

UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE ESPECIALIDADES EMPRESARIALES

CARRERA TECNICO SUPERIOR ELECTRONICO EN COMPUTACION

PRESENTACIÓN DEL TEMA DE TESIS DE GRADO:

SEGURIDAD DE LA INFORMACION EN E-COMMERCE

ELABORADO POR:

VICTOR DANIEL SANZ ZAMBRANO

AÑO LECTIVO

2009 - 2010

	Página No.
INDICE DE CONTENIDO	2
<u>CAPITULO I</u>	5
<u>DEFINICION DEL PROBLEMA</u>	5
I.1 Presentación Del Problema	5
I.2 Propósito Del Estudio	6
<u>CAPITULO II</u>	7
<u>MARCO TEORICO</u>	7
II.1 Seguridad	7
II.1.1 Seguridad Lógica	7
II.1.1.1 Controles De Acceso	8
II.1.2 Seguridad Organizacional/Operacional	14
II.1.2.1 Recuperación De Desastres	15
II.1.2.2 Seguridad Física	33
II.1.2.3 Forénsica	48
II.1.2.4 Educación y Documentación	

II.1.3 Criptología	53
II.1.3.1 Cifrado Simétrico	54
II.1.3.2 Cifrado Asimétrico	62
II.1.3.3 Criptografía De Resumen	65
II.1.3.4 Firma Digital	69
II.1.3.5 Certificados Digitales	72
II.1.3.6 PKI (Public Key infraestructure)	73
II.1.4 seguridad en comunicaciones	75
II.1.4.1 OSI VS TCP/IP	76
II.1.4.2 Seguridad a nivel de aplicación	78
II.1.4.3 seguridad a nivel de transporte	79
II.1.4.4 seguridad a nivel de red	80
II.1.5 seguridad en infraestructura	81
II.1.5.1 Filtros	81
II.1.5.2 Sistemas De Dirección De Intrusos (IDS)	84
II.1.6 Niveles De Seguridad Informática	84
II.2 Comercio Electrónico (E-COMMERCE)	95
II.3 Marco Legal.	101
II.1.3.1 Consideraciones Jurídicas En Internet.	101
II.1.3.2 Ley de Comercio electrónico, Firmas y Mensajes De Datos.	106
II.1.3.2.1 Título Preliminar.	107
II.1.3.2.2 De Los Mensajes De Datos (principios generales).	107
II.1.3.2.3 De Las Firmas Electrónicas.	112
II.1.3.2.4 De Los Certificados De Firmas Electrónicas.	115
II.1.3.2.5 De Las Entidades De Certificación De Información.	119

II.1.3.2.6 De Los Organismos De Promoción y Difusión De Los Servicios Electrónicos y De Regulación y Control De las Entidades De Certificación Acreditadas.	122
II.1.3.2.7 De Los Servicios Electrónicos.	127
II.1.3.2.8 De La Contratación Electrónica y Telemática.	128
II.1.3.2.9 De Los Derechos a Los Usuarios o Consumidores De De servicios Electrónicos.	129
II.1.3.2.10 De Los Instrumentos Públicos.	132
II.1.3.2.11 De La Prueba y Notificaciones Electrónicas.	132
II.1.3.2.12 De las Infracciones Informáticas	135
II.1.3.3 Disposiciones Generales.	139
II.1.3.4 Disposiciones Transitorias	143
II.1.3.5 Disposición Final	144
II.1.3.6 Reglamento General a la Ley De Comercio Electrónico, firmas Electrónicas y mensajes de datos.	145
<u>CAPITULO III</u>	160
<u>APLICACIÓN</u>	160
Construyendo Una Infraestructura Confiable De E-Commerce.	160
III.1 Seguridad En El Comercio Electrónico	161
III.2 Certificados Digitales	177
Fuentes de Información.	179

CAPITULO I

DEFINICION DEL PROBLEMA

PRESENTACION DEL PROBLEMA

El crecimiento de la tecnología en los últimos años, ha generado avances y cambios en todos los aspectos. La evolución de Internet ha sido uno de estos grandes cambios. Internet ha influido en nuestras vidas y en nuestras costumbres, en nuestra forma de buscar información, de entretenernos, de comunicarnos y por supuesto han aparecido nuevas formas de comprar y vender bienes.

Estos cambios traen grandes beneficios, por ejemplo hoy en día las personas se comunican desde dos puntos muy distantes del planeta, ya sea a través del teléfono o de algunos de los medios que ofrece Internet; así mismo, las empresas han encontrado grandes oportunidades en los desarrollos de las comunicaciones, destacando que los costos de las comunicaciones se reducen y que estas tecnologías están al alcance tanto de grandes empresas como de pequeñas empresas. Internet ha iniciado una revolución tanto o más grande que la industrial y no podemos quedarnos atrás a los cambios que se han venido dando, esto incluye en hacer negocios. Sin embargo, en nuestro medio, los usuarios finales no disponen de información clara de cómo involucrarse en esta revolución de manera segura. No existe una guía para la selección de una solución de seguridad.

La seguridad en el comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia. Para ello es necesario disponer de un servidor seguro a través del cual toda la información confidencial es *encriptada* y viaja de forma segura, ésto brinda confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocios. El usuario final en nuestro medio no dispone de información del entorno que gira alrededor del tema de E-commerce (comercio electrónico) , ni tampoco de

criterios para decidir cuándo debe aplicar seguridad del tipo de firmas digitales, u otros tipos de seguridad.

PROPÓSITO DEL ESTUDIO

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

Asimismo, dar a conocer los elementos involucrados en el tema de comercio electrónico.

CAPITULO II

MARCO TEORICO

II.1SEGURIDAD

II.1.1 Seguridad Lógica

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe de estar prohibido” y eso es lo que debe asegurar la seguridad lógica, Podemos pensar en la seguridad lógica como la manera de aplicar procedimientos Que aseguren que solo podrán tener acceso a los datos las personas o sistemas de información autorizadas 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 solo por el destinatario al cual ha sido dirigida y por ningún otro.
5. Asegura 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.

II.1.1.1 Controles De Acceso

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

Estos controles 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 protegida la información (restringiendo la cantidad de usuarios y procesos con autorización de acceso) y para resguardar la autorización confidencial de accesos no autorizados.

Las consideraciones relacionadas al procedimiento 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 autenticación

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 caso 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 **Autenticación** es la verificación que realiza el sistema de 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 son 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 un manera bastante efectiva de implementar el control de accesos, siempre que el proceso de definición de roles este 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 numero de cuenta que proporciona 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 más 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 de este tipo de control es:

Cuando 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.

(Todo lleva un límite de tiempo)

Otro ejemplo podría ser cuando los usuarios de una red, tienen permitido intercambiar emails entre si, pero no tienen permitido conectarse para intercambiar emails 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 puedan 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 que 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 ese 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) pueden o no hacer con los recursos del sistema. Se detallaran cinco métodos de control de acceso interno:

Palabras claves (passwords)

Las palabras clave o passwords, están comúnmente asociadas con la autenticación del usuario, pero también son usadas para proteger datos, aplicaciones e incluso PC's.

Por ejemplo, en caso de aquel que 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 poseen la clave apropiada. La criptología es un tema cuya amplitud será tratada en un subcapítulo aparte.

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 Interface 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 interface de usuario.

Los límites sobre la interface 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 interface 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.

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.

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.

Un ejemplo de autenticación basada en Host es el *Network File System (NFS)* que permite a un servidor poner a disposición de un grupo específico de computadoras determinados sistemas y/o directorios.

II.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

II.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.

Los sismos son perturbaciones súbitas en el interior de la tierra que dan origen a vibraciones o movimientos del suelo; la causa principal y responsable de la mayoría de los sismos (grandes y pequeños) es la ruptura y fracturamiento de las rocas en las capas más exteriores de la tierra.

Como resultado d un proceso gradual de acumulación de energía debido a los fenómenos geológicos que deforman la superficie de la tierra, dando lugar a las grandes cadenas montañosas.

En el interior de la tierra ocurre un fracturamiento súbito cuando la energía acumulada excede la resistencia de las rocas. Al ocurrir la ruptura, se propagan (en el interior de la tierra) una serie de ondas sísmicas que al llegar a la superficie sentimos como un temblor.

Generalmente, los sismos ocurren en zonas de debilidad de la corteza terrestre que llamamos fallas geológicas. Existen también sismos menos frecuentes causados por la actividad volcánica en el interior de la tierra, y temblores artificiales ocasionados por la detonación de explosivos.

El sitio donde se inicia la ruptura se llama foco y su proyección en la superficie de la tierra, epicentro.

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 sísmo resistente propio 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

JUNTA PROVINCIAL DE SEGURIDAD CIUDADANA Y DEFENSA CIVIL DEL GUAYAS

<http://www.defensacivilgye.50megs.com/dcgye.htm>

Maremotos

Tsunami (del japonés *tsu*, «puerto» o «bahía», y *nami*, «ola»; literalmente significa *gran ola en el puerto*) es una ola o un grupo de olas de gran energía y tamaño que se producen cuando algún fenómeno extraordinario desplaza verticalmente una gran masa de agua.

Se calcula que el 90% de estos fenómenos son provocados por terremotos, en cuyo caso reciben el nombre, más preciso, de *maremotos tectónicos*. La energía de un tsunami depende de su altura (amplitud de la onda) y de su velocidad.

La energía total descargada sobre una zona costera también dependerá de la cantidad de picos que lleve el tren de ondas (en el reciente maremoto del Océano

Índico hubo 7 picos). Este tipo de olas remueven una cantidad de agua muy superior a las olas superficiales producidas por el viento.

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 arrojado 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 de energía en un intervalo temporal ínfimo. De esta forma, la potencia de la explosión es proporcional al tiempo requerido. Los órdenes de magnitud rondan los gigawatts. Los orígenes de las explosiones se suelen dividir en dos clases:

- Físicos: mecánicos (choques de móviles), electromagnéticos (relámpagos) o neumáticos (presiones y gases).
- Químicos: de reacciones de cinética rápida.

Una explosión causa ondas de presión en los alrededores donde se produce. Las explosiones se pueden categorizar según si las ondas son subsónicas y

detonaciones si son supersónicas (ondas de choque). Estas velocidades deben considerarse respecto del medio de propagación (el explosivo).

El efecto destructivo de una explosión es precisamente por la potencia de la detonación que produce ondas de choque o diferencias de presión subyacentes de duración muy corta, extremadamente bruscas.

JUNTA PROVINCIAL DE SEGURIDAD CIUDADANA Y DEFENSA CIVIL DEL GUAYAS

<http://www.defensacivilgve.50megs.com/dcgve.htm>

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

Una **inundación** es la ocupación por parte del agua de zonas que habitualmente están libres de ésta, bien por desbordamiento de ríos y ramblas, por subida de las mareas por encima del nivel habitual o por avalanchas causadas por tsunamis.

Las inundaciones fluviales son procesos naturales que se han producido periódicamente y que han sido la causa de la formación de las llanuras en los valles de los ríos, tierras fértiles donde tradicionalmente se ha desarrollado la agricultura en vegas y riberas.

En las zonas costeras los embates del mar han servido para modelar las costas y crear zonas pantanosas como albuferas y lagunas que, tras su ocupación atópica, se han convertido en zonas vulnerables.

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

Un **incendio** es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse. Puede afectar a estructuras y a seres vivos. La exposición a un incendio puede producir la muerte, generalmente por inhalación de humo o por desvanecimiento producido por la intoxicación y posteriormente quemaduras graves. Para que se inicie un fuego es necesario que se den conjuntamente estos tres factores: combustible, oxígeno y calor o energía de activación.

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 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 (CO₂) 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 (CO₂) 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.” 5 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 18° 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

Tesis “Seguridad Informática: Sus implicancias e implementación”. Cristian Borghello 2001 <http://www.segu-info.com.ar/>

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 más que perder, ya sea en imagen o prestigio, no se da publicidad a este tipo de situaciones.

Sabotaje

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

1. Fraudes cometidos mediante manipulación de computadoras
 - Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
 - La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
 - Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude

del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.

2. Manipulación de los datos de entrada

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3. Daños o modificaciones de programas o datos computarizados

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- Acceso no autorizado a servicios y sistemas informáticos: estos accesos se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
- Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas

informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información.

Ellas son:

- "Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos."

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 más duros, el saboteador puede ser un empleado o un sujeto ajeno a la empresa y sus motivos pueden ser de lo más variados.

Al estar más familiarizados con las aplicaciones, los empleados saben que acciones causarían más 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 más 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 engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

Infracción del Copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan «downloads» de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

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

En informática, un **hacker** es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:

- Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("*Black hats*"). Pero también incluye a aquellos que depuran y arreglan errores en los sistemas ("*White hats*") y a los de moral ambigua como son los "*Grey hats*".
- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT.² Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de hackers.³ El RFC 1392⁴ amplía este significado como "*persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas*".
- La comunidad de aficionados a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de ordenador, crackeo de software, la demoscene) de entre los ochenta/noventa.

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980. A los criminales se le pueden sumar los llamados "*script kiddies*", gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre como funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los hackers aficionados reconocen los tres tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "*crackers*" (analogía de "*safecracker*", que en español se traduce como "*un ladrón de cajas fuertes*").

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.

Worm: 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.

II.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

Uno de los factores críticos a la hora de gestionar la seguridad de la información en las organizaciones, es el factor humano.

Aún así, es frecuente observar cómo, por norma general, los esfuerzos de seguridad técnica suelen ser muy considerados, pero sin embargo, la seguridad del factor humano a veces es menospreciada o en el peor de los casos, pasada por alto.

En éstos casos, hablamos del enemigo que está dentro, bien sea por la intencionalidad de sus actos, bien sea por negligencia en el tratamiento de los activos de la información.

Si nos ceñimos al marco normativo más reconocido, el que nos ofrece ISO 17799:2000, hay varios puntos de control que tienen que ver con el factor humano. Además de la seguridad física y del entorno, el punto de control principal viene reflejado claramente en lo que se suele denominar seguridad ligada al personal.

La idea de controlar al personal no está relacionada con la restricción de la libertad y la comodidad de los empleados en las organizaciones: se trata de imponer puntos de control en el factor humano que opera con la información, de modo que se eviten fugas de información, errores en el manejo de datos, brechas en la confidencialidad y que la protección de aspectos importantes, como los secretos industriales y el "know-how" de los negocios, sea una realidad no sujeta a posibles fisuras causadas por el espionaje industrial o la competencia desleal.

En las labores de consultoría de seguridad es frecuente que se realicen muchos trabajos para definir radiográficamente la situación de una empresa determinada en cuanto a la robustez de su infraestructura técnica. Los análisis generales, las auditorías perimetrales, los test de intrusión, la analítica forense y otros tipos de pruebas son muy útiles para saber si las puertas de entrada aguantarán los golpes de los arietes, o si la cerradura será suficientemente segura para que ninguna ganzúa pueda abrirla. Es el enfoque tradicional de seguridad ante los ataques de fuerza bruta y ante los intentos de intrusión sigilosos y técnicamente depurados, metodologías de ataque que aunque pueden actuar por separado, normalmente, suelen ir de la mano.

Llegados a este punto, sería conveniente plantearnos un paso más allá de la seguridad tradicional basada en las pruebas técnicas. Según lo que se plantea,

abordar las cuestiones de seguridad relativas al personal parece una medida muy interesante, ya que a fin de cuentas, el hardware y el software está operado, supervisado y administrado por usuarios. En otra ocasión, desde Hispasec Sistemas, hemos hablado de la gestión del riesgo. Hoy complementaremos esa información con las nociones elementales de la seguridad ligada al personal.

La seguridad ligada al personal debe ser meticulosamente planificada. El tratamiento de las medidas de control, aplicadas a seres humanos, requiere tacto y requiere tener en cuenta que cada empleado tiene sus propias determinaciones y condiciones laborales. Aún así, es posible planificar la seguridad del personal como un conjunto de medidas de control general, que hagan que éstas sean efectivas independientemente del sujeto afecto, y sin que éstas medidas supongan un menoscabo de los derechos y el confort de los trabajadores

Las principales medidas de control que se suelen recomendar son las siguientes: Reducción del riesgo del factor humano, debido a errores, pérdidas, robos y usos indebidos de la información. Los acuerdos de confidencialidad, la selección rigurosa del personal y la inclusión de la seguridad dentro de las responsabilidades contractuales son buenas prácticas aconsejables en este punto. Concienciación del personal en cuanto a política de seguridad y medidas que deben contemplar para evitar riesgos. La única manera de propagar la esencia de la gestión de la seguridad es que el personal conozca los riesgos y sus consecuencias, con lo que la empresa debe invertir en la formación sobre los principios básicos de gestión segura de la información.

Minimización de las consecuencias de los incidentes provocados por el factor humano, tomando el error como fuente de aprendizaje para la prevención de futuros problemas. El error es una importante fuente de retroalimentación que puede permitir que en futuras repeticiones de una problemática hayamos aprendido a minimizar los impactos. Es imperativo ajustar y dar a conocer los

medios de difusión de los incidentes una vez ocurran, de modo que todos los integrantes de la cadena de responsabilidad sepan qué han de hacer y a quién deben informar en todo momento. Cuando exista intencionalidad en el personal infractor, temerario o negligente, es evidente que la empresa debe recurrir a procesos disciplinarios y represalias legales.

Estudio del personal crítico, es decir, del personal que debe cubrir las tareas críticas de la organización cuya importancia es vital para la empresa. Los procesos críticos son más importantes que los procesos de apoyo, luego el personal que debe atenderlos es más importante para la empresa, independientemente que todos los empleados son de importancia vital para las organizaciones.

De esto se deduce claramente que un error o mala intención de un asalariado crítico normalmente será más dañino que un error de un empleado adscrito a un proceso no crítico.

Los consejos, a modo de resumen, que pueden emitirse son de diversa índole. Estos diez consejos, basados en la documentación de la consultora norteamericana Covelight Systems, pueden ser un buen resumen para la amenaza interna de carácter intencionada. Las recomendaciones para la amenaza no intencionada, son obvias: formación de los empleados y políticas de concienciación y aprendizaje.

1. Vigile las cajas que contienen las joyas, no las salidas del edificio. Es decir, céntrese en las medidas y objetivos a priori, y no en las medidas a posteriori. Éstas son secundarias.
2. Sea proactivo. Trate de anticiparse a los movimientos de los posibles infractores.
3. Trate la seguridad con independencia y objetividad.

4. Ordene a los empleados en función a los privilegios a los que pueden acceder. La relación entre riesgo y privilegios de los que se gozan es directamente proporcional.

5. Esté atento al comportamiento sospechoso de los usuarios. Suele ser el primer indicativo de que puede haber en curso un problema de seguridad.

6. No pase por alto lo obvio. La mayoría de las veces, la amenaza interna es relativamente fácil de visualizar. No busque amenazas intrincadas, trate primero de analizar lo evidente.

7. Apóyese en sistemas automatizados de vigilancia. Pueden complementar los resultados de la gestión.

8. Registre toda la actividad crítica, siempre y cuando la legislación y el respeto a los derechos de los trabajadores se lo permita.

9. Informe claramente a los empleados de cuáles son los riesgos y las consecuencias de los mismos. Asegúrese de que la política de seguridad y las condiciones de responsabilidad sean conocidas y practicadas por todos.

10. La seguridad de la información es un concepto amplio y con interrelaciones. Consulte a los responsables de todas las áreas implicadas y establezca los vínculos oportunos.

Poco a poco, las empresas van invirtiendo en una adecuada gestión de la seguridad, pero el camino para que el factor humano sea un factor controlado y seguro es largo y tortuoso. Quizás es buen momento para que usted comience la andadura, si todavía no lo ha hecho.

Existen otras medidas que pueden complementar a estas cuatro medidas generales. No son las únicas, ni tienen por que ser el referente a la hora de

gestionar la seguridad del personal, pero en circunstancias normales, son cuatro conjuntos de factores que deberían ser vigilados estrechamente

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 a eliminarlas, la idea es adicionar barreras para reducir el riesgo en las áreas cubiertas por dichas barreras.

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 deben ser modificados 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 más 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 captadas 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 termo grama, 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.

II.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 forense 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 forensica 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.

II.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 **cómo** 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 más 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 estas razones 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.

II.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 descifrado o descifrado.

El término Criptografía consta de los vocablos griegos *Crypto* : 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.

II.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 descifrado 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 232, 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 232. 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
RJNDAEL	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

Figura II.1

Fuente: Seguridad Informática y Criptografía. Jorge Ramió Aguirre,
Universidad Politécnica de Madrid (1998).

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 : $256 = 7.2 \cdot 1016$, 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 'cifrate' 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 más 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.

II.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 E_k no revela ningún dato acerca de D_k o viceversa
- La clave pública no permite que la otra pueda ser deducida
- Cada usuario dispone del par (E_k, D_k) , donde E_k es pública y D_k es privada
- El mensaje cifrado se obtiene de la siguiente manera: $c_A = \{E_B(m_A)\}$, donde A es el emisor y B el receptor.
- El mensaje original se obtiene o descifra : $m_A = D_B\{E_B(m_A)\}$
- Se verifica además: $m_A = E_B\{D_B(m_A)\}$

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

II.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 recalculan el hash usando la clave pública correspondiente y así verificar la integridad del mensaje.

Función Hash

Mensaje = M Función Resumen = H(M)

Firma: $f = \text{EdE}\{H(M)\}$

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: $EeE(r) = H(M)$

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.

7. *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.

II.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.

II.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 este las norms 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.

II.1.3.6 PKI (Public Key Infrastructure)

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 órdenes de compra.

Internet es uno de los medios más hostiles en el mundo, ya que existen más de 10 millones de usuarios alrededor del, 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:
 - 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

II.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.

II.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

Aplicación		Aplicación
Presentación		
Sesión		
Transporte		TCP
Red		IP
Enlace de Datos		Enlace de Datos y Físico
Físico		

Niveles del Modelo OSI

Niveles TCP/IP

Figura II.2

~ / / ~

II.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

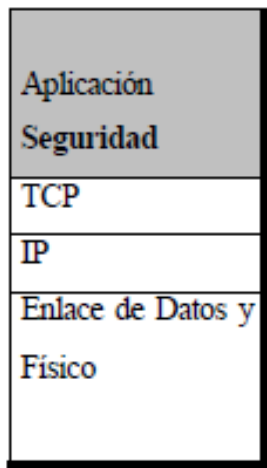


Figura II.3

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

II.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.

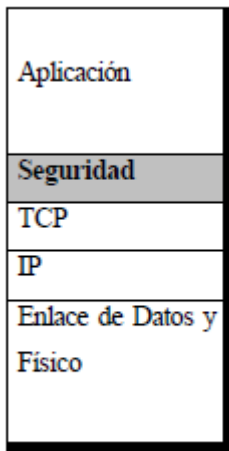


Figura II.4

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.

II.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.

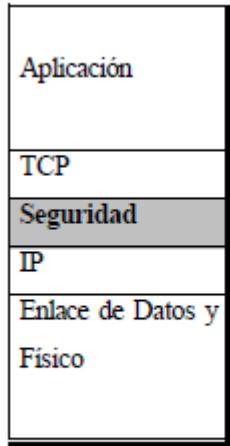


Figura II.5

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.

II.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 otra posible medida de salvaguarda.

II.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 autenticación 'fuerte' del usuario en dos niveles: o El clásico de Identificador + contraseña., poco robusto contra ataques de husmeadores o sniffers. o 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

II.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.

II.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 más 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 <u>información</u> referencial	Como <u>información</u> referencial para definir <u>re</u> querimientos y formular <u>espe-</u> cificaciones de seguridad para TOE's,	Como <u>información</u> 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 <u>inter</u> pretan las <u>decla</u> raciones de <u>reque</u> rimientos y la formulación de especificaciones funcionales de los TOE's	Criterios de <u>eva</u> luación <u>mandato</u> rios para <u>determi</u> nar si un TOE presenta <u>efectiva</u> mente las <u>funcio</u> nes de seguridad que declara.
Parte 3 : Requerimientos de Aseguramiento	Como soporte para determinar los niveles de <u>ase</u> guramiento <u>reque</u> ridos	Como referencia para interpretar requerimientos de <u>aseguramiento</u> y determinar los alcances de <u>ase</u> guramiento de los TOE's	Criterios de <u>eva</u> luación <u>mandato</u> rios para <u>determi</u> nar el <u>asegura</u> miento de los TOE's y para evaluar los PP's y ST's

Figura II.6Fuente: "Common Criteria. An 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 más 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 más 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 mas 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	E0
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 los Mencionados 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.

II.2 COMERCIO ELECTRÓNICO (E-COMMERCE)

Podemos resumir de manera sencilla las siguientes ideas:

COMERCIO = Intercambio con beneficio

ELECTRÓNICO = Utilización de medios informáticos (en el contexto del tema que tratamos)

Desarrollo en Ecuador

Si tomamos en cuenta la definición de correo electrónico, podemos darnos cuenta de que el comercio electrónico está más difundido en Ecuador de lo que suponemos. ¿Cuántas veces te has comunicado por e-mail con un cliente/proveedor?

No contamos con datos estadísticos del comercio electrónico en Ecuador. Lo que sí podemos hacer es medir la cantidad de comunicaciones electrónicas de negocios, cuántas empresas que conoces ya tienen su sitio web, cuántas vallas, tarjetas de presentación incluyen una dirección electrónica. En otras palabras el comercio electrónico ya está entre nosotros a diario.

Seguro que ahora estás pensando en el desarrollo de una transacción completa online. Tenemos en ese caso 2 líneas de trabajo:

- Productos tangibles o servicios que se venden a través de Internet
- Productos “electrónicos” que se venden a través de Internet.

En el caso de la primera línea de trabajo tienes empresas ecuatorianas que realizan ventas online, entre las que se cuentan: universidades, cines, aerolíneas, libros, boletos e incluso licores.

En el segundo caso existen menos evidencias de empresas ecuatorianas, pero podemos indicar el caso de suscripciones electrónicas, publicidad electrónica, venta de software.

En conclusión: el Comercio Electrónico es la consecución de transacciones comerciales, utilizando en todo o en parte del proceso, medios de comunicación electrónica.

Opciones con Black Box Ecuador

El referente que tenemos en otros países de cómo el volumen de transacciones en Internet es cada vez más importante, nos invita a tomar la delantera desarrollando estrategias de comercio electrónico en Ecuador. Black Box Ecuador tiene para su organización:

- Desarrollo de estrategias de comercio electrónico
- Desarrollo de sitios Web
- Implementación del servicio de pedidos online
- Integración con sistemas de comercio electrónico
- Investigaciones para antes y después de vender en línea

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)

- 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

II.3 MARCO LEGAL

II.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, pingping 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

II.1.3.2 Ley de Comercio electrónico, Firmas y Mensajes De Datos.

Ley de comercio electrónico, firmas electrónicas y

Mensajes de datos

(Ley No. 2002-67)

CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la Internet ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

Que se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

Que a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter

civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia;

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales; y, En uso de sus atribuciones, expide la siguiente:

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y

MENSAJES DE DATOS

II.1.3.2.1 Título Preliminar

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Título I

II.1.3.2.2 DE LOS MENSAJES DE DATOS

Capítulo I

PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia,

valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos. Se considera que un mensaje de datos permanece íntegro, si se

mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación. Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Art. 8.- Conservación de los mensajes de datos.- Toda información sometida a esta

Ley, podrá ser conservada; éste requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

- a. Que la información que contenga sea accesible para su posterior consulta;
- b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
- c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
- d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:

- a. Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
- b. Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

- a. Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;
- b. Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información

o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,

c. Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Art. 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

Título II

DE LAS FIRMAS ELECTRÓNICAS, CERTIFICADOS DE FIRMA ELECTRÓNICA, ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN, ORGANISMOS DE PROMOCIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS

Capítulo I

II.1.3.2.3 DE LAS FIRMAS ELECTRÓNICAS

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

- a. Ser individual y estar vinculada exclusivamente a su titular;
- b. Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;
- c. Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.
- d. Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,
- e. Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

- a. Cumplir con las obligaciones derivadas del uso de la firma electrónica;
- b. Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
- c. Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
- d. Verificar la exactitud de sus declaraciones;
- e. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
- f. Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
- g. Las demás señaladas en la Ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

- a. Voluntad de su titular;
- b. Fallecimiento o incapacidad de su titular;
- c. Disolución o liquidación de la persona jurídica, titular de la firma; y,
- d. Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Capítulo II

II.1.3.2.4 DE LOS CERTIFICADOS DE FIRMA ELECTRÓNICA

Art. 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 21.- Uso del certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.

Art. 22.- Requisitos del certificado de firma electrónica.- El certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

- a. Identificación de la entidad de certificación de información;
- b. Domicilio legal de la entidad de certificación de información;
- c. Los datos del titular del certificado que permitan su ubicación e identificación;
- d. El método de verificación de la firma del titular del certificado;
- e. Las fechas de emisión y expiración del certificado;

- f. El número único de serie que identifica el certificado;
- g. La firma electrónica de la entidad de certificación de información;
- h. Las limitaciones o restricciones para los usos del certificado; e,
- i. Los demás señalados en esta ley y los reglamentos.

Art. 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta Ley.

Art. 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica, se extinguen, por las siguientes causas:

- a. Solicitud de su titular;
- b. Extinción de la firma electrónica, de conformidad con lo establecido en el Art. 19 de esta Ley; y,
- c. Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art. 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

- a. Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;
- b. Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
- c. Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley, cuando:

- a. La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,

b. Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada. La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.-

Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta Ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de

normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores

Capítulo III

II.1.3.2.5 DE LAS ENTIDADES DE CERTIFICACIÓN DE INFORMACIÓN

Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

- a. Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones;
- b. Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
- c. Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información;
- d. Mantener sistemas de respaldo de la información relativa a los certificados;

e. Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato de la Superintendencia de Telecomunicaciones, en los casos que se especifiquen en esta ley;

f. Mantener una publicación del estado de los certificados electrónicos emitidos;

g. Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;

h. Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,

i. Las demás establecidas en esta ley y los reglamentos.

Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.-

Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor.

Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar.

Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Art. 34.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.

Art. 35.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

Capítulo IV

II.1.3.2.6 DE LOS ORGANISMOS DE PROMOCIÓN Y DIFUSIÓN DE LOS SERVICIOS ELECTRÓNICOS, Y DE REGULACIÓN Y CONTROL DE LAS ENTIDADES DE CERTIFICACIÓN ACREDITADAS

Art. 36.- Organismo de promoción y difusión.- Para efectos de esta Ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.-

El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas.

En su calidad de organismo de autorización podrá además:

- a. Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;
- b. Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y,
- c. Las demás atribuidas en la ley y en los reglamentos.

Art. 38.- Organismo de control de las entidades de certificación de información acreditadas.- Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Art. 39.- Funciones del organismo de control.- Para el ejercicio de las atribuciones establecidas en esta ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

- a. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas;
- b. Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;

c. Realizar auditorías técnicas a las entidades de certificación de información acreditadas;

d. Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;

e. Imponer de conformidad con la ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;

f. Emitir los informes motivados previstos en esta ley;

g. Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,

h. Las demás atribuidas en la ley y en los reglamentos.

Art. 40.- Infracciones administrativas.- Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,

2. Cualquier otro incumplimiento de las obligaciones impuestas por esta Ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;
4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,
5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

- a. La gravedad de las infracciones cometidas y su reincidencia;
- b. El daño causado o el beneficio reportado al infractor; y,
- c. La repercusión social de las infracciones.

Art. 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

- a. Amonestación escrita;
- b. Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
- c. Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
- d. Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica.

Art. 42.- Medidas cautelares.- En los procedimientos instaurados por infracciones graves, se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Art. 43.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

Título III

II.1.3.2.7 DE LOS SERVICIOS ELECTRÓNICOS, LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PÚBLICOS.

Capítulo I

DE LOS SERVICIOS ELECTRÓNICOS

Art. 44.- Cumplimiento de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rijan, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

Capítulo II

II.1.3.2.8 DE LA CONTRATACIÓN ELECTRÓNICA Y TELEMÁTICA.

Art. 45.- Validez de los contratos electrónicos.- Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Art. 46.- Perfeccionamiento y aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral, en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

II.1.3.2.9 DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRÓNICOS

Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias.

En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,

b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;

2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;

3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,

4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del

Consumidor y su Reglamento. Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

Capítulo IV

II.1.3.2.10 DE LOS INSTRUMENTOS PÚBLICOS

Art. 51.- Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.

Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

Título IV

II.1.3.2.11 DE LA PRUEBA Y NOTIFICACIONES ELECTRÓNICAS

Capítulo I

DE LA PRUEBA

Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Art. 53.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la Ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Art. 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a. Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;

b. En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados;

c. El faxcímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectuó con el empleo de otros métodos que aconsejen la técnica y la tecnología.

En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Art. 56.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un

Abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

Título V

II.1.3.2.12 DE LAS INFRACCIONES INFORMÁTICAS

Capítulo I

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art.- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión

menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art.- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

Art. 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo."

Art. 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

"Art.- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho. El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo."

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art.- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica."

Art. 62.- A continuación del Art. 553, añadase los siguientes artículos innumerados:

"Art.- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes."

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos."

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."

II.1.3.3 DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación de información extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la Ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El Reglamento de aplicación de la Ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta Ley.

Cuarta.- No se admitirá ninguna exclusión restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente Ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimientos e instrumentos empleados.

Novena.- Glosario de Términos.- Para efectos de esta Ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red Electrónica de Información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio Electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Datos Personales Autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quién, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta Ley y su reglamento.

Factura electrónica: Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes reformas al Código Penal, contenidas en el Título V de esta ley, se tomaran en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

II.1.3.4 DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta Ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 57 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta Ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

II.1.3.5 DISPOSICIÓN FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente Ley.

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dada en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la sala de sesiones del Pleno del Congreso Nacional del Ecuador, a los diez días del mes de abril del año dos mil dos.

http://www.conatel.gov.ec/site_conatel/

FUENTES DE LA PRESENTE EDICIÓN DE LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

1.- Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002).

Fuente: FIEL Magister 7.1 (c). Derechos Reservados. 2004.

<http://www.edicioneslegales.com/>

Esta versión de la norma legal no equivale ni sustituye o reemplaza a la publicada en el Registro Oficial Ecuatoriano, por lo tanto el usuario asume bajo su entera responsabilidad el uso de esta información.

**II.1.3.6 Reglamento General a la Ley De Comercio Electrónico, firmas
Electrónicas y mensajes de datos.**

**Reglamento a la Ley de comercio electrónico, firmas electrónicas y mensajes
de datos
(Decreto No. 3496)**

Gustavo Noboa Bejarano

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Considerando:

Que mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 577 de 17 de abril del 2002 se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos; Que la disposición final de la citada ley dispone que el Presidente de la República debe expedir el correspondiente reglamento; y,
En ejercicio de la facultad prevista en el artículo 171 numeral 5 de la Constitución Política de la República,

Decreta:

Expedir el siguiente

**REGLAMENTO GENERAL A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS
ELECTRÓNICAS Y MENSAJES DE DATOS.**

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos y a cuyo

contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación.

En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte.

Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico. Cuando las leyes así lo determinen, cierto tipo de información

deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Art.2.-Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art.3.-Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a. Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b. Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art.4.-Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art.2.-Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art.3.-Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a. Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los
}

remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b. Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art.4.-Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art.2.-Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando

los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art.3.-Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a. Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b. Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art.4.-Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona

autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico.

Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

- a. No-discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
- b. Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente 1;
- c. El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso

de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);

d. Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios; y,

e. Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Art. 11.- Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición.

Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.

Art. 12.- Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67.

Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos.

Los períodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Art. 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento.

Art. 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.-La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al artículo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículo 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

a. (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005) Siempre en la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,

b. Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica.

Opcionalmente, en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Art. 16.-Reconocimiento internacional de certificados de firma electrónica.-

(Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador una vez obtenida la revalidación respectiva emitida por el CONATEL, él deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Art. 17.-Régimen de acreditación de entidades de certificación de información.-

(Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONATEL, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Art. 18.- Responsabilidades de las entidades de certificación de información.-

Es responsabilidad de la entidad certificadora de información o de la entidad de registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Art. 19.- Obligaciones del titular de la firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control prevista en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales.

En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio.

Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos.

En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la

información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envío de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

- a. Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción (SIC);
- b. Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;
- c. Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;

d. A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,

e. Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Art. 23.-Sellado de tiempo.- (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONATEL para prestar este servicio.

El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONATEL; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios, de sellado de tiempo se realizará en régimen de libre competencia y contratación.

Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulan su relación.

Artículo Final.- El presente reglamento entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Palacio Nacional, en Quito, a 12 de diciembre del 2002.

FUENTES DE LA PRESENTE EDICIÓN DEL REGLAMENTO GENERAL A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

1.- Decreto 3496 (Registro Oficial 735, 31-XII-2002)

2.- Decreto 908 (Registro Oficial 168, 19-XII-2005).

Fuente: FIEL Magister 7.1 (c). Derechos Reservados. 2004.

<http://www.edicioneslegales.com/>

Esta versión de la norma legal no equivale ni sustituye o reemplaza a la publicada en el Registro Oficial Ecuatoriano, por lo tanto el usuario asume bajo su entera responsabilidad el uso de esta información.

http://www.conatel.gov.ec/site_conatel/

CAPITULO III

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:

Autenticación
Confidencialidad
Integridad
No repudio

La solución para los objetivos propuestos incluye 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.

III.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 ENCRIPCIÓN

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 incomprendible, 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 adquirente); 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

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.

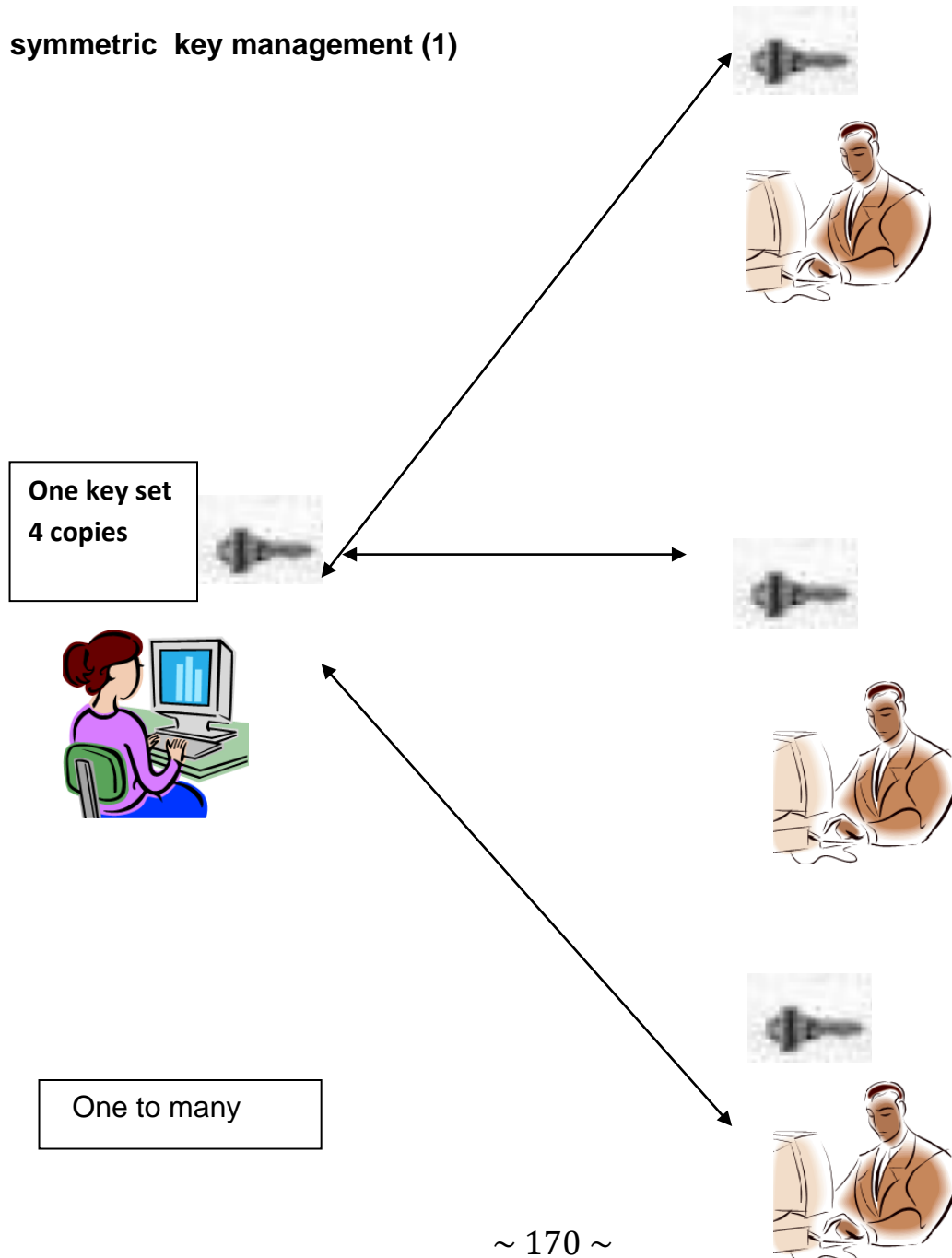
El control de accesos puede ser garantizado por una tercera parte, que puede ser un Centro de Control de Accesos (ACC por sus siglas en inglés).

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.

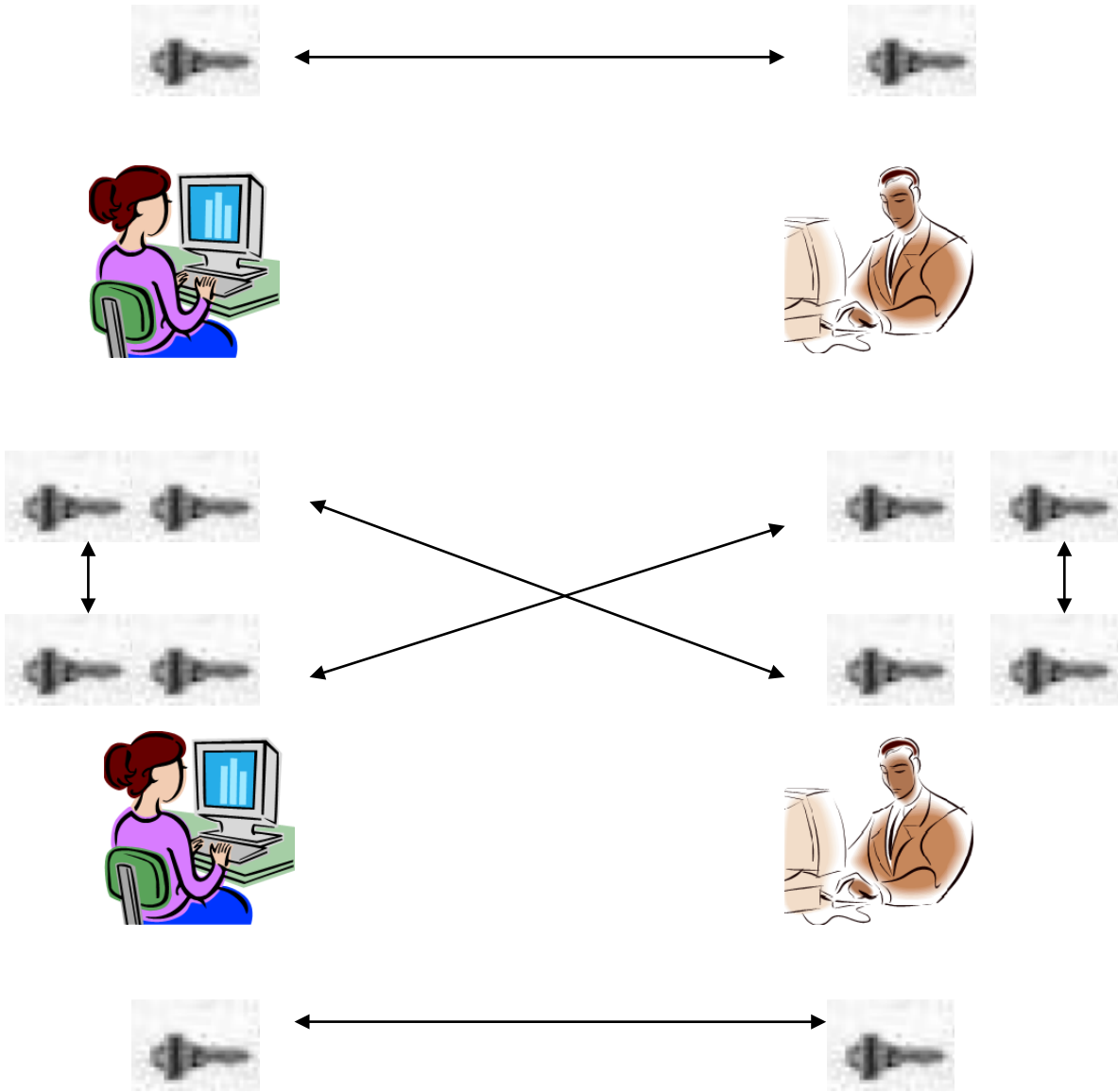
Además, debe existir mucha confianza entre esta autoridad y los usuarios, de tal manera que confiemos plenamente que el usuario que utiliza una llave autorizada por la CA, es quien dice ser.

symmetric key management (1)



symmetric key management (2)

6 unique private key pairs



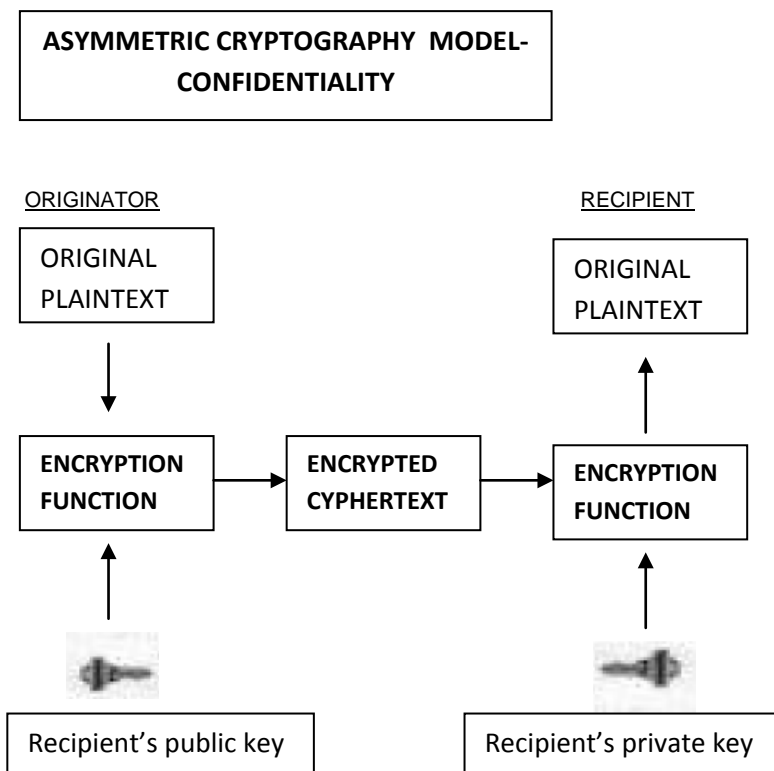
MANY TO MANY

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

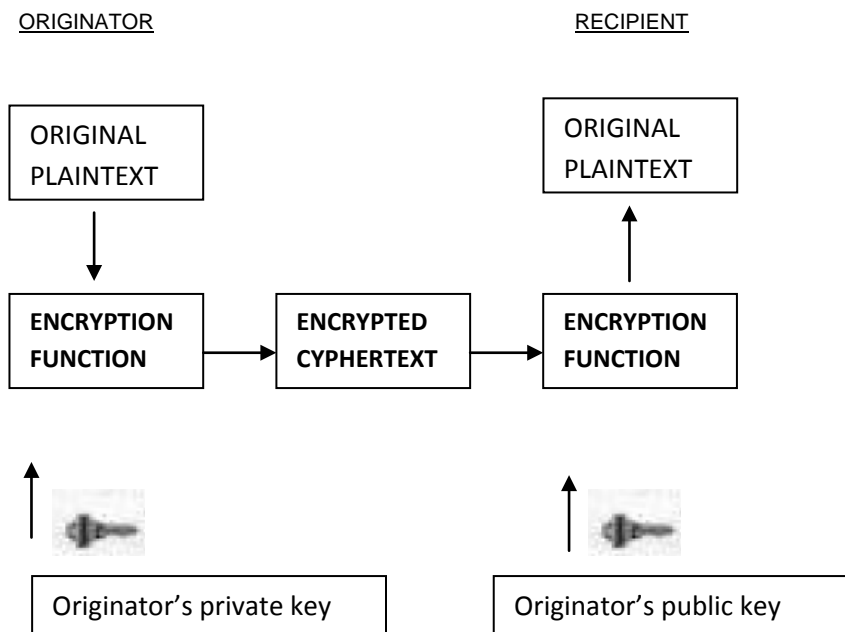
Todas las partes autorizadas deberán utilizar el mismo algoritmo de encriptación, por ejemplo el Rivest, Shamir, Adleman (RSA); y tener acceso a las llaves.

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/descriptación.



**ASYMMETRIC CRYPTOGRAPHY MODEL-
AUTHENTICATION**



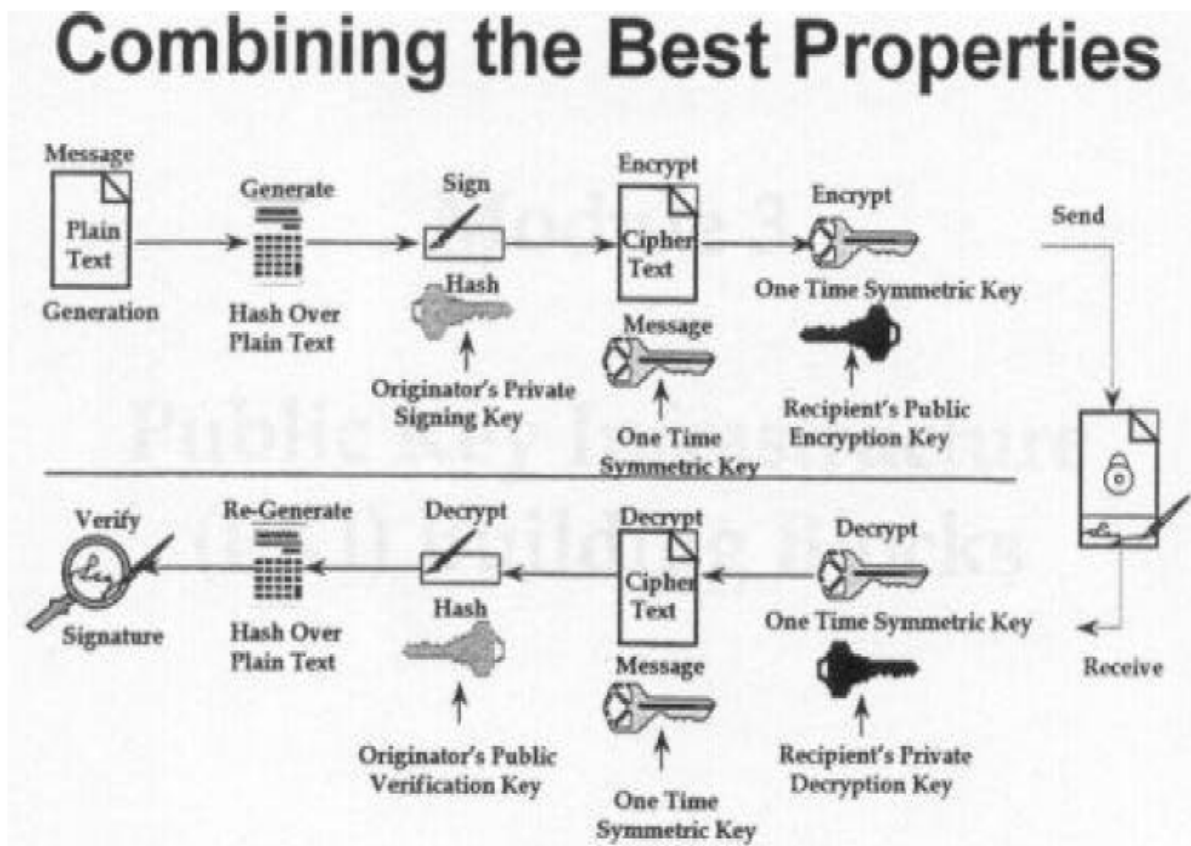
COMBINANDO LAS MEJORES PROPIEDADES

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.



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.	Autenticación.	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.

III.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. 1 certificado, 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.

FUENTES DE INFORMACIÓN

- http://www.conatel.gov.ec/site_conatel/
- <http://inforc.ec/noticia03.htm>
- <http://www.nist.gov/index.html>
- Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002). Fuente: FIEL Magister 7.1 (c). Derechos Reservados. 2004.

<http://www.edicioneslegales.com/>

- 1.- Decreto 3496 (Registro Oficial 735, 31-XII-2002)
- 2.- Decreto 908 (Registro Oficial 168, 19-XII-2005).

Fuente: FIEL Magister 7.1 (c). Derechos Reservados. 2004.

<http://www.edicioneslegales.com/>

- JUNTA PROVINCIAL DE SEGURIDAD CIUDADANA Y DEFENSA CIVIL DEL GUAYAS

<http://www.defensacivilgye.50megs.com/dcgye.htm>

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

www.auerbach-publications.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/
- 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
- <http://www.corpece.org.ec/isoc/news.php>
- <http://www.corpece.net/hc3.asp>
- 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.cfbssoft.iespana.es/cfbssoft/seguridad/tesis.htm>
- VirusProt. www.virusprot.com



COMPRAS DE PRODUCTOS Y SERVICIOS POR INTERNET



Ahora, comprar y vender por Internet en el Ecuador es seguro, fácil y rápido.

Diners Club y Visa Banco del Pichincha apoyando al comercio electrónico en el Ecuador, ha creado herramientas de pago electrónico con el respaldo de Interdin y Verified by Visa, que la garantiza seguridad y confiabilidad a los establecimientos o clientes Diners Club y Visa que venden y compran por Internet.

Es una solución tecnológica con más de cuatro años en el mercado ecuatoriano y con casos de negocios exitosos. El establecimiento que instala Botón de Pagos pagos en su sitio web, transforma su site de informativo a transaccional, donde el socio Diners Club o el cliente Visa Banco del Pichincha, que visite el sitio puede comprar todos los productos o servicios que el establecimiento oferta, totalmente en línea, es decir las afectaciones a la cuenta del establecimiento y del socio que compra se registran en ese momento.

BENEFICIOS

Seguridad

La información de la tarjeta de crédito que el socio Diners Club o cliente Visa Banco del Pichincha, proporciona para la compra, bajo ninguna circunstancia es entregada al establecimiento.

El socio Diners Club podrá generar su clave de compras por Internet durante la compra en uno de nuestros establecimientos afiliados, al igual el Cliente Visa Banco del Pichincha podrá generar su clave de Verified by Visa.

Se garantizan esquemas de seguridad basados en encriptaciones, firmas digitales y intercambios de llaves, bajo estándares de comercio electrónico.

En el caso de Visa se trabaja bajo la plataforma 3DSecure, que permite al sitio de comercio electrónico realizar una validación de autenticación en línea sobre un tarjeta habiente que quiera realizar una compra online y que este enrolado dentro del programa Verified by Visa. El alcance de este programa es internacional.







Comodidad

Los socios Diners Club y clientes Visa Banco del Pichincha, desde la comodidad de su casa u oficina, podrán hacer compras a través del sitio web del establecimiento, las 24 horas del día, los 7 días de la semana.

Rapidez

Invirtiéndolos unos pocos minutos, desde un dispositivo conectado a Internet, el socio Diners Club y cliente Visa Banco del Pichincha, puede evitar colas y hacer compras totalmente seguras y en línea.

Los Establecimientos Afiliados a Diners y Visa Banco del Pichincha son los siguientes:

		Establecimiento	Diners Club	Visa	Dirección Electrónica
1.		PONTIFICIA UNIVERSIDAD CATÓLICA. Pago de matrículas	X	X	http://www.puce.edu.ec
2.		UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL Pago de matrículas	X	X	http://www.ute.edu.ec
3.		UTPL (Universidad Técnica Particular de Loja) Pago de matrículas	X	X	http://www.utpl.edu.ec
4.		ESPE (Escuela Politécnica del Ejército) Pago de matrículas	X	X	http://www.espe.edu.ec
5.		UCSG (Universidad Católica Santiago de Guayaquil) Pago de matrículas	X	X	http://www.ucsg.edu.ec
6.		UDA (Universidad del Azuay) Pago de matrículas	X	X	http://www.uazuay.edu.ec

7.		CMSFQ (Colegio menor San Francisco de Quito) Pago de matrículas	X		http://www.cmsfq.edu.ec
8.		FLACSO (Facultad Latinoamericana de Ciencias Sociales) Pago Cursos / Venta Libros	X	X	http://www.flacso.org.ec
9.		MULTICINES Venta de entradas	X	X	http://www.multicines.com.ec
10.		TRIBUNAL CONSTITUCIONAL Suscripción al registro oficial	X	X	http://tribunalconstitucional.gov.ec
11.		CITOTUSA Compra abonos y entradas sueltas	X		http://www.feriadequito.com
12.		PORFINEMPLEO.COM Publicación de anuncios laborales	X		http://www.profinempleo.com
13.		NORMA Venta de libros	X	X	http://www.norma.com
14.		AEROGAL Venta de pasajes aéreos	X	X	http://www.aerogal.com.ec
15.		TAME Venta de pasajes aéreos	X	X	http://www.tame.com.ec
16.		JF NASSER Venta de licores	X	X	http://www.shopzona.com



<http://www.bce.fin.ec/contenido.php?CNT=ARB000005>



<http://www.bolivariano.com/>



<http://www.bancoguayaquil.com/bg/banco-de-guayaquil.html>



<http://wwwp2.pichincha.com/web/index.php>



<https://www.bancodelpacifico.com/>

Qué compran en Internet

Mucho se comenta de la cantidad de navegantes en la Web pero poco se conocía sobre cuantos realmente han usado la Internet para hacer una compra.

En la encuesta Global Online Survey elaborada por The Nielsen Company, se indagó entre 26,312 personas mayores de 15 años en todo el mundo qué habían comprado por Internet, arrojando los siguientes resultados.

41% Libros

36% Ropa, accesorios y zapatos

24% DVD's, Videos y Juegos

24% Tiquetes aéreos / Reservaciones de vuelos

23% Electrónica de consumo

19% Música

19% Cosméticos y suplementos nutritivos

16% Equipo de computo

16% Tours y reservaciones de hotel

15% Boletas para eventos

14% Software

14% Mercado

9% Juguetes y Muñecas

8% Elementos deportivos

4% Automóviles y partes

3% Elementos Coleccionistas

20% Otros

COMPARACION ENTRE ECUADOR CON LOS PAISES DE AMERICA DEL SUR

ECUADOR CON UN PORCENTAJE DE PENETRACION DEL 5.2% Y PARAGUAY CON UNA PENETRACIÓN DEL 2.7% ES DECIR AMBOS PAISES TIENEN UN PORCENTAJE MUY BAJO A COMPARACIÓN CIN LOS DEMAS EL PAIS QUE TIENE EL MAYOR INDICE DE PORCENTAJE ES CHILE CON UN PORCENTAJE DEL 36.1%, URUGUAY CON UN PORCENTAJE DEL 20.9%, ARGENTINA CON EL 20.6%, GUAYANA FRANCESA CON 19.6% GUAYANA CON EL 16.5%, PERU CON EL 16.3%, VENEZUELA CON EL 12.2%, COLOMBIA CON UN 7.8%, LUEGO SURINAME CON UN 6.5%, BOLIVIA CON UN 3.9%.