soporta todos los requisitos de servicios de seguridad. La desventaja es la de tener un proceso sobrecargado de encriptación/decriptación.

COMBINANDO LAS MEJORES PROPIEDADES

Dado que la velocidad de encriptación/desencriptación de la encriptación simétrica es mucho más veloz que la de encriptación asimétrica, es preferible utilizar ambos. Teniendo los datos listos para enviar, estos son encriptados, y luego firmados con la llave privada del autor. Son nuevamente encriptados y nuevamente firmados con una llave simétrica de un solo uso, y nuevamente encriptado utilizando la llave pública del destinatario. El proceso de desencriptado es hecho a la inversa, y de esta manera tenemos una manera segura y confiable de asegurar que los datos recibidos son de quien dice ser.

Debemos mencionar que los procesos de firma y cifrado se hacen de manera independiente. Podemos hacerlo de manera conjunta o separada. Además, todos los procesos son hechos de manera automática por nuestro sistema, no teniendo nosotros que preocuparnos de verificar los certificados uno por uno, sino que el sistema lo hará automáticamente.


Combining the Best Properties
Message
Plain Text
Generation
Generate
Hash Over Plain Text
Sign
Hash
Originator's Private Signing Key
Encrypt
Cipher Text
Message
One Time Symmetric Key
Encrypt
One Time Symmetric Key
Recipient's Public Encryption Key
Send
Receive
Verify
Signature
Re-Generate
Hash Over Plain Text
Decrypt
Hash
Originator's Public Verification Key
Decrypt
Cipher Text
Message
One Time Symmetric Key
Decrypt
One Time Symmetric Key
Recipient's Private Decryption Key

AMENAZAS A LA SEGURIDAD Y SOLUCIONES

Amenaza	Seguridad y solución	Función	Tecnología
Datos interceptados, leídos o modificados ilícitamente.	Encriptamiento	Los datos se codifican para evitar su alteración.	Encriptamiento simétrico y asimétrico.
Los usuarios asumen otra identidad para cometer un fraude.	Autentificación	Verifica la identidad del receptor y emisor.	Firmas digitales.
Un usuario no autorizado en una red obtiene acceso a otra red	Firewall	Filtra y evita que cierto tráfico ingrese a la red o servidor.	Firewall; redes virtuales privadas.

ESTANDARES DE SEGURIDAD PARA INTERNET

Estándar	Función	Aplicación
Secure HTTP (S-HTTP)	Asegura las transacciones en el web.	Exploradores, servidores web, aplicaciones para Internet.
Secure Sockets Layer (SSL)	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones p/ Internet
Secure MIME (S/MIME).	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electrónico con encriptamiento RSA y firma digital.
Secure Wide-Area Nets (S/WAN)	Encriptamiento punto a punto entre cortafuegos y enrutadores.	Redes virtuales privadas.
Secure Electronic Transaction (SET)	Asegura las transacciones con tarjeta de crédito.	Tarjetas inteligentes, servidores de transacción, comercio electrónico.

3.2 Certificados Digitales

Es la **Certificación Electrónica** que vincula unos datos de verificación de firma a un signatario y **confirman su identidad.**

El Certificado Digital es un conjunto de datos a prueba de falsificación protegidos por una contraseña y con validez de un año o más. Se almacena en la base de datos del navegador de Internet o en otro tipo de dispositivo de almacenamiento, permitiendo la transferencia segura de información a través de redes abiertas como Internet.

Características del Producto:

- El cifrado y la firma digital que un certificado nos permite, se debe a que está basado en Criptografía Asimétrica la cual trabaja con un par de claves que se generan al momento de descargar un certificado.
- La clave pública: aquella que se difunde al resto de los usuarios para poder verificar la firma de un texto o cifrar mensajes.
- La clave privada: utilizada por el usuario para poder descifrar mensajes recibidos o para firmar digitalmente.

¿QUIÉN EMITE LOS CERTIFICADOS?

- **ACE** (Agencia de Certificación Electrónica), es la Autoridad de Certificación (CA) que emitirá los certificados una vez que los datos proporcionados hayan sido verificados por la Autoridad de registro designada (Por ej. Telefónica Data).
- **VeriSign** es aquella que suministra servicios de seguridad electrónica en Internet, tiene una red global de afiliados.
- **Cosapi Soft,** otorga certificados SSL y de usuario
- **Qnet/GMD,** ofrece certificados SSL pero sólo si la solución lo requiere.

- **IDCert,** otorga certificados SSL y de usuario y presta servicio de timestamp.
- **ATM Technology,** representante de IDENTIDATA otorga sólo un tipo de certificado. 1certificado, 1 lectora, tarjeta inteligente y sw de instalación.

Dependiendo del navegador que utilice el comprador puede comprobar que se encuentra en un ambiente seguro. Si está usando Explorer, le aparecerá un candado en la parte inferior de la barra de información. Si está usando Netscape, el candado en la parte de herramientas se activará.

CONCLUSIONES Y RECOMENDACIONES

- El impacto que está generando el uso de comercio electrónico y que generará es arrollador, tanto en las empresas como en la sociedad en su conjunto.

- Es necesario tener definido un marco jurídico para las operaciones que se realizan en un ambiente de comercio electrónico.

- Por falta de una normatividad jurídica, operativa, técnica se pueden estar presentando problemas de evasión de pago de impuestos al no cumplirse el ciclo completo de la transacción con la entrega de la factura al comprador.

- A pesar de que aún quedan temas abiertos por resolver (marco jurídico, seguridad, tecnológico), el comercio electrónico ya está en marcha y además de forma acelerada.

- Esta nueva tecnología está adquiriendo gran importancia debido a que las empresas están teniendo una presencia electrónica básica sobre la red global abierta, aprendiendo de la experiencia, siendo gradualmente más sofisticada en el uso que hacen de las tecnologías.

- Se debe recalcar que los sectores o niveles básicos de comercio electrónico ya están bien establecidos y soportados en soluciones normalizadas, a pesar de que los niveles más avanzados de comercio electrónico enfrentan aún retos sustanciales.

- Las instituciones bancarias son las que han realizado mayor avance en comercio electrónico con la implantación de sus operaciones bancarias por medio de internet, preocupándose con prioridad en el tema de seguridad y privacidad de la información.

ANEXOS

Glosario

Abonado. Persona natural o jurídica que tiene derecho al uso permanente de un servicio de telecomunicaciones mediante el pago de una suscripción periódica.

Ancho de banda: Capacidad de un medio para transportar archivos y mensajes. En general se trata de la capacidad que posee un medio para transmitir una señal. Habitualmente se mide en kilobits por segundo (Kbps) o megabits por segundo (Mbps).

Arancel ad Valorem: Tarifa o tasa que se paga como porcentaje del Valor CIF de una importación para que el producto adquiera el derecho de internamiento en el país.

BIT (Binary Digit): Es un número de un solo dígito en base 2. Es decir, es el 1 ó 0. Es la unidad más pequeña de información computarizada. El ancho de banda generalmente se mide en bits por segundo.

BPS (Bits por segundo): Es la medida de cuan rápido se mueve la información de un lugar a otro.

BYTE: Es un conjunto de bits que representan un solo carácter. Usualmente existen 8 bits en un byte, algunas veces más, dependiendo como se esté midiendo.

Ciberespacio (Cyberspace): Este término sirve para describir todos los rangos y recursos de información disponibles a través de redes de computadoras.

Correo electrónico: Son mensajes, usualmente textos, que se envían de una persona a otra, vía computadora conectada a una red. El correo electrónico puede ser mandado a un gran número de direcciones en forma simultánea.

Digitalización: Conversión a partir de la tecnología analógica, que se basa sobre la variación continua de la señal, a otra tecnología en la que la señal es representada por su presencia (unos) o ausencia (ceros) en forma de bits. La digitalización permite a los sistemas de comunicaciones interactuar directamente con los ordenadores y en otros equipos y software. En los últimos años, también la radio y la televisión digitalizan sus señales, abriendo la posibilidad de convergencia de estos medios con la informática y las comunicaciones.

Gigabyte (Gb): 1024 megabytes. Equivalente a 1,073,741,824 bytes.

Hardware: Circuitos electrónicos y dispositivos electromagnéticos que constituyen el sistema de computación. Corresponde a este término cualquier parte física de

un sistema de cómputo tal como circuitos integrados, impresora, teclado, monitor, disquetera, etc.

Hipertexto (Hipertext): Es generalmente cualquier texto que tienen vínculos a otros documentos, como palabras y frases que pueden ser escogidas por un lector y que pueden causar que otro documento pueda ser traído y expuesto.

HOST (Anfitrión): Es cualquier computadora o red de computadoras que son depositarias de servicios disponibles a otras computadoras en la red.

HTTP (Hyper Text Transfer Protocol): Es el protocolo para mover archivos de hipertexto a través de Internet. Para su uso, se requiere un programa cliente HTTP en un lado, y un programa servidor HTTP en otro lado. Actualmente en la WWW, el HTTP es el protocolo que más se usa.

Infovía: Es una vía de acceso universal, sencilla y económica para que una computadora personal o estación de trabajo pueda acceder a un servidor que le proporcione servicios de información.

INMARSAT: Servicio de comunicaciones, de datos y/o telefonía, vía satélite.

INTERNET: Se refiere a la vasta colección de redes de computadoras conectadas a nivel mundial.

IP Number (Internet Protocol Number): Llamado muchas veces una cuadrícula punteada. Es un número único que consiste en cuatro partes separadas por puntos.
Cada computadora que está en Internet tiene un número IP.

MAINFRAME: Computadora grande. Computadora con enorme memoria RAM, disco duro de alta capacidad de almacenamiento y gran velocidad de procesamiento.

RED: Cada vez que dos computadoras se conectan entre sí, se convierte en una red. Cada vez que tres redes se conectan entre sí, tenemos Internet.

VIRUS: Cualquier tipo de programa que interrumpe la secuencia normal de trabajo de la computadora.

WWW (Word Wide Web): Es el universo de servidores de hipertexto (HTTP) que permiten observar al usuario texto, gráficos, archivos de sonido, etc., y que se pueden combinar.

Business to Consumer (B2C): Negocios para el consumidor

Business to Business (B2B): Negocio entre empresas.

Mensajes de datos: Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

Emisor: Persona, natural o jurídica, pública o privada, que origina un Mensaje de Datos por sí mismo, o a través de terceros autorizados..

Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido utilizado.

Signatario: Es la persona, natural o jurídica, publica o privada, titular de una Firma Electrónica o Certificado Electrónico.

Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.

Destinatario: Persona natural o jurídica a quien va dirigido el Mensaje de Datos.

Proveedor de Servicios de Certificación: Persona legalmente facultada para proporcionar Certificados Electrónicos.

Sistema de Información: Aquel utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma Mensajes de Datos.

Usuario: Toda persona que utilice un sistema de información.

Quiebra técnica: Es la incapacidad temporal o permanente del Proveedor de Servicios de Certificación que impida garantizar el cumplimiento de sus servicios, así como, con los requisitos y condiciones establecidos en esta Ley para el ejercicio de sus actividades.

FUENTES DE INFORMACIÓN

LIBROS

SCHULTZ, Eugene. SHUMWAY, Russell. Incident Response: A strategic guide to handling System and Network Security Breaches. New Riders. First Edition. November, 2001. ISBN 1-57870-256-9. *www.newriders.com*

TIPTON, Harold. KRAUSE, Micki. EDITORS. Information Security Management Handbook. Auerbach. Fourth Edition. 2000. ISBN 1-8493-9829-0. *www.auerbach-publications.com*

MINOLI, Daniel. MINOLI, Emma. Web Commerce Technology Handbook. McGraw-Hill Series on Computer Communications. 1998. ISBN 0-07-042978-2. *www.computing.mcgraw-hill.com*

MERKOW, Mark. BREITHAUPT, Jim. WHELEER, Ken. Building Set Applications for Secure Transactions. Wiley Computer Publishing. 1998. ISBN 0-471-28305-3. *www.wiley.com/compbooks/*

KLEVINSKY, T.J. LALIBERTE, Scott. GUPTA, Ajay. Hack I.T. – Security Through Penetration Testing. Addison Wesley. 2002. ISBN 0-201-71965-8. *www.aw.com*

BICKERTON, Pauline. BICKERTON, Matthew. SIMPSON-HOLLEY, Kate. Trad. Jorge
Toraya. Ciberestrategia. Prentice Hall.

MALCA, Oscar. Universidad del Pacífico

RAMIÓ AGUIRRE, Jorge. Seguridad Informática y Criptografía. Universidad Politécnica de Madrid. Tercera Edición. Marzo 2003. ISBN 84-86451-69-8.

Documento de libre distribución en Internet. *www.criptored.upm.es*

MATÍAS, Gustavo. RAMÍREZ, Patricio. SANZ, José. E-comercio Seguro. Grupo Negocio, Editores Asociados I+D. Libro III

ENTREVISTAS

ANGEL, José de Jesús. Magíster en Ciencias. Seguridata. México. Entrevista vía email.

REVISTAS Y PUBLICACIONES

Communications of ACM. Vol.46, num. 5. May 2003

Communications of ACM. Vol.46. num. 8.. Aug. 2003

Revista Perspectiva Nº5. Seguridad. Publicación virtual. *www.microsoft.com/spain/enterprise/perspectivas/numero_5*

INTERNET

Common Criteria. *http://commoncriteria.org/cc/cc.html*

Programa de Doctorado en Ingeniería Telemática. Curso: Seguridad en Internet. Prof.: Jordi Forné.
http://www-mat.upc.es/~jforne/seguridad_internet.html

Red Temática Iberoamericana de Criptografía y Seguridad de la Información
http://www.cfbsoft.iespana.es/cfbsoft/seguridad/tesis.htm

VirusProt. *www.virusprot.com*

Red Temática Iberoamericana de Criptografía y Seguridad de la Información.
www.criptored.upm.es