UNIVERSIDAD MICHOACANA DE SAN NICOLAS DE HIDALGO

FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS

TESIS

SEGURIDAD DE LA INFORMACIÓN ATRAVÉS DE LA CRIPTOGRAFIA

PARA OBTENER EL TITULO DE LIC. EN INFORMATICA ADMINISTRATIVA

OMAR GUZMAN GUZMAN
ASESOR: M.A. ERIK ALFARO CALDERON

MORELIA, MICHOACAN FEBRERO 2010

AGRADECIMIENTOS

Agradezco a mi familia por todo su apoyo día con día, a todos mis compañeros y amigos con los cuales compartí momentos inolvidables y a todos los profesores que nos ayudaron a cumplir con nuestros objetivos a lo largo de nuestra carrera, en especial al Dr. Gerardo Alfaro Calderón por su apoyo en la realización de este proyecto.

DEDICATORIA

A dios por darme fortaleza y salud, a mi familia por todo su apoyo
la cual es parte fundamental para cumplir con mis objetivos,
a Lissette por estar siempre a mi lado.

INDICE

INDICE IMÁGENES Y FIGURAS

INTRODUCCION

Hoy en día la seguridad de la información en las empresas es muy importante ya que es un recurso valioso lo cual le permitirá que sigan adelante cumpliendo sus objetivos hacia el éxito, en la actualidad hay muchos peligros al interactuar en la red (Internet e intranet), entre los que resalta, el robo de datos por parte de expertos informáticos que buscan hacer mal uso de ellos, ya sea para hacer fraudes, extorsionar o para copiar ideas de otras organizaciones e implantarlas en las suyas, dañar información confidencial e importante, o realizar cualquier acción ilícita que perjudique a la organización o usuarios.

Hoy en día, el manejo de información usando TICs[1] tanto para las personas como para las empresas se ha hecho indispensable, es muy común hacer compras-ventas (comercio electrónico) a través de la red, hacer transacciones bancarias, enviar correos electrónicos, y todo tipo de datos que para nosotros es confidencial, pero uno se pregunta ¿es realmente confiable hacer todo esto?, la realidad y las cifras nos indican que no, existen numerosos fraudes, robos de información y cuentas bancarias por parte de gente maliciosa que se apoderan de esos datos para hacer daño, robar dinero o datos importantes.

Es por esto que en este documento analizamos la importancia de la información en las empresas, desde como se genera hasta la forma y medios seguros de transmitirla a cualquier parte del mundo a través de la red sin que sea interceptada por malware, a través de técnicas y los diferentes métodos de encriptación. De esta manera los usuarios y las organizaciones tendrán una manera más segura de hacer movimientos a través de la red, sin el temor de que su información sea vista por cibercriminales y de esta forma interactuar, enviar y recibirlos datos de forma confiable con usuarios, clientes, empresas nacionales, internacionales, así como poder manipular nuestros datos de los sistemas de información de forma segura a través de accesos remotos a nuestras paginas Web.

[1] **TICs**: (Tecnologías de información y Comunicaciones) Son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas.

DEFINICION DEL PROBLEMAS

Los fraudes y robos de información que hay en el envío y recepción de los datos a través de la red, a las empresas y usuarios en general al hacer diferentes transacciones y uso de la información en los diferentes servicios de Internet.

Se desea realizar el envío de mensajes e información en general desde un usuario que actúa como emisor hacia un usuario que actúa como receptor mediante el uso de un canal considerado como inseguro. Durante el paso del mensaje o información por el canal inseguro, se corre el peligro de que exista una tercera persona interceptando y/o recibiendo la información destinada al receptor que se encuentra en forma legible y decodificada. Quizás en muchos casos los mensajes o información enviada puede que no sea un gran secreto, sin embargo, cuando sí se requiere del envío de información confidencial este proceso inseguro puede ser un gran problema, además de tener seguridad en el acceso a nuestros datos en los sistemas de información a través de la Web.

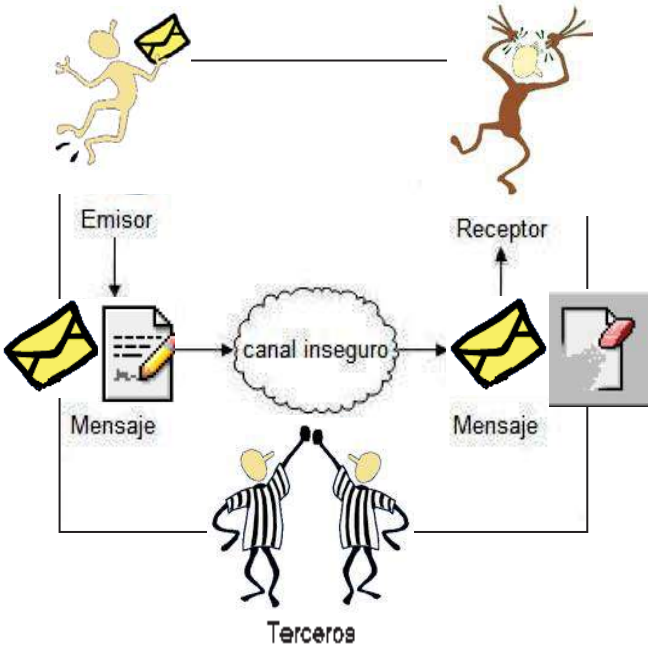


Fig. 1 Envío de información a través de un canal inseguro

PREGUNTAS

- ¿Es necesario la protección de los datos en las empresas y usuarios en general?
- ¿Existe seguridad en la información de las empresas y usuarios?
- ¿Las empresas están tomando acciones para proteger su información?
- ¿El gobierno se interesa en la seguridad de los datos en las empresas y usuarios?
- ¿Que instituciones son mas atacadas por los cibercriminales?
- ¿Que métodos de seguridad utilizan instituciones y usuarios para protegerse?
- ¿La criptografía es un método efectivo y seguro para proteger nuestros datos?
- ¿Como protegernos de los cibercriminales?
- Que métodos de seguridad se utiliza para proteger sitios Web y sus sistemas de información?

HIPOTESIS

Se lograra la protección de la información en el envío y recepción de los datos a través del uso de la criptografía, además serán mas seguras las operaciones en la red al tomar ciertas acciones que nos escudaran de los cibercriminales, se evitara que muchas empresas sean objeto de fraudes, será un método complemento de mucha importancia y seguridad ligado a las demás acciones de protección que deben tener las empresa y usuarios para blindar la información confidencial.

Será de gran importancia para toda la comunidad cibernauta en general, conocer como protegernos de los extorsionistas en la red y que todas las instituciones y usuarios estén concientes de los peligros que existen y como combatirlos, de esta manera al administrar webs, accesar a sistemas, realizar acciones compras o ventas en Internet se tendrá mayor seguridad y así poder disfrutar de todas las cosas positivas que existen en la red.

JUSTIFICACION

En la actualidad millones de personas en el mundo utilizan la red para realizar diferentes actividades y la mayoría no tiene los conocimientos necesario en el aspecto de seguridad, lo cuales son presa fácil al momento de ingresar al mundo cibernético.

Muchas empresas gasta infinidad de dinero en la seguridad de la información ya que en estos días los fraudes están en su auge, todas la organizaciones y usuarios en general que hacen transacciones en la Web no tienen la seguridad al hacerlo, para esto las empresas proveedoras de estos servicios pagan por nuevas técnicas de cifrados de información para que al momento de ser interceptado algún dato sea imposible descifrarlo.

Y no solo las empresas tienen la necesidad de tener seguridad en el envío y recepción de la información los usuarios en general son vulnerables a hacer compras electrónicas, consultar sus cuentas bancarias, envío de correo etc, es importante tener conocimiento de ciertas acciones, técnicas y métodos para tener a salvo y protegida nuestra información confidencial.

Es por esto la importancia de conocer la criptografía como método para el envío y recepción de información a través de la Web, que permitirá el traslado de los datos íntegros sin que sea interceptada por personas que quieran hacer mal uso de ella. Así como la forma segura de accesar a los datos de los sistemas de información a través de la red.

Al conocer los diferentes algoritmos para realizar procesos criptográficos y acciones de seguridad, podremos lograr el resguardo de la información de forma segura y confidencial, ya que son herramientas importantes que debemos tener en cuenta al momento de introducirnos al mundo del Internet y así poder disfrutar de todos los beneficios que nos ofrecen sin ser sorprendidos.

OBJETIVOS

- Conocer las diferentes técnicas y acciones para la seguridad de la información.
- Mantener integra y segura nuestra información a través del cifrado de los datos al realizar transacciones y acceso a sistemas de información.
- Establecer estrategias para el manejo de los datos seguros en nuestra empresa y fuera de ella a través de la red.
- Implantar dispositivos y técnicas de seguridad en el envío y recepción de la información.
- Conocer las formas de extorsión y de robo de información a los usuarios y empresas.
- Identificar medidas para evitar el robo de los datos en las transacciones y en los sistemas de información desde nuestra Web.
- Utilizar los algoritmos criptográficos como medio para garantizar el envío y recepción de datos de forma segura.
- Utilizar servicios de proveedores que certifique nuestras páginas Web para que el cliente tenga la certeza de que esta en una pagina verdadera y segura

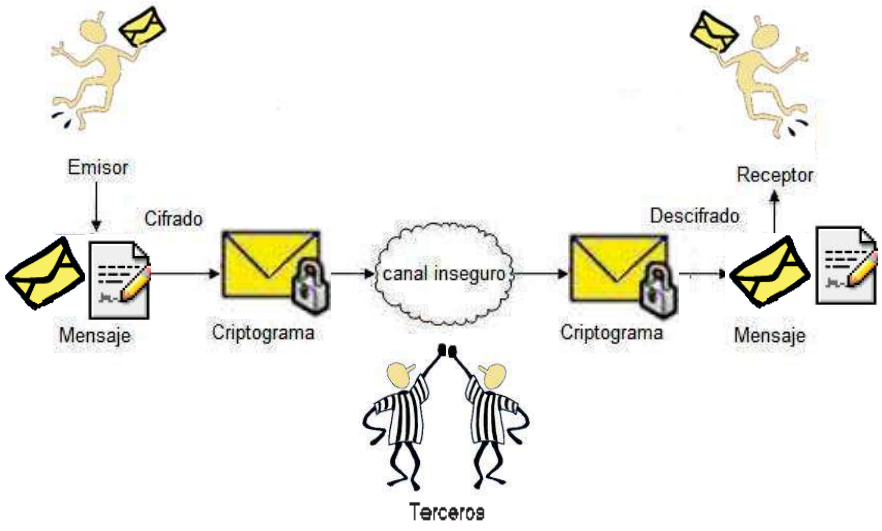


Fig. 2 Envío de información encriptada a través de un canal inseguro

1. QUE ES LA INFORMACION

Los datos son comunicados por varios tipos de símbolos tales como las letras del alfabeto, números, movimientos de labios, puntos y rayas, señales con la mano, dibujos, etc.

En sentido general, la información es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. De esta manera, si por ejemplo organizamos datos sobre un país (número de habitantes, densidad de población, nombre del presidente, etc.) y escribimos por ejemplo, el capítulo de un libro, podemos decir que ese capítulo constituye información sobre ese país. Cuando tenemos que resolver un determinado problema o tenemos que tomar una decisión, empleamos diversas fuentes de información (como podría ser el capítulo mencionado de este imaginario libro), y construimos lo que en general se denomina conocimiento o información organizada que permite la resolución de problemas o la toma de decisiones (ver apartado sobre conocimiento).

Según otro punto de vista, la información es un fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información por tanto, procesa y genera el conocimiento humano. Aunque muchos seres vivos se comunican transmitiendo información para su supervivencia, la superioridad de los seres humanos radica en su capacidad de generar y perfeccionar tanto códigos como símbolos con significados que conformaron lenguajes comunes útiles para la convivencia en sociedad, a partir del establecimiento de sistemas de señales y lenguajes para la comunicación.

Los datos se perciben mediante los sentidos, estos los integran y generan la información necesaria para producir el conocimiento que es el que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la

existencia social. La sabiduría consiste en juzgar correctamente cuando, cómo, donde y con qué objetivo emplear conocimiento adquirido.

El ser humano ha logrado simbolizar los datos en forma representativa (lenguaje) para posibilitar el conocimiento de algo concreto y creó las formas de almacenar y utilizar el conocimiento representado.
Existe una relación indisoluble entre los datos, la información, el conocimiento, el pensamiento y el lenguaje, por lo que una mejor comprensión de los conceptos sobre información redundará en un aumento del conocimiento, ampliando así las posibilidades del pensamiento humano, que también emplea el lenguaje -oral, escrito, gesticular, etc.-, y un sistema de señales y símbolos interrelacionados.

Función de la información

- Aumentar el conocimiento del usuario.
- Proporcionar a quien toma decisión probabilidades para la elección, reduciendo la gama de decisiones.
- Proporcionar una serie de reglas de evaluación y reglas de decisión para fines de control.

1.1 HISTORIA DE LA INFORMACION

La comunicación surgió cuando el hombre prehistórico apareció. Este tenía una serie de métodos para que este se entendiera entre sí con los demás que estaban en su grupo. Los métodos con los que se comunicaba se pueden clasificar en: *Señales de humo*: Este fue uno de los métodos que el hombre desarrolló más. Este se originaba mediante el humo que se producía por las fogatas que el hombre hacía, estas se originaban mediante el fuego que los descubrieron. *Signos*: Este es otro de los métodos que el hombre más desarrolló. Este se producía mediante signos que se hacían mediante piedras de colores. Estos hacían signos de animales y a veces de paisajes que ellos veían.
En los períodos Eolíticos (l, 300,000 años A.C.) y del Paleolítico Inferior, se empiezan a dar modos de comunicación de acuerdo a un limitado proceso de comunicación, quizás más basado en gestos, interjecciones vocales, dibujos y pinturas rupestres

Las primeras manifestaciones de escritura como un conjunto de caracteres se dan en Mesopotamia 300 A.C., en Sumer, Acad, Babilonia, Egipto, China aporta desde el siglo II A.C.
Cuando los sistemas de escritura fueron inventados en las antiguas civilizaciones el hombre utilizó todos los soportes de escritura de los que se hizo servir: tablillas con cera, plomo, pieles, hueso, madera, papiros o tablas de masilla.

La escritura fue el resultado de un proceso lento de evolución de diferentes pasos: reproducción directa de objetos: Pictografía[2]; representación de símbolos: Ideografía; para acabar con la reproducción de sílabas: Escritura fonética.

[2] **Pictografía**: Forma de escritura en la que los objetos o conceptos son representados con dibujos

Es probable que la primera escritura apareciera en Asia en la antigua Mesopotamia, mediante signos cuneiformes: escritura cuneiforme (se utilizaba una herramienta de caña con sección triangular que hendida en arcilla dejaba una marca en forma de cuña). La usaron los sumerios, acadios, asirios, hititas, persas, babilonios etc.

Sobre la escritura egipcia podemos distinguir la escritura jeroglífica, que representa las palabras mediante figuras (otros pueblos, como los hititas y los aztecas también tuvieron este tipo de escritura) que evolucionó en cursiva: en las escrituras hierática y demótica y también en una escritura fonética con 22 signos consonánticos y 36 silábicos.

1.2 PROCESO DE LA INFORMACIÓN

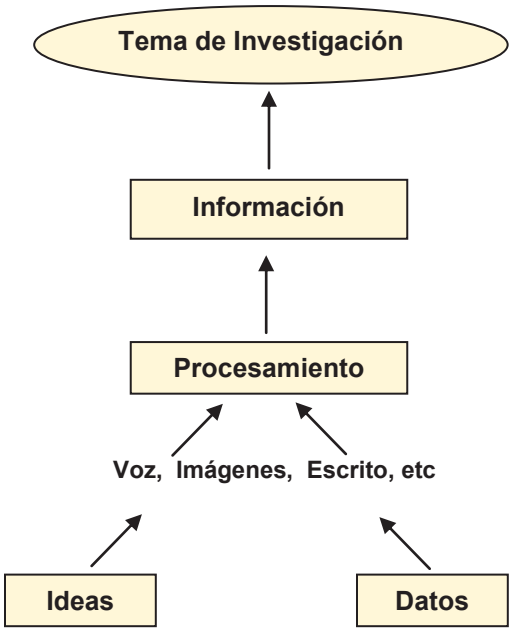


Fig.3 Estructura del proceso de la información

Ideas: "Representación mental de una cosa abstracta o universal", "Imagen de una cosa percibida por los sentidos", "Conocimiento puro, racional", "Plan y disposición que se ordena en la fantasía"..." "Ingenio para inventar y disponer".

Diccionario Ideológico de Julio Casares, 1988

Dato: Un dato es un conjunto discreto, de factores objetivos sobre un hecho real.

Davenport y Prusak (1999)

Procesamiento: Obliga a codificar la información en unidades manejables, a descomponerla en bloques significativos, que implica un agrupamiento en función, tanto de los objetivos del procesamiento (comprender, memorizar, interpretar, etc.) como de los esquemas propios de conocimiento previos.

G. A. Miller (1956)
Estudio y procesamiento de la información

Información: Es un mensaje, normalmente bajo la forma de un documento o algún tipo de comunicación audible o visible. Como cualquier mensaje, tiene un emisor y un receptor.

Davenport y Prusak (1999)

Tema investigado: Una investigación involucra una serie de procesos de manejo de información. La realización de estos procesos no es lineal, los procesos se conectan entre sí, por lo que es posible trabajar en varios procesos a la vez o bien estar en uno y regresar a otro en el que trabajaste previamente.
Una investigación puede iniciar con una inquietud personal o una duda, cuando surge en ti una necesidad de aprender más sobre algo, buscas aclarar tus preguntas, explicarte un objeto o un hecho que no entiendes o comunicar algo con fundamentos. O bien puede surgir de una solicitud externa, cuando alguna autoridad te pide que realices un determinado trabajo o proyecto.

1.3 CARACTERISTICAS DE LA INFORMACIÓN

En primer lugar, la información debe estar actualizada, lo que implica que ésta es capturada cuando se genera y no un tiempo después mediante procesos adicionales. Es decir, cuando se factura en un almacén, se debe descargar del inventario y contabilizar con la misma transacción (no necesariamente en tiempo real, pero no debe involucrar procesos manuales adicionales). También debe haber una conectividad con entidades externas como clientes, proveedores, entidades de gobierno entre otras, de tal manera que la información que deba circular por fuera de la empresa, también lo haga de manera ágil permitiendo la actualización permanente.

Ante tanta información disponible, la que se presente para tomas de decisiones debe ser relevante, es decir, ni más ni menos que la necesaria. Para poder proveer la cantidad exacta de información, se debe contar con sistemas que permitan tener análisis a diferentes niveles de detalle: unas bases de información consolidada para la gestión, y unas bases de información de producción para el manejo de las transacciones. Se debe proveer el mecanismo más ágil disponible para el acceso a esta información y garantizar que haya conectividad entre las diferentes bases de información.

La velocidad de los negocios exige una oportunidad en esta información, lo que implica tener una alta velocidad de acceso a la información la cual se puede proveer con conexiones permanentes en "línea" a las bases de datos. Adicionalmente, la oportunidad exige disponibilidad de alto nivel, lo que ocasiona el establecimiento de planes de continuidad que garanticen el acceso a la misma.

Si bien es importante el manejo de la cantidad de la información y el acceso a la misma, es tal vez más importante la calidad de la información que se presente en sus niveles de confiabilidad. Es decir, qué tanto se puede creer en la información que se está recibiendo. Afortunadamente este factor se diseña

mediante la implementación de procesamiento automático de información, establecimiento de seguridades a diferentes niveles, y la auditabilidad de las actividades, específicamente identificando quién hizo qué, cuando y desde donde. Las bases de datos actualmente proveen herramientas como la integridad referencial, sin embargo si no hay conciencia en la necesidad de la calidad sobre la velocidad o facilidad de uso para el usuario, es probable que el sistema de información quede produciendo a altas velocidades cifras irrelevantes que ocasionen errores en las decisiones.

La última característica necesaria es que la información pueda ser explicable. Es decir, se debe poder ver a todos los niveles de detalle el origen de toda información. Para cada total, se tienen también los valores de los componentes de estos totales. Además se deberá poder analizar la información en el tiempo por lo que se requiere acceso a la información tanto presente como histórica.

1.4 IMPORTANCIA DE LA INFORMACION

Nuestras vidas giran en torno a la información que podemos percibir de nuestro entorno, si no logramos sacar conclusiones acertadas, estamos en clara desventaja de nuestros convivientes humanos. El existencialismo plantea que toda la vida es una constante decisión, debemos elegir en cada momento de nuestras vidas, y las decisiones claramente deben estar basadas en información, esta se produce cuando logramos interpretar datos, es decir, señales de nuestro entorno, si combinamos señales atómicas y concluimos algo de ellas, es porque hemos extraído información, luego si nuestro razonamiento es acertado tenemos la capacidad de hacer una, en teoría, buena decisión. Por otra parte, la información debe tener una serie de características implícitas para que podemos utilizarla (debe ser fidedigna, a tiempo, etc.), asumiendo cumplidos estos requisitos pasamos a la etapa de la razón en donde podemos transformar esa información en conocimiento y agregar así un ítem más a nuestro *saber*..

Diego Arenas C
Julio 09, 2006

1.5 IMPORTANCIA DE LA INFORMACION EN LAS EMPRESAS.

La Información es un recurso vital, producido por los sistemas de información. Las organizaciones utilizan también otros recursos como materiales, materias primas, energía y recursos humanos, todos ellos sujetos a cada vez mayores restricciones en su uso y crecimiento, debido a problemas de escasez y, por tanto, de coste.

Dentro de cualquier organización la información fluye día con día, y cada actividad genera mas información que puede apoyar las distintas tareas que se llevan a cabo para su buen funcionamiento. En todos los departamento de todas las organizaciones se genera información, como lo son el los departamento de recursos humano, finanzas, contabilidad, limpieza, producción y todos los departamentos mas que se imaginen. La información se genera debido a las actividades que se llevan a cabo en cada departamento y el éxito de estos mismos depende de la visión que se tenga y en que se apoyen para lograr las metas establecidas, sin duda alguna, el apoyo en la información que se genera dentro de ese departamento es una base sumamente sustentable y creíble para tomarse en cuanta para posibles tareas.

Con los adelantos tecnológicos actuales, sobre todo en las tecnologías de información, es casi imposible que una empresa no haga uso de la información para el desarrollo de sus actividades cotidianas; tan solo tener la información adecuada de un estado financiero no necesariamente en computadoras demuestra que es necesaria la información para todo tipo de actividades y si ha esto le agregamos el uso de computadoras como herramientas junto con sistemas capaces de ofrecernos la información en forma rápida, ordenada, y concreta, además que la Internet se ha vuelto tan importante y popular para cualquier tipo de persona como para cualquier tipo de empresa sabiendo de antemano que la información es vital en todos los aspectos, muchas empresas emplean Internet como medio de información con sus posibles consumidores, proveedores, socios.

La información es la parte fundamental de toda empresa para tener un alto nivel de competitividad y posibilidades de desarrollo. El objetivo básico de la información es la de apoyar a la toma de decisiones de todo gerente, este tendrá mas bases sustentables para poder decidir que es lo que se va a hacer y que rumbo tomar para lograr los objetivos que se planearon; contara con un mayor numero de armas para afrontar el camino que decidirá el futuro de la organización.

Debe considerarse que un sistema de información no tiene porqué ser asociado a los sistemas informáticos, con los que muchas veces se les confunde. Por el contrario, un sistema de información puede ser una persona, un departamento, toda la empresa (o al menos toda parte o elemento de la empresa, o relación entre los mismos, que trate con información). El Sistema de Información comprende, pues, planificación, recursos humanos y materiales, objetivos concretos a corto, medio y largo plazo, etc., aunque también tecnología y técnicas.

De esta forma, constituyen un campo esencial de estudio en administración y gerencia de empresas. Es por esta razón que todos los profesionales en el área de Administración de Empresas deberían o más bien deben, tomar un curso de sistemas de información. Por otro lado es importante tener una comprensión básica de los sistemas de información para entender cualquier otra área funcional en la empresa, por eso es importante también, tener una cultura informática en nuestras organizaciones que permitan y den las condiciones necesarias para que los sistemas de información logren los objetivos.
Existen dos tipo de información Publica y privada, la publica es la información a la que puede acceder cualquier persona, y la información privada, es la que no puede ir mas allá de las personas que deban manejarla, datos concretos sobre contabilidad, nuevas ideas, negocios en marcha, datos importantes de clientes etc. Solo las personas que tienen un alto grado de confianza acceden a ellas.

Sergio Alejandro Martínez De La Cruz , 11-2005
Pequeñas y medianas empresas, PyME

2. SISTEMA DE INFORMACION

Hoy en día los sistemas de información juegan un papel cada vez mas importante en las modernas organizaciones empresariales, hasta el punto de condicionar su éxito o su fracaso en un entorno económico y social tan dinámico y turbulento como el que caracteriza al mundo actual.

Nuevos fenómenos como la globalización o el transito hacia una economía mas basada en el conocimiento han inducido importantes cambios en las organización empresariales. En este nuevo contexto, los sistemas y las Tecnología de la Información y Comunicaciones (TICs) se han convertido en un elemento esencial como motor del cambio y fuente de ventajas competitivas.

Dentro de una organización un Sistema de Información actúa como el “sistema nervioso” ya que este es el que se encarga de hacer llegar a tiempo la información que necesitan los distintos elementos de la organización empresarial (departamentos, áreas funcionales, equipos de trabajo, delegaciones etc.) permitiendo de esta forma una actuación conjunta y coordinada, ágil y orientada hacia los resultados.

Un sistema de Información se puede definir como un conjunto de elementos interrelacionados (Entre los que podemos considerar los distintos medios técnicos, las personas y los procedimientos) cuyo cometido es capturar datos, almacenarlos y trasformarlos de manera adecuada y distribuir la información obtenida mediante todo este proceso.

Un sistema de información realiza cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

Entrada de Información: Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas

son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfases automáticas. Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de diskette, los códigos de barras, los escáners, la voz, los monitores sensibles al tacto, el teclado y el Mouse, etc.

Almacenamiento de información: El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada.

Procesamiento de Información: Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.

Salida de Información: La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior.

Durante los próximos años, los Sistemas de Información cumplirán tres objetivos básicos dentro de las organizaciones:

1. Automatización de procesos operativos.
2. Proporcionar información para el apoyo al proceso de toma de decisiones.
3. Lograr ventajas competitivas a través de su implantación y uso.

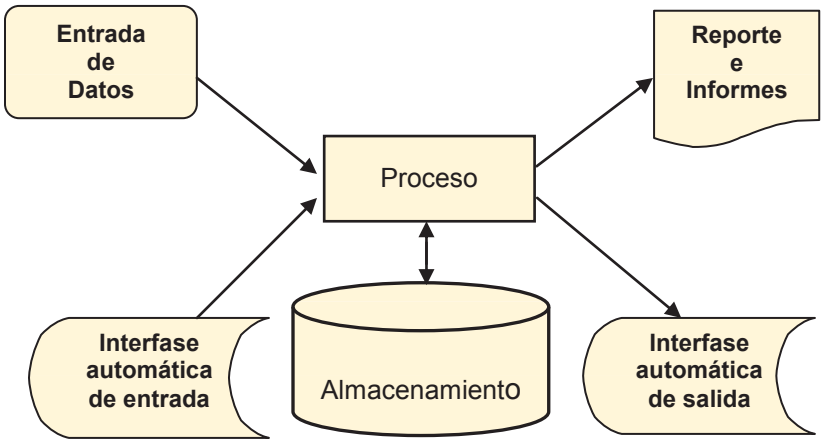


Fig. 4. Sistema de Información

Los Sistemas de Información que logran la automatización de procesos operativos dentro de una organización, son llamados frecuentemente Sistemas Transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas, etc.

2.1 CARACTERÍSTICAS DE LOS SISTEMAS DE INFORMACIÓN

Si tuviéramos que resumir con una sola frase el principal cometido de un sistema de Información dentro de una organización podríamos afirmas que este se encarga de entregar la información oportuna y precisa, con la presentación y el formato adecuado, a la persona que la necesita dentro de la organización para tomar una decisión o realizar alguna operación y justo en el momento en que esta persona necesita disponer de dicha información.

Hoy en día, la información debería ser considerada como uno de los mas valiosos recursos de una organización y el Sistema de Información es el encargado de que esta sea gestionada siguiendo criterios de Eficiencia y Eficacia.

2.2 PROCESO DE UN SISTEMA DE INFORMACIÓN.

Su propósito es apoyar y mejorar las operaciones cotidianas de la empresa, así como satisfacer las necesidades de información para la resolución de problemas y la toma de decisiones por parte de los directivos de la empresa.

Un sistema tiene Inputs (datos) y unos outputs (información), unos procesos de transformación de los inputs en outputs y unos mecanismos de retroalimentación, como se puede apreciar en la siguiente figura.

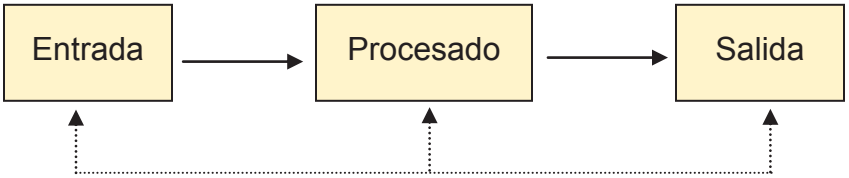


Fig. 5. Los proceso de los SI

La información facilita la integración y coordinación de las actividades que constituyen los distintos procesos de la organización, eliminando las barreras espaciales y temporales. De esta forma el sistema de información se convierte en el Sistema nervioso de la organización, ocupándose de capturar los hechos en cuanto se producen, ya sean estos internos o externos, procesar los datos obtenidos y comunicarlos a los distintos elementos de la organización para que puedan reaccionar a tiempo ante ellos

Los sistemas de información pueden ser manuales o computarizados. Hoy en día lo mas normal es que se de el segundo caso, es decir, que se recurra a un soporte informático (constituidos por elementos como el hardware, el software, las bases de datos, y los sistemas de telecomunicaciones) para la capturar los datos, procesarlos y presentar la información obtenida.

Sistemas de Información “Herramienta practica para la gestión empresarial”
Alvaro Gomez Vieites, Carlos Suarez Rey
2004, Alfaomega Grupo editor

2.3 TIPOS Y USOS DE LOS SISTEMAS DE INFORMACIÓN

Sistemas Transaccionales. Sus principales características son:

- A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas de la organización.
- Con frecuencia es el primer tipo de Sistemas de Información que se implanta.
- Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- Tienen la propiedad de ser recolectores de información
- Son fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.

Sistemas de Apoyo de las Decisiones. Las principales características de estos son:

- Suelen introducirse después de haber implantado los Sistemas Transaccionales más relevantes de la empresa.
- La información que generan sirve de apoyo a los mandos intermedios y a la alta administración en el proceso de toma de decisiones.
- Suelen ser intensivos en cálculos y escasos en entradas y salidas de información.
- No suelen ahorrar mano de obra.
- Suelen ser Sistemas de Información interactivos y amigables
- Apoyan la toma de decisiones que, por su misma naturaleza son repetitivos y de decisiones no estructuradas que no suelen repetirse
- Estos sistemas pueden ser desarrollados directamente por el usuario final

Sistemas Estratégicos. Sus principales características son:

- Su función primordial no es apoyar la automatización de procesos operativos ni proporcionar información para apoyar la toma de decisiones.

- Suelen desarrollarse dentro de la organización,
- Típicamente su forma de desarrollo es a base de incrementos y a través de su evolución dentro de la organización.
- Su función es lograr ventajas que los competidores no posean.

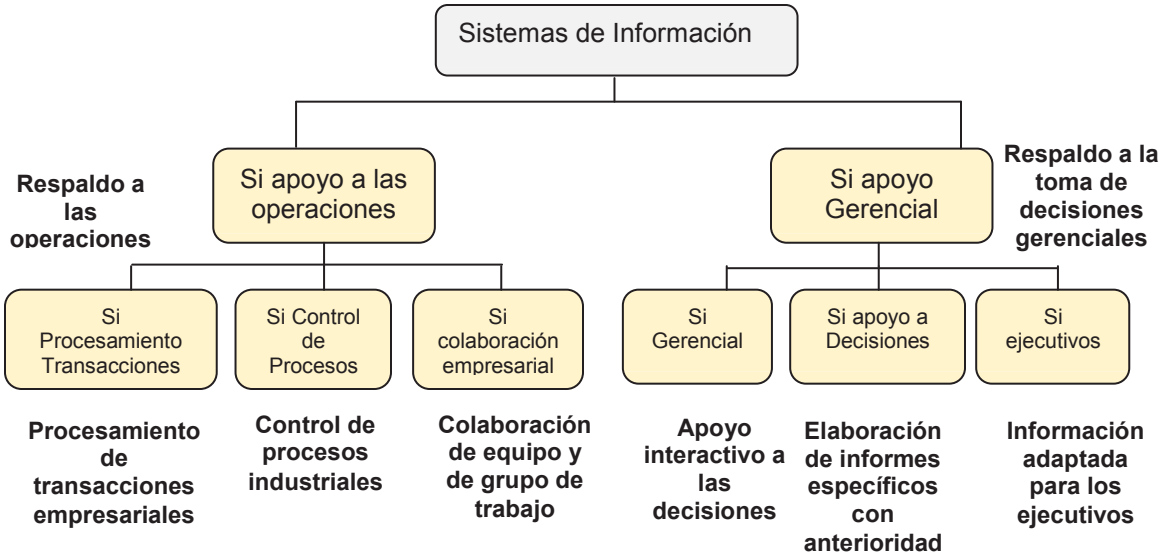


Fig. 6 Tipos de Sistema de información

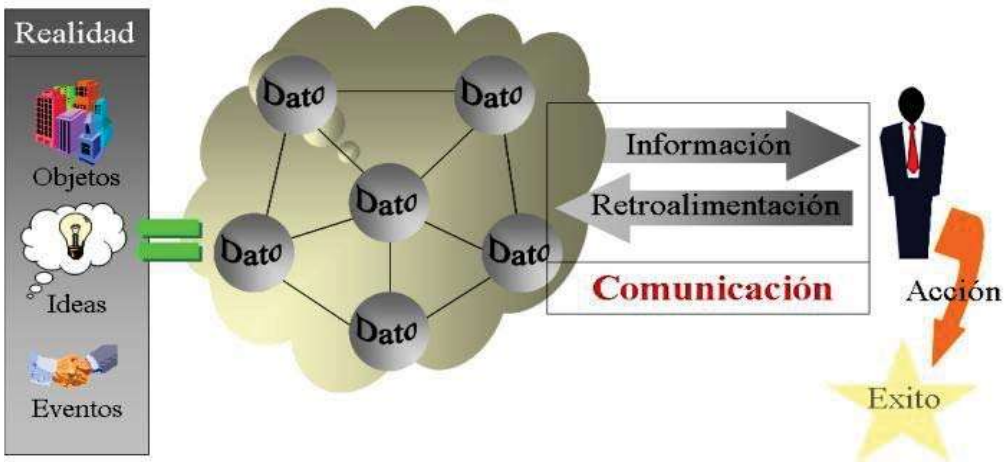


Fig. 7 Proceso de la información a través de los sistemas

Sergio Etcheverry G. S.I.A. I
03/06/07

2.4. SISTEMA DE INFORMACIÓN Y CONTROL A TRAVÉS DE INTERNET.

El control de procesos mediante Internet ha alcanzado en la actualidad un amplio interés en diferentes áreas de la industria. Actualmente es posible obtener resultados a distancia de alta calidad aprovechando la utilidad que brindan la Internet y el uso de las computadoras (PC). Generalmente el monitoreo a distancia se realiza con una estructura cliente – servidor en la que ambos deben poseer una aplicación en cada extremo de la conexión y así compartir información.

El Sistema de Monitoreo y Control mediante Internet puede ser manejado desde cualquier PC conectada a Internet y que cuente con un programa navegador. Dicha computadora (cliente) no requiere instalación alguna de controladores ó software específico para el manejo del Sistema.

Mediante este Sistema es posible monitorear y controlar procesos, es absolutamente configurable desde el cliente, respondiendo en forma automática a los cambios en el proceso, según los requerimientos configurados por el usuario. Las operaciones que controlan el Sistema son realizadas en el equipo Servidor, el cuál posee un Sistema Operativo de servidor y utiliza la tecnología ASP que le proporciona características de Sitio Web dinámico, ya que la información enviada por el cliente a través del explorador es interpretada y ejecutada en el Servidor, que realizará las acciones correspondientes sobre el Sistema, enviando finalmente los resultados al explorador del cliente.

Rafael Migueles, Roberto Williams.
Diciembre 2005, Facultad de Ingeniería,
Dpto. Electrónica,

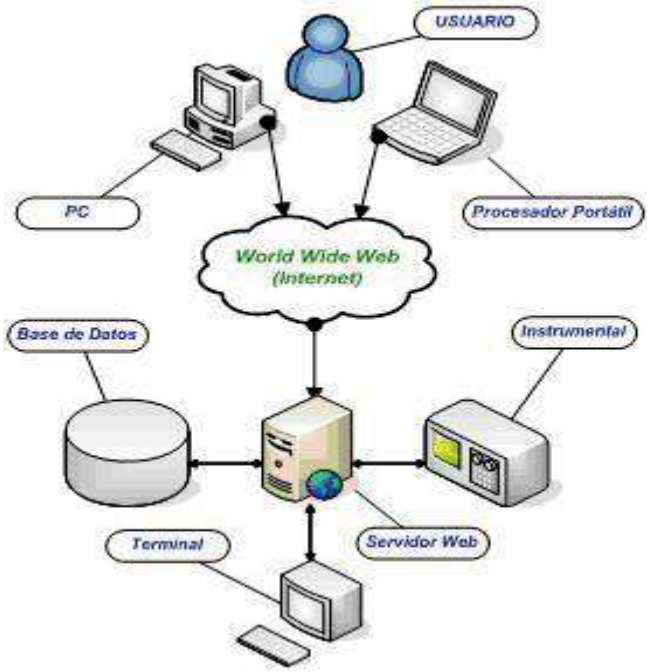


Fig. 8 Control de bases de datos a través de Internet

2.4.1 SERVICIOS DE ACCESO REMOTO.

Los empleados de las empresas desean cada vez más poder trabajar lejos de sus oficinas, ya sea en sus casas u otros lugares. El personal de ventas desea cada vez más poder accesar bases de datos y los administradores desempeñar sus funciones desde ubicaciones remotas.

De acuerdo a la importancia que han recobrado las redes, la capacidad de las personas para marcar y tener acceso a redes cada vez es más importante.

2.4.2 CLIENTE- SERVIDOR

Un servidor es una aplicación que ofrece un servicio a usuarios de Internet; un cliente es el que pide ese servicio. Una aplicación consta de una parte de servidor y una de cliente, que se pueden ejecutar en el mismo o en diferentes sistemas.

Los usuarios invocan la parte cliente de la aplicación, que construye una solicitud para ese servicio y se la envía al servidor de la aplicación que usa TCP/IP como transporte.

El servidor es un programa que recibe una solicitud, realiza el servicio requerido y devuelve los resultados en forma de una respuesta. Generalmente un servidor puede tratar múltiples peticiones (múltiples clientes) al mismo tiempo.

Los sistemas Cliente-Servidor pueden ser de muchos tipos, dependiendo de las aplicaciones que el servidor pone a disposición de los clientes. Entre otros, existen:

- Servidores de Impresión, mediante el cual los usuarios comparten impresoras.
- Servidores de Archivos, con el cual los clientes comparten discos duros
- Servidores de Bases de Datos, donde existe una única base de datos.
- Servidores de Lotus Notes, que permite el trabajo simultáneo de distintos clientes con los mismos datos, documentos o modelos.
- Los *Servidores Web* también utilizan la tecnología Cliente- Servidor, aunque añaden aspectos nuevos y propios a la misma.

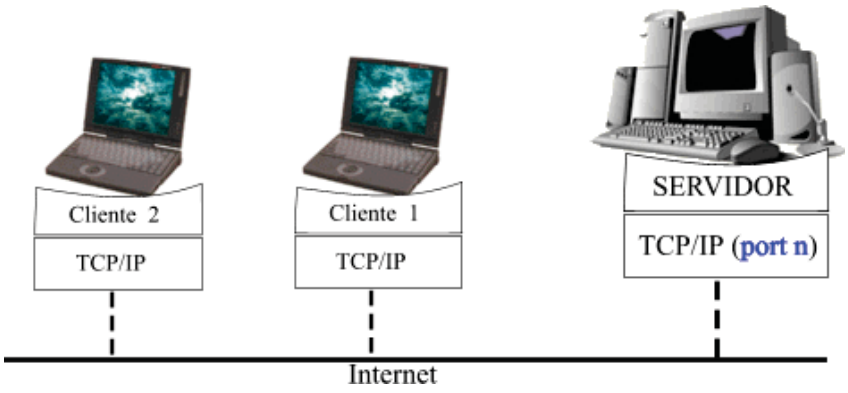


Figura 9. El modelo de aplicación cliente/servidor

3. RED INFORMATICA

Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

Una red tiene tres niveles de componentes: software de aplicaciones, software de red y hardware de red. El software de aplicaciones está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco). Un tipo de software de aplicaciones se denomina cliente-servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otras computadoras llamadas servidores, que controlan datos y aplicaciones. Otro tipo de software de aplicación se conoce como 'de igual a igual' (peer to peer). En una red de este tipo, los ordenadores se envían entre sí mensajes y peticiones directamente sin utilizar un servidor como intermediario.

El software de red consiste en programas informáticos que establecen protocolos[3], o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

El hardware de red está formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (típicamente cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que

[3] **Protocolo**: conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

3.1 MEDIOS DE TRANSMISIÓN DE LA INFORMACION

La comunicación es la transferencia de información desde un lugar a otro. Por otra parte la información es un patrón físico al cual se le ha asignado un significado comúnmente acordado. El patrón debe ser único "separado y distinto", capaz de ser enviado por un transmisor y capaz de ser detectado y entendido por un receptor. La información es transmitida a través de señales eléctricas o por medio de señales ópticas a través de un canal de comunicación o medio de transmisión.

El medio de transmisión es el enlace eléctrico ú óptico entre el transmisor y el receptor, siendo el puente de unión entre la fuente y el destino. Este medio de comunicación puede ser un par de alambres, un cable coaxial, inclusive el aire mismo. Pero sin importar el tipo, todos los medios de transmisión se caracterizan por la atenuación, ruido, interferencia, desvanecimiento y otros factores muy importantes que impiden que la señal sea propagada libremente por el medio. Todos estos factores son los que hay que contrarrestar al momento de transmitir cualquier información al canal con ruido.

Por otro lado, existen los medios no-físicos o no-confinados, es decir no están contenidos en ninguno de los materiales descritos anteriormente. Los medios no físicos o no-confinados son aquellos donde las señales de radio frecuencia (RF) originadas por la fuente se radian libremente a través del medio y se esparcen por éste " el aire por ejemplo. El medio, aire, es conocido técnicamente como el espectro radioeléctrico o electromagnético. Comúnmente conocemos a este tipo de medios como medios inalámbricos; del inglés *wireless* o sin alambres.

3.1.1 MEDIOS CONFINADOS

En los medios confinados tenemos en primer lugar al alambre sin aislar. El alambre fue el primer medio de comunicación empleado tras haberse inventado el telégrafo en 1844. Hoy en día los alambres vienen protegidos con materiales aislantes. El material del conductor puede ser cobre, aluminio u otros materiales conductores y se emplea en conducción de electricidad, telefonía, redes, etc.

Los grosores de los cables son medidos de diversas maneras, el método predominante en los Estados Unidos y en otros países sigue siendo el *American Wire Gauge Standard* (AWG), "gauge" significa diámetro. Mediante este sistema se puede distinguir un cable de otro mediante su diámetro. El grosor del cable determina otras características eléctricas importantes: resistencia o impedancia.

3.1.2 CABLE COAXIAL

Este tipo de cable consiste de un conductor central fijo sobre un forro de material aislante, que después lleva una cubierta metálica en forma de malla como segundo conductor. La capa exterior evita que las señales de otros cables o que la radiación electromagnética afecte la información conducida por el cable coaxial.

Fig. 10 cable coaxial

Los dos tipos de cables coaxiales más empleados para aplicaciones de LAN son el 10Base5 y el 10Base2. El 10Base5 es conocido comúnmente como cable coaxial grueso, en cambio el 10Base2 es conocido como cable coaxial delgado.

3.1.3 CABLE PAR TRENZADO

El cable par trenzado (twisted pair) está compuesto de conductores de cobre aislados por material plástico y trenzados en pares. Este trenzado ayuda a disminuir la diafonía, el ruido y la interferencia. El trenzado es en promedio de tres trenzas por pulgada. Para mejores resultados, el trenzado debe ser variado entre los diferentes pares. Este tipo de cables de par trenzado tienen la ventaja de no ser caros, ser flexibles y fáciles de conectar, entre otras más propiedades que no las tiene el coaxial en las aplicaciones de redes. Como medio de comunicación tiene la desventaja de tener que usarse a distancias limitadas (menos de 100 metros) ya que la señal se va atenuando y puede llegar a ser imperceptible si se rebasa ese límite.

Fig. 11 Cable par trenzado

Los cables de par trenzado más comúnmente usados como interfaces de capa física son los siguientes: 10BaseT (Ethernet), 100BaseTX (Fast Ethernet), 100BaseT4 (Fast Ethernet con 4 pares) y 1000BaseT (Gigabit Ethernet).

Existen dos tipos de cable par trenzado, el UTP (Unshielded Twisted Pair Cabling), o cable par trenzado sin blindaje y el cable STP (Shielded Twisted Pair Cabling), o cable par trenzado blindado.

3.1.4 FIBRA ÓPTICA

La fibra óptica es muy medio de comunicación que utiliza la luz confinada en una fibra de vidrio para transmitir grandes cantidades de información en el orden de Gigabits ($1x10^9$ bits) por segundo. Para transmitir los haces de luz se utiliza una fuente de luz como un LED (Light-Emitting Diode) o un diodo láser. En la parte receptora se utiliza un fotodiodo o fototransistor para detectar la luz emitida. También será necesario poner al final de cada extremo un conversor de luz (óptico) a señales eléctricas.

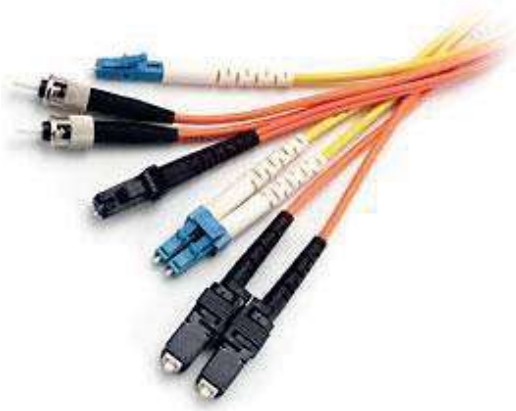


Fig. 12 Fibra óptica

Debido a que el láser trabaja a frecuencias muy altas, entre el intervalo de la luz visible e infrarroja, la fibra óptica es casi inmune a la interferencia y el ruido.

La transmisión óptica involucra la modulación de una señal de luz " usualmente apagando, encendiendo y variando la intensidad de la luz " sobre una fibra muy estrecha de vidrio llamado núcleo " el diámetro de una fibra puede llegar a ser de una décima del diámetro de un cabello humano.

La otra capa concéntrica de vidrio que rodea el núcleo se llama revestimiento. Después de introducir la luz dentro del núcleo ésta es reflejada por el revestimiento, lo cual hace que siga una trayectoria *zigzag* a través del núcleo. Por lo tanto las dos formas de transmitir sobre una fibra son conocidas como transmisión en *modo simple* y *multimodo*. En el modo simple o monomodo, se transmite un haz de luz por cada fibra, mientras en una fibra multimodo más de

un haz de luz puede ser transmitido. Dada las características de transmisión de las fibras monomodo, es posible la propagación del haz de luz a decenas de kilómetros. Este tipo de fibra es comúnmente utilizada para enlaces de larga distancia, por ejemplo la interconexión de centrales telefónicas. La fibra multimodo en cambio se utiliza para distancias más cortas y sirve para interconectar redes de área local entre edificios, intercampus, etc.

La tecnología de la fibra óptica ha avanzado muy rápidamente y en la actualidad es posible incrementar la capacidad de una fibra y aumentar la distancia de propagación.

La fibra óptica como medio de transmisión en el área de las telecomunicaciones ha demostrado su potencialidad al cursar por éstas casi todo el tráfico de voz y datos del mundo, así como el tráfico de Internet. Pero también en el campo de la medicina la fibra óptica tiene un uso muy vasto, la *laparoscopía, colposcopía* y la *endoscopía* son sólo unos ejemplos.

3.1.5 MEDIOS NO-CONFINADOS

Los medios no-confinados utilizan el aire como medio de transmisión, y cada medio de transmisión viene siendo un servicio que utiliza una banda del espectro de frecuencias. A todo el rango de frecuencias se le conoce como espectro electromagnético. El espectro electromagnético ha sido un recurso muy apreciado y como es limitado, tiene que ser bien administrado y regulado.

Fig. 13. Antena receptora de transmisión

3.1.6 MICROONDAS TERRESTRES

Las microondas son todas aquellas bandas de frecuencia en el rango de 1 GHz en adelante, el término microondas viene porque la longitud de onda de esta banda es muy pequeñ (milimétricas o micrométricas), resultado de dividir la velocidad de la luz ($3x10^8$ m/s) entre la frecuencia en Hertz[4]. Pero por costumbre el término microondas se le asocia a la tecnología conocida como microondas terrestres que utilizan un par de radios y antenas de microondas.

Fig. 14 Microondas terrestres

Los operadores tanto de redes fijas como móviles están utilizando las microondas para superar el cuello de botella de la última milla de otros medios de comunicación. Las estaciones de microondas consisten de un par de antenas con línea de vista conectadas a un radio transmisor que radian radio frecuencia (RF) en el orden de 1 GHz a 50 GHz. Las principales frecuencias utilizadas en microondas se encuentran alrededor de los 10-15 GHz, 18, 23 y 26 GHz, las cuales son capaces de conectar dos localidades de hasta 24 kilómetros de distancia una de la otra. Los equipos de microondas que operan a frecuencias más bajas, entre 2-8 GHz, puede transmitir a distancias entre 30 y 45 kilómetros. La única limitante de estos enlaces es la curvatura de la tierra, aunque con el uso de repetidores se puede extender su cobertura a miles de kilómetros.

Evelio Martínez Martínez, (15 de octubre de 2008)
Publicado en la Revista RED en la edición especial
"El ABC de las Telecomunicaciones", Diciembre del 2002

[4] **Hertz**: Unidad de frecuencia (número de veces que se repite por segundo cualquier fenómeno) electromagnética

4. SEGURIDAD DE LA INFORMACIÓN

Dentro de un organismo han sufrido principalmente dos cambios en las últimas décadas, antes de que se extendiera la utilización de los grupos de procesamiento de datos, la seguridad de la información. Por ejemplo el uso de cajas fuertes con combinación de apertura para almacenar documentos confidenciales.

Con la introducción de las computadoras, fue evidente la necesidad de herramientas automáticas para proteger ficheros y otra información almacenada en computadores. Este es especialmente el de los sistemas multiusuarios, como con los sistemas de tiempo compartido la necesidad es mas para los sistemas a los que se puede acceder desde teléfonos públicos o redes de datos. El termino general del campo que trata las herramientas diseñadas para proteger los datos y frustrar a los piratas informáticos es seguridad en computadores.

El segundo cambio relevante, que ha afectado a la seguridad, es la introducción de sistemas distribuidos y la utilización de redes y facilidades de comunicación para trasportar datos entre terminales de usuarios y computador y de computador a computador. Las medidas de seguridad en red son necesarios para proteger los datos durante su trasmisión y garantizar que los datos sean auténticos.

Virtualmente la tecnología esencial subyacente en todas las redes automáticas y las aplicaciones de seguridad en computadores es el cifrado.

Comunicaciones y Redes de Computadores
William Stallings
6ta edición, Ed. Prentice Hall, 2000

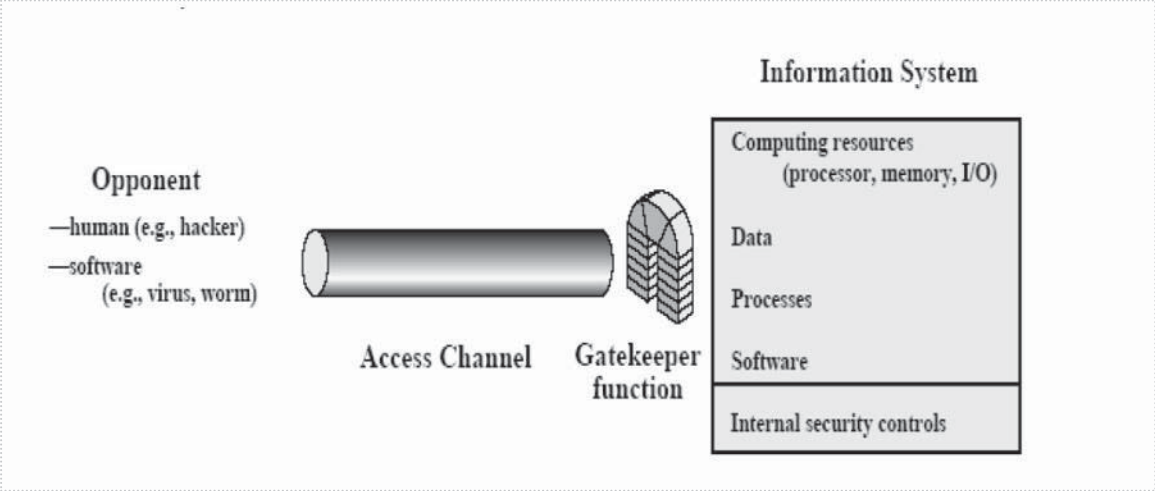


Fig. 15 Modelo de seguridad en acceso a redes

El intruso puede realizar varios tipos de ataques:

- Disponibilidad del sistema.
- Averiguar información confidencial.
- Falsificar el contenido o la identidad de origen de un mensaje.
- Cambiar de orden.
- Retener un mensaje.
- Analizar flujo de tráfico.

B. Alarcos, E. de la Hoz
Universidad de Alcala
Dpto. de Automatica

4.1 IMPORTANCIA, LA SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS

Una empresa es un organismo. Vive, respira, muta, crece. Durante la vida de una empresa se notan épocas de crecimiento y re organización que en forma cíclica marcan su pulso.

Generalmente, cuando una empresa comienza su crecimiento se presenta todo un análisis por parte de la gerencia general en el cual se redunda en explicaciones de visión, misión y valores a fin de poder poner un rumbo a ese organismo que o bien está pasando un buen momento y no lo aprovecha del todo o está mal y hay que levantarlo con algún antibiótico.

En estos momentos, una decisión inteligente es la de pensar cuales son los recursos con los que se cuenta tanto humanos como de producción. Pero hay algo que muchas organizaciones se olvidan. Su capital tecnológico.

Pensar en cualquier PYME[5] sin recursos de tecnología (llamese comunicación, equipamiento informático, capacidad humana para mantenerla, etc) es sentenciarla a muerte, ya que las actividades requieren un uso exhaustivo de estos recursos.

Este problema se presenta más en empresas las cuales no son de tecnología (aunque he visto cumplirse el dicho en casa de herrero cuchillo de palo) las cuales al no tener un enfoque de su negocio en esta área, requieren de personal o terceros que los asesoren y casi siempre sus sugerencias son tomadas como “gasto” en lugar de “inversión”.

El problema es que solo notan que existe un área de sistemas cuando algo no funciona y si se tiene un buen personal de sistemas, puede ser que hasta se olviden como se llama el “chico que anda con cables”.

La información que llega a los tomadores de decisión de estas PYMES tendría que ser suficiente como para conocer esta situación, sin embargo muchas veces se sigue dejando de lado a la tecnología en aspectos generales como el pensar

[5] **PYMES**: Pequeña y medianas empresas

una nueva imagen de la organización o generar estrategias que permitan llevar a la empresa hasta el próximo nivel.
El personal de sistemas o la empresa o persona tercerizada es un aliado que tiene que ser tomado en cuenta para tomar decisiones siendo estos quienes conocen la técnica que permitirá reducir costos y brindar mejores servicios, tanto dentro como fuera de la empresa.

El problema con la seguridad hoy por hoy está en las PYMES ya que tienen poco o ningún presupuesto asignado, cuentan con una sola persona (que además tiene que hacer otras tareas administrativas) o tienen contratada a una empresa o a alguna persona la cual puede o no conocer todas las actividades de la empresa y mucho menos de los empleados.
Esta situación es conocida por las personas que son "amigo de lo ajeno informático" al punto que son las PYMES las que están recibiendo la mayor cantidad de ataques en forma de SPAM[6], phishing, spyware y gusanos que roban información.

Se podrán preguntar para que lo hacen. Simple. Un rédito económico. Los empleados usan las computadoras de la empresa para pagar impuestos, comprar con tarjeta de crédito o entrar a su home bancking[7]. Esto es más apetitoso que una gran víctima más grande y presenta menos riesgo (así como mayor facilidad) la obtención de tan preciado botín como un numero de Visa.
El error más común es pensar que no se tiene ningún dato que pueda ser de interés para esta gente, cuando la realidad y las cifras nos muestran que son su plato fuerte. La tecnología y la seguridad para su uso, son las herramienta que tienen que estar presentes en cada decisión gerencial y ser tenidas en cuenta para hacerla crecer al mismo nivel que se quiere hacer crecer a la organización.

[6] **SPAM**: Correo basura, los mensajes no solicitados, habitualmente de tipo publicitario.

[7] **Home banking**: Servicio del banco a través de Internet.

En la actualidad, más del 70% de las compañías están infectadas con malware[8] (Malicius software), es decir, están expuestas a situaciones tales como la pérdida de datos importantes, lo cual puede provocar la detención de los negocios o hasta el quiebre de una empresa, según un estudio de investigación realizado por PandaLabs en 2007.

En nuestro país, la mayoría de las grandes compañías tiene muy claro la importancia y las ventajas de contar con una seguridad informática de alto nivel al interior de su empresa. Por lo tanto, es común el delegar la seguridad en partners tecnológicos, dedicándose así a su core business en un 100%.

En el 2006, el presupuesto de inversión en Tecnologías de Información (TI) como porcentaje de la facturación era de un 2,24%, y según el último Estudio Nacional de Tecnologías de la Información (ENTI) 2008, la cifra llegó al 2,28%. Esto demuestra que las compañías aún no valoran a las TI como una herramienta clave del negocio, ya que en países desarrollados estas cifras son cercanas al 4%.

Es más, aún un porcentaje de empresas cree que tomando medidas tales como instalar un antivirus o firewalls y evitando navegar en algunos sitios, no tendrán virus, ataques o pérdida de información vital.

Si sumamos a esta falsa sensación de seguridad, la falta de información, podemos dar cuenta de por qué existe un gran incremento de la exposición de las empresas a virus, spyware y a otras amenazas de internet e inclusive desde sus mismas redes internas, que pueden tener graves consecuencias.

Por estos motivos se hace fundamental, la generación de conciencia de lo significa la seguridad de la información en las empresas. Es conocida la

[8] **Malware**: Es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades maliciosas

situación de que sólo alrededor de un 30% de las grandes empresas tienen una sección dedicada a la seguridad de la información, otras solo cubren aspectos limitados como ser la seguridad informática. Sin embargo, queda un 70% de éstas empresas, en donde no se dispone de ninguna de las dos áreas mencionadas o dependen de gerencias inadecuadas que no pueden garantizar las inversiones necesarias, las capacitaciones internas, la definición e instrumentación de procesos y los planes de auditorías.

Los especialistas de seguridad se preocupan cada vez más en definir controles relacionados con los servicios de seguridad perimetral, avanzada y de contenidos a nivel aplicativo. De esta forma, tienen la posibilidad de realizar un seguimiento proactivo de los eventos, realizar análisis y reportes de vulnerabilidades así como los típicos “penetration tests”, entre otras cosas.

Una recomendación general como compañía especializada en esta área, es realizar un seguimiento proactivo del comportamiento anómalo que hay en las redes, e incluso llevar a cabo auditorías de seguridad frecuentemente, muy necesarias en estos tiempos debido a la gran actividad que hay en el mundo del underground.[9]

Marcelo Gimenez, 5/09/2008,
Regional Technology and Operations Security Manager,
Global Crossing Latin America

En 2007 hubo más de 2 mil acciones de hackers[10] para robar información personal; las instituciones bancarias son las más atacadas: PFP
Ante los daños que han afectado los bienes, recursos económicos, identidad y reputación de las personas, es fundamental trabajar en la seguridad de los

[9] **Underground:** Lo que no se debería saber"(ya que puede causar conmoción popular o porque el mal uso de esa información puede llegar a causar problemas) todo tipo de información cubierta por el Gobierno, la NASA, el FBI, la CIA, la DEA, la policía, los bancos y todo aquel que esta en contra del libre flujo de la información.

[10] **Hackers**: Termino utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática.

usuarios de Internet en México, señaló Alejandro Pisanty Baruch, titular de la Dirección General de Servicios de Cómputo Académico (DGSCA), de la UNAM. Sostuvo que en el mundo hay 22 millones de usuarios directos de la red, pero aproximadamente mil 500 millones de personas la utilizan en todo el mundo.

Hay una sociedad que depende de las tecnologías de la información y de la comunicación permanente y ubicua, agregó.
"somos parte de la construcción de una cultura de seguridad en el manejo de la información y la tecnología con que actualmente se manipula ésta".
Señaló que desde su primera versión (hace 12 años) el Congreso se ha propuesto discutir, informar y cuestionar los métodos de seguridad que existen en un medio tan difundido como Internet.
Instituciones afectadas

Por su parte, Juan Carlos Guel López, jefe del Departamento de Seguridad en Cómputo de la UNAM, y Eduardo Zepeda Estrada, de la Policía Federal Preventiva (PFP), apuntaron que el año pasado se registraron en el país 2 mil 50 casos de phishing, que es un conjunto de técnicas y mecanismos empleados por los intrusos o hackers con el propósito de robar información personal de un usuario y suplantar su identidad.

Señalaron que en los primeros cuatro meses de 2007 se han detectado al menos 600 casos, mientras que el año pasado el mayor número de reportes se presentó entre agosto y octubre.
Las instituciones mexicanas más afectadas fueron las bancarias. En Banamex se reportaron 72 por ciento de los casos; en Santander Serfin, 4 por ciento, y en el Banco de Bajío, 1.7 por ciento. Los especialistas en delitos cibernéticos que participaron en este encuentro propusieron a las instituciones financieras crear un equipo de respuesta a incidentes de seguridad para compartir experiencias y tratar de encontrar los mecanismos para contrarrestar estos delitos.

(La Jornada), México, DF 08/06/2007

Los sitios de Internet requieren de sistemas de seguridad adecuados para evitar cualquier fuga de información o robo de la misma por terceras personas. De la misma forma, el usuario requiere estar familiarizado con las medidas básicas para su propia protección en la red, pues muchas veces puede ser el eslabón más débil en esta comunicación y ser víctima de los conocidos fraudes cibernéticos, una problemática importante y un factor nodal en la economía mundial.

Miko Hypponen, jefe de investigación de F-Secure Corporation (grupo especializado en detección y prevención de crímenes corporativos) asegura que los delitos financieros por Internet, representan la actividad con mayor crecimiento en la industria de las Tecnologías de la Información y Comunicación (TIC), tal y como lo demuestran estudios recientes realizados por diversas compañías proveedoras de servicios de seguridad para corporativos y usuarios en general.

Entre enero y junio de 2008, las principales amenazas de malware, detectadas por la empresa Bitdefender, fueron los correos masivos y los troyanos que se han convertido en los tipos más populares de infección para cometer cualquier tipo de fraude en sistemas de búsqueda de información.

La compañía de soluciones antivirus Trend Micro emitió un reporte hace unos días donde afirma que el spam representa el 90% de todo el correo electrónico que circula en la WWW[11], mientras Viruslist, otra empresa del ramo de seguridad informática, señala que los rubros más afectados por este ilícito son: salud, medicamentos, servicios, educación, computadoras, Internet, viajes y turismo.

Miko Hypponen, quien recientemente dictó una ponencia en el Congreso de Seguridad en Cómputo, organizado por la UNAM a través de la DGSCA y su Departamento de Seguridad en Cómputo, se refirió a técnicas como el spam.

[11] **WWW**: Red Global Mundial es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.

Explicó que dada la ingeniería social usada por los difusores y la falta de legislación global o acuerdos internacionales para combatirlo, los spammers continúan enriqueciéndose y poco se puede hacer para combatirlos.

En México, el Sistema de Pagos Electrónicos Interbancarios (SPEI) es una alternativa propuesta por el Banco de México (Banxico), para agilizar y conectar todo el sistema financiero nacional a través de transacciones seguras por Internet. Con este sistema se garantizan las transacciones financieras en línea, en tiempo y forma, con información encriptada y niveles de seguridad basados en estándares mundiales, lo que evita el robo de identidades o credenciales bancarias. Por ejemplo, se tiene conocimiento de diversos tipos de malware que sustraen información personal y financiera de las personas, lo cual facilita a los criminales realizar ilícitos a nombre de los usuarios.

Según la empresa de seguridad Web Finjan, a través de sistemas de malware, se registraron medio millón de infecciones satisfactorias en un mes, con un paquete de herramientas muy “creativo” que puede robar información bancaria como nombres de usuario, contraseñas, números de tarjeta de crédito y números de seguridad social sin dejar huella.

El phishing es otro tipo de fraude que implica un grave problema para los usuarios de la banca en línea. Según Hypponen, los países donde más se practica este ilícito son Estados Unidos, Corea del Sur, India y China. En América Latina, Brasil es la nación con el mayor índice de casos registrados.

El reporte de Consumer, en Estados Unidos, indica que en ese país se registró una pérdida de más de siete millones de dólares en los últimos dos años, debido a delitos como el phishing scam, virus y spyware, porque gran parte de los cibernautas de esa región han sucumbido a contestar o aceptar este tipo de prácticas que consideran lícitas.

Como señala Miko Hypponen, estas actividades han dejado de ser propias de algunos personajes solitarios que en sus ratos de ocio se encargaban de estafar a usuarios; hoy en día, existen verdaderas organizaciones criminales que ya presuponen una delincuencia organizada.

“Quienes cometen este tipo de delitos y abusos son personas que han visto en este tipo de prácticas un negocio redituable, y muchos de ellos tienen que considerárseles como delincuentes de cuello blanco, pues actúan desde una posición directiva dentro de alguna industria de las TIC”, resaltó Hypponen.

Sin embargo, mientras algunas naciones promueven y ejecutan la legislación al respecto, otras no consideran urgente tener este tipo de leyes que protejan a los usuarios de los fraudes en la red, por lo tanto, sin respaldo legal, poco se puede hacer para combatir este tipo de prácticas.

Hace unos días fue detenido y condenado a 30 años de cárcel en Estados Unidos, Christopher William Smith, quien obtuvo 24 millones de dólares por vender medicamentos vía Internet, mediante publicidad enviada a través de correo electrónico no solicitado o spam.

El delito cibernético tiene muchas aristas, cada día surgen nuevas y sofisticadas formas de cometerlo. Son las instituciones públicas, privadas y de educación, además de los diversos corporativos existentes en cada país, los responsables de capacitar y difundir las medidas necesarias para la protección de su personal y su información.

Crimen en línea, Rubén Aquino Luna
Gustavo Alberto Gutiérrez Ramírez, 27 /11/2008
Año 7 Núm. 74, Publicación Mensual,

4.2 AMENAZAS A LA SEGURIDAD DE UNA RED.

Para entender los tipos de amenazas a la seguridad que existen conviene definir los requisitos de seguridad. La seguridad en computadores y en redes implica tres requisitos:

- **Secreto**: requiere que la información en un computador sea accesible para lectura solo por los entes autorizados. Este tipo de acceso incluye la impresión, mostrar en pantalla y otros formas de revelacion que incluye cualquier forma de dar a conocer la existencia de un objeto.
- **Integridad:** Requiere que los recursos de un computador sean modificados solamente por entes autorizados, la modificacion incluye escribir, cambiar, cambiar de estado, suprimir y crear.
- **Disponibilidad:** requiere que los recursos de un computador estesn disponibles a los entes autorizados.

Ataques pasivos: Son del tipo escuchadas, monitorizaciones, de las trasmisiones. La meta del oponente es obtener información que esta siendo trasmitida. Existen dos tipos de agresiones: divulgación del contenido de un mensaje y análisis del tráfico.

La divulgación del contenido de un mensaje: Una conversación telefónica, un mensaje de correo electrónico, un fichero trasferido puede contener información sensible o confidencial. Así, será deseable prevenir que el oponente se entere del contenido de estas trasmisiones.

Análisis del trafico: Es mas sutil, supongamos que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de trafico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado.

Pero incluso si tenemos protección de cifrado el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se esta realizando.

Los ataques pasivos son muy difíciles de detectar ya que no implica la alteración de los datos. Sin embargo. Es factible prevenir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones esta en la prevención antes que la detención.

Ataques Activos: Los ataques activos suponen alguna modificación del flujo de datos o la creación de flujos falsos y se subdivide en 4 categorías: enmascaramiento, repetición, modificación de mensajes y denegación de un servicio.

Un enmascaramiento: Tienen lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo se puede captar una secuencia de autentificación y reemplazarla por otra secuencia de autentificación valida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La repetición: Supone la captura pasiva de unidades de datos y su retransmisión subsecuente para producir un efecto no autorizado.

La modificación de mensajes: Significa sencillamente que alguna porción de un mensaje legitimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo un mensaje con un significado: Permitir a “Juan Smith leer el fichero confidencial de cuentas” se modifica para

tener el significado “Permitir a Omar Guzmán leer el fichero confidencial de cuentas”

La denegación de un servicio inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular, la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

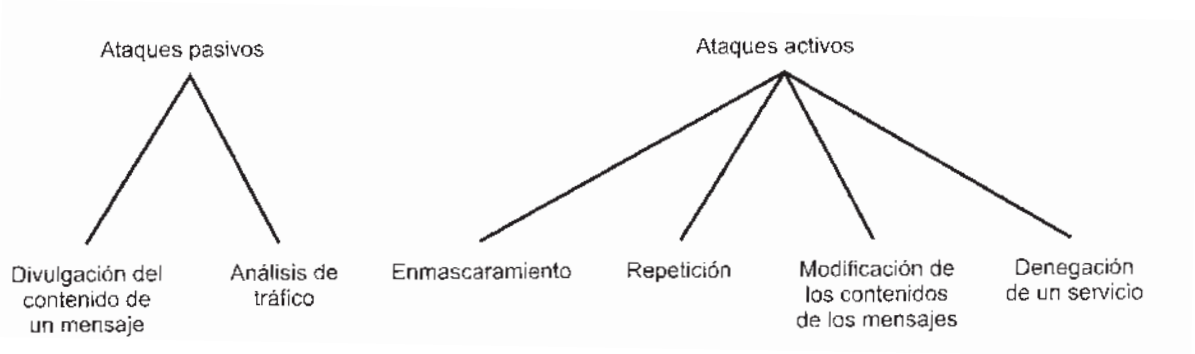


Fig. 16 Ataques activos y pasivos

Existen dos enfoques para atacar el esquema del cifrado convencional.

El primer ataque se conoce como criptoanálisis, se basa en la naturaleza del algoritmo más quizás algún conocimiento de las características generales del texto nativo o incluso de algunos pares texto nativo-texto cifrado. Este tipo de ataque explota las características del algoritmo para intentar deducir un texto nativo especifico o deducir la clave que se esta utilizando. Si el ataque tiene éxito en deducir la clave, el efecto es catastrófico: todos los mensajes cifrados antiguos y futuros con esa clave están comprometidos.

El segundo método, conocido como ataque de fuerza bruta, es intentar cada clave posible en un trozo de texto cifrado hasta que se obtenga una traducción de texto nativo.

Tamaño de la clave (bits)	Número de claves alternativas	Tiempo necesario a 1 cifrado/μs	Tiempo necesario a 10^6 cifrados/μs
32	$2^{32} = 4{,}3 \times 10^{9}$	2^{31} μs = 35,8 minutos	2,15 milisegundos
56	$2^{56} = 7{,}2 \times 10^{16}$	2^{55} μs = 1.142 años	10,01 horas
128	$2^{128} = 3{,}4 \times 10^{38}$	2^{127} μs = $5{,}4 \times 10^{24}$ años	$5{,}4 \times 10^{18}$ años
168	$2^{168} = 3{,}7 \times 10^{50}$	2^{167} μs = $5{,}9 \times 10^{36}$ años	$5{,}9 \times 10^{30}$ años

Fig. 17 Tamaño de claves y tiempo en descifrar

La tabla muestra los resultados para cada tamaño de clave, suponiendo que se tarda 1 µs[12]. en llevar a cabo un único descifrado, que es un orden de magnitud razonable para los computadores de hoy en día.

Comunicaciones y Redes de Computadores
William Stallings
6ta edición, Ed. Prentice Hall, 2000

4.3 MÉTODOS USADOS PARA ROBAR INFORMACIÓN.

A continuación, se exponen dos de los principales métodos actuales para obtener información personal de usuarios. El primero de ellos, el phishing, hace referencia a la obtención de información confidencial en sitios web, y el segundo, los troyanos bancarios (bankers) refieren a la utilización de códigos maliciosos para el mismo fin.

El phishing es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente involuntaria y fraudulenta, datos personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social.

Los primeros casos de phishing a entidades bancarias fueron reportados en Estados Unidos durante el 2003 y desde entonces, esta modalidad delictiva se ha ido diseminando a lo largo del planeta, constituyendo en la actualidad una de las principales amenazas para cualquier sitio que maneje información confidencial.

[12] **µs**: Es la abreviación de microsegundo es la millonésima parte de un segundo, 10^{-6} s

La mayoría de los casos de ataques de phishing se presentan ante los usuarios en forma de correo electrónico masivo (spam) invitándolo a ingresar a un sitio web similar al de la entidad financiera para solicitarle información confidencial (usuario, contraseña, PIN, número de tarjeta de crédito, etc).

Los Códigos Maliciosos: A continuación, se exponen aquellos tipos de ataques de malware más representativos de la actualidad haciendo referencia a su línea evolutiva a largo del tiempo.

Backdoor: A finales de los '90, las aplicaciones backdoor, como Sub7 o BackOriffice [2], dieron origen al robo de información de forma remota. Dichas aplicaciones poseían componentes que permitían interceptar cualquier tipo de información y enviarla al atacante a través de la red. En ese momento, la información relacionada a tarjetas de crédito podía ser parte de los objetivos de las personas malintencionadas que utilizaban estas aplicaciones, para luego usar esos datos para adquirir distintos servicios y/o productos en forma fraudulenta, perjudicando directamente al dueño real de la tarjeta.

Keylogger: Estas aplicaciones son troyanos y se caracterizan por poseer la capacidad de capturar y monitorear, de manera oculta, todo aquello que se escribe a través del teclado e incluso con el clic del mouse. Además, existen dispositivos físicos que se acoplan a modo de adaptadores al equipo y cuyas funcionalidades son similares a las de un keylogger de software.

Un atacante busca instalar keyloggers en el sistema de la víctima y configurarlo para que le envíe toda la información que haya capturado y almacenado, incluyendo las contraseñas de acceso a diferentes servicios, como por ejemplo el Home Banking[13].

[13] **Banca en línea:** es la banca a la que se puede acceder mediante Internet. Pueden ser entidades con sucursales físicas o que sólo operan por Internet o por teléfono.

Troyanos bancarios (bankers) La evolución de los códigos maliciosos fue dando origen a nuevas estrategias de engaño que permiten obtener información particular de las computadoras comprometidas a través de troyanos. Debido a sus características singulares, algunos de estos códigos maliciosos, reciben el nombre genérico de troyanos bancarios, ya que su objetivo general es obtener información bancaria de los usuarios.

Virus: "Programas informáticos o secuencias de comandos que intentan propagarse sin el consentimiento y conocimiento del usuario" (Fuentes, 2006) y que realizan alguna acción maliciosa. Entre sus principales características podemos identificar las siguientes:

- Se presentan como archivos ejecutables, o han adherido su código malicioso a imágenes, hojas de cálculo o documentos.
- No pueden reproducirse por sí mismos, es decir para infectar otras computadoras es necesario que el usuario intervenga.
- Llevan a cabo una actividad maliciosa

Caballo de troya (troyano): "Programa de computadora que aparenta tener una función útil, pero que contiene código posiblemente malicioso para evadir mecanismos de seguridad, a veces explotando accesos legítimos en un sistema."

Gusanos: "Son programas que buscan propagarse lo más rápido posible tratando de infectar el mayor número posible de equipos, lo que en ocasiones tiene como consecuencia el colapso de las comunicaciones en la red."

***Bot*:** "Programa o *script* que realiza funciones que de otra manera habría que hacer manualmente. También se refiere a una computadora que ha sido comprometida y que ejecuta las instrucciones que el intruso ordena."

***Spyware*:** "También conocido como programa espía y comúnmente se refiere a aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario."

***Adware*:** Son programas que se instalan en el equipo con o sin intervención del usuario, su objetivo principal es descargar publicidad a la computadora infectada.

***Dialers*:** Programas que utilizan el modem[14] para realizar llamadas a servicios telefónicos con alto costo.

Punto seguridad, defensa digital
Número 1, mayo 2009.I

4.4 TIPOS DE ATAQUES

Una vez descriptas algunas de las herramientas utilizadas por los delincuentes, es necesario estudiar las diversas metodologías y tipos de ataques posibles que buscan robar información confidencial del usuario para utilizarla fraudulentamente para adquirir productos o servicios:

Ataques de phishing basados en suplantación: En estos casos, la metodología consiste en suplantar la dirección verdadera de un sitio Web por una dirección falsa. Entre las técnicas que se utilizan para llevar a cabo ataques de phishing por suplantación, los más utilizados son los siguientes:

Nombres de dominios erróneos: Consiste en registrar dominios similares a los utilizados por las entidades bancarias. Fue una de las primeras formas explotadas y si bien los sitios pueden ser fácilmente rastreados e inhabilitados, sigue siendo utilizado en la actualidad. Ejemplo:

www.bancoenlinea.com _ www.bancoenlineas.com.

[14] M**ódem:** es un dispositivo que sirve para modular y una señal llamada portadora mediante otra señal de entrada llamada moduladora.

Es decir, para la primera dirección verdadera, www.bancoenlinea.com, el phisher[15] registra una dirección similar www.bancoenlineas.com. El truco radica en registrar un nombre similar al original, por lo general agregando o cambiando alguna de los caracteres del dominio original. Con esto, se logra que el usuario ingrese al sitio falso cuando comete el error de tipear la URL o cuando ingresa desde un enlace sin notar la diferencia en el nombre del dominio.

En esta metodología, conocida como typosquatting1, el atacante puede "jugar" con los caracteres y registrar una dirección Web que a simple vista parece la original, como por ejemplo:

www.banc0enlinea.com

Donde la letra "o" se ha remplazado por el número "0".

Ofuscación[16] de URL: Se crea un sitio Web falso ocultando, o evitando la fácil lectura, de la dirección o URL a la que el usuario ingresa. Esta técnica es denominada ofuscación2 de URL.

En este caso, el phisher busca dificultar la lectura de la URL[17] a través de diferentes trucos que básicamente consisten en ocultar la dirección Web codificando la dirección IP[18] de distintas maneras. Como resultado, lo que el usuario visualiza en la barra de navegación podría ser algo similar a lo siguiente:

- Visualización de la dirección en sistema decimal:
http://201.60.31.236/
- Visualización de la dirección en sistema hexadecimal:

[15] **Pisher**: Persona que comete estafas al adquirir información confidencial en la red de forma fraudulenta (como puede ser una contraseña o información de tarjetas de crédito etc).

[16] **Ofuscación**: Técnica que consiste en dificultar la lectura del texto

[17] **URL**: Significa Uniform Rezurce Locator, es decir, localizador uniforme de recurso.

[18] **IP**: Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

http://0xc9.0x3c.0x1f.0xec/

- Visualización de la dirección en sistema octal:

http://0311.0074.0037.354/

Clonación de páginas Web: Consiste en hostear o alojar una página Web falsa, muy similar a la original de la entidad atacada, en un servidor controlado por el atacante. Actualmente, esta técnica es la más común y la más explotada para realizar ataques de phishing.

A continuación, se presenta una página Web de una entidad bancaria, que ha sido copiada, pero presenta algunas alteraciones con respecto a la original.

En la pagina falsa no contiene el logo de la autoridad certificadora Verisign e imágenes que le banco presenta, además de logo de advertencia contra fraudes.

Fig. 18. Ejemplo de clonación de páginas Web.

Al contrario de lo que se puede suponer, cualquier persona puede realizar un ataque de phishing sin poseer conocimientos avanzados del tema, debido a que existen aplicaciones que permiten “automatizar” el desarrollo de estos ataques. Estos kits son comercializados a través de sitios Web y foros, con lo que el atacante sólo necesita un servidor Web para concretar los ataques y obtener la información bancaria y financiera de los clientes de una determinada institución en cuestión de horas.

Utilización de troyanos bancarios. A diferencia de los keyloggers convencionales, los troyanos bancarios están diseñados para detectar patrones de cadenas como por ejemplo “password” o “contraseña” cada vez que el usuario ingresa a la zona de registro de la entidad atacada. En ese momento, se activa la captura de información específica, obteniendo los datos de registro del usuario. Ante esta problemática, las entidades comenzaron a implementar contramedidas como los teclados virtuales con el ánimo de minimizar el impacto causado por las acciones de estos ataques.

Esta medida de seguridad permite ingresar la información solicitada mediante la utilización del mouse y a través de un teclado que se despliega en pantalla, posibilitando que el usuario ingrese sus datos sin presionar ninguna tecla en el teclado físico.

Fig. 19 Teclados virtuales

Posteriormente, los atacantes comenzaron a implementar, en estos troyanos, un módulo que permite no sólo el registro de lo que se escribe con el teclado, sino que también permite realizar capturas de pantalla (imágenes) cada vez que el usuario accede al sitio Web y realiza un clic sobre el teclado virtual. De esta manera, los creadores de códigos maliciosos lograron saltar las restricciones provistas por esta contramedida. Del mismo modo, muchos de estos troyanos bancarios basados en componentes keylogger, también poseen la capacidad de grabar videos. Estos videos capturan parte de la pantalla del usuario tomando como referencia el cursor del mouse, precisamente en la zona donde se ubica el teclado virtual, permitiendo que el atacante logre obtener, de igual forma, la información que busca.

Redireccionamiento Web Otra de las técnicas utilizadas por los troyanos bancarios es la denominada DNS[19] Poisoning (envenenamiento de DNS), consistente en modificar los DNS3 para redireccionar el dominio real hacia una dirección IP falsa creada por el atacante.
De esta manera, cada vez que el usuario ingrese a una determinada dirección, como por ejemplo www.bancoenlinea.com o a una dirección IP como 201.60.31.236, será redireccionado hacia la página Web previamente creada por el atacante con el fin de engañar a la víctima.

La técnica más utilizada por los troyanos bancarios es la denominada
Pharming Local. En este caso, cuando el troyano bancario compromete un equipo, lo que modifica es un archivo llamado “hosts”[20] que puede ser encontrado en cualquier sistema operativo.
Este es un archivo de texto que funciona a modo de caché interno permitiendo resolver, de manera local, nombres de dominio contra direcciones IP, de manera tal que la relación entre los nombres de los sitios Web configurados en tal

[19] **DNS**: Consiste en un sistema que permite la traducción de los nombres de dominio por direcciones IP y viceversa.

[20] **Un host o anfitrión:** Es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio Web.

archivo, identifican de manera unívoca las direcciones IP, establecidas en el archivo en cuestión.

Superposición de imágenes. La técnica se basa en la superposición de una imagen en la zona de acceso del sitio Web. Se utiliza otra variante de troyano bancario para controlar el momento en que el usuario ingresa al sitio Web de la entidad elegida. Cuando esto sucede, el troyano muestra una imagen que se superpone a la del sitio Web, en la zona de acceso del login de usuario.
Es decir que el usuario ingresa a la página real de la entidad bancaria, sin percatarse de que en la zona de acceso se superpuso una imagen falsa. Cuando el usuario hace clic sobre la imagen desplegada por el código malicioso, y no sobre la verdadera zona de acceso, ingresa al sitio Web falso donde sus datos serán grabados por el troyano y enviados al atacante.

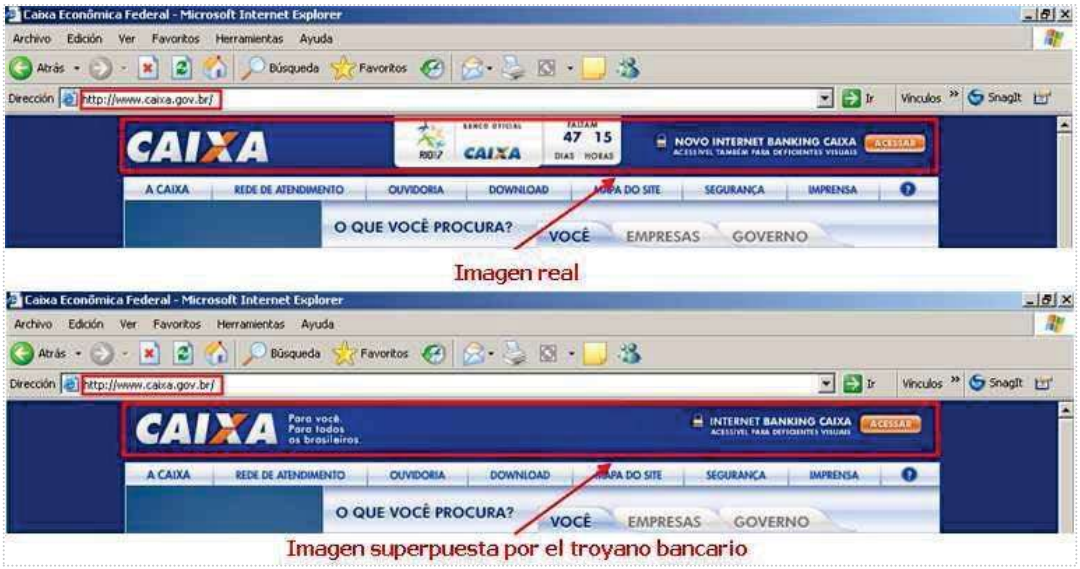


Fig. 20 Superposición de imágenes

Una problemática mundial **l**amentablemente, los ataques descriptos son cada vez mayores y se encuentran en crecimiento a nivel mundial. Según el APWG, sólo durante enero del 2008 se reportaron alrededor de 30.000 casos de ataques de phishing, siendo Estados Unidos el país con mayor tasa de

hospedaje de sitios Web falsos con casi el 37,25%, seguido por Rusia, China y Alemania con el 11,66%, 10,3% y 5,64% respectivamente.

En Latinoamérica, esta problemática también alcanzó tasas de propagación realmente preocupantes registrándose una gran actividad de ataques en muchos países de la zona. Por su lado, Brasil se encuentra entre los países de América Latina que realizan mayor cantidad de ataques de phishing.

Robo de Información personal online
Jorge Mieres, Cristian Borghello
Martes 26 de junio del 2008

Robo de información: Entre la información que puede buscar un intruso a través de un código maliciosos encontramos: información relacionada con juegos, datos personales (teléfonos, direcciones, nombres, etcétera), información de inicio de sesión (usuarios y contraseñas) y también información relacionada con la actividad que realizamos en nuestra computadora, incluyendo hábitos de navegación y programas comúnmente utilizados.

Envío de correo no deseado (*spam*): Algunos programas maliciosos se encargan de utilizar nuestra computadora y conexión a Internet para enviar correos publicitarios o con contenido malicioso a múltiples usuarios en Internet.
Control remoto: Esta acción permite a un usuario malicioso tomar control de nuestro equipo, esto le permitiría utilizar nuestros recursos para almacenar más *malware* o para instalar programas o eliminar datos; aunque también podría utilizarse el equipo para llevar a cabo ataques a otros equipos de Internet.

Ataques de ingeniería social: Existe una nueva tendencia de fabricar *malware* que tiene por objetivo intimidar, espantar o molestar a los usuarios para que compren ciertos productos (Roberts, 2008). Por ejemplo, existe código malicioso que se hace pasar por un antivirus y alerta a los usuarios de que el equipo está supuestamente infectado y que la única manera de eliminar la infección es adquiriendo un *software* promocionado por el *malware* (Garnham, 2009).

Punto seguridad, defensa digital
Número 1 | mayo 2009.

4.5 CIBERCRIMINALES

Bot-herders: Se trata de criminales que infectan miles de computadoras con programas maliciosos que les permiten tomar el control de éstas y robar información o utilizarlas para realizar sus crímenes.

Carders: Se especializan en el robo de información personal de usuarios de tarjetas de crédito para realizar fraudes bancarios.

Cybergangs: Son grupos de hackers que utilizan las computadoras para realizar crímenes on-line. Estos grupos están establecidos en países donde las leyes en cuanto a los delitos cibernéticos son ligeras o nulas.

Cybermules: Son los miembros de los cybergangs.

Cyberpunk: Son delincuentes que utilizan sus computadoras para irrumpir en redes. El dinero no es su principal objetivo.

Hackers y Crackers: Operan de manera individual y su principal objetivo es tener buena reputación entre su comunidad.

Phishers, pharmers, y spammers: Son delincuentes especializados en el robo de información para después venderla a redes criminales.

Script kiddy: Se trata de una especie de hacker que no tiene a su disposición mayor tecnología, usualmente son adolescentes, aunque podrían hacer serios daños en algunas computadoras con comandos que obtienen on-line.

Punto seguridad, defensa digital
Número 1 | mayo 2009.

4.6 ACCIONES ILICITAS EN LA RED EN LOS ULTIMOS AÑOS

Extorsión: Este tipo de ataque afectó tanto a empresas como a usuarios individuales. Los criminales roban la información personal, sobre todo la financiera y entonces pedían dinero a cambio de no utilizarla para cometer robos.

Fraude (phishing, pharming, spoofing, hijacking): Este tipo de ataques se daban a través de correos electrónicos disfrazados de alguna institución bancaria o de algún sitio de entretenimiento que pedía los datos de los usuarios y así robar información sensible.

Lavado de dinero: Este tipo de actividad se dio de manera importante durante este año, es sencillo hacerlo a través de Internet. Los criminales utilizaban la banca por Internet, los casinos on-line, y servicios financieros en línea para realizar transacciones.

Spamming: En este tipo de ataques, los delincuentes utilizan los botnets para enviar miles de correos spam y robar información sensible.

Robo de información: Los cibercriminales roban información financiera, ya sea de usuarios individuales o empresas. Además roban información de proyectos de empresas para venderlos después

A pesar de que a nivel internacional se reforzaron leyes en contra del cibercrimen, señala el informe, la delincuencia cibernética sigue creciendo y los esfuerzos no resultan suficientes, pues los criminales van un paso adelante.

“El Internet aumenta en valor todos los días, pero su seguridad no puede mantener el ritmo” asevera el reporte de McAfee. Y prevén que para los próximos meses continuarán atacando de esta manera y que combinarán muchas de sus herramientas para seguir pasando desapercibidos mientras se llenan las manos de dinero.

Héctor A. González Campos
Miércoles 21/11/2007 num. 0
Security

El delegado de la dependencia en la región, En tamaulipas Juan José Espino, dijo que sólo en esta ciudad se han interpuestas 700 inconformidades, la mayoría porque a usuarios de tarjetas de crédito les han sustraído cantidades entre los tres mil pesos y 700 mil pesos.

Destacó que los robos cibernéticos son graves, "pues en Internet con un click los delincuentes pueden sustraer cantidades millonarias a empresas que mueven de dos a tres millones de dólares".

Alertó a los usuarios de Internet para que tenga más cuidado con las ventas que ofertan por la Red, y agregó que "deben verificar que las compañías estén establecidas y no dejarse llevar por las promociones fáciles, ya que después no llega el producto".

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef)
México, 04 Junio 2009

De acuerdo con el último “Informe sobre amenazas a la seguridad en Internet” realizado por Symantec, se descubrió que México es el segundo país con más actividad maliciosa en América Latina: “Notamos que los países con economías emergentes, como es el caso de México y Brasil, están siendo aprovechados por los generadores de *malware*, quienes ven que en éstos no hay una conciencia adecuada sobre la seguridad y, de paso, buscan explotar la creciente adopción de tecnologías como la banda ancha”, comentó Rafael García, gerente regional de Mercadotecnia de Producto en Symantec.

Según dicho estudio, México registró un 17% en cuanto a actividad maliciosa a nivel de América Latina, sólo detrás de Brasil, país que representó un 34 por ciento. García expuso además que el 58% de los ataques de *malware* hacia la región proviene de Estados Unidos: “Pero también observamos un incremento en la participación de países de la misma zona en la generación de código malicioso, como es el caso de Chile y Colombia, quienes por primera vez resaltaron en el estudio”.

Lo anterior se debe, dijo, a que los atacantes buscan ahora enfocarse en los países donde pueden compartir estructuras similares (por ejemplo el idioma) para hacer más efectivos sus ataques.

En el estudio realizado por la firma de seguridad también se descubrió que México es el sexto generador de *spam* en la región, aparte de que este tipo de ataques tuvo un incremento del 192%, pasando de 119.6 billones de mensajes en 2007 a 349.6 billones en 2008.

"Los atacantes cada vez más buscan vulnerar sitios Web con mucho tránsito, aprovechando alguna vulnerabilidad para poder comprometer un servidor, el cual no precisamente será quien provea el *malware* sino que simplemente lo redireccionará a otro donde el atacante tiene el control total del mismo", explicó el ejecutivo.

Añadió que datos de las tarjetas de crédito, así como de cuentas de banco, continúan siendo el tipo de información más robada a través de estos ataques, y respectivamente les corresponde el 32% y 19% de los objetos más comprados en la economía clandestina.

Éstos son algunos precios de la información que suele ser robada y posteriormente vendida

- Información de tarjeta de crédito: desde 0.06 hasta 30 dólares.
- Credenciales de cuentas bancarias: desde 10 hasta 1,000 dólares.
- Cuentas de correo electrónico: desde 0.10 hasta 100 dólares.
- Direcciones de correo electrónico: desde 0.33 hasta 100 dólares.
- Identidad completa: desde 0.70 hasta 60 dólares.

Expertos de seguridad informática señalan a México como probable futura sede de criminales cibernéticos en el mediano plazo. Investigadores de los laboratorios de seguridad de F-Secure aseguran que en los próximos cinco años habrá un importante incremento en la actividad del crimen cibernético y que México podría convertirse en uno de los focos rojos de actividades informáticas ilegales.

De acuerdo con un reporte de la empresa, en México se conjuntan un marco legal insuficiente, una buena penetración de tecnología y un nivel alto de personas capacitadas en tecnologías de información que no pueden conseguir empleos adecuados a causa del ambiente económico.

Otras zonas donde se prevé un incremento importante son África, China, India y América Central, de acuerdo con los expertos. Los delincuentes informáticos existen en todos los países, pero la mayoría operan por ahora desde Rusia, China y América del Sur. Este panorama, de acuerdo con la empresa, cambiaría a partir de 2008 y en los próximos años, debido a las lagunas legales en materia de tecnología que imperan en México y varios países de África y Centroamérica.

"El papel de México, por ser uno de los países más desarrollados de América Latina, con una buena tasa de penetración de internet en la población y buen nivel de educación TI, igualmente tomaría su posición en el dibujo final".

Monday, February 11, 2008
Posted in Seguridad informática

Los fraudes electrónicos se incrementan 30 por ciento al año, cada vez que se realizan operaciones bancarias existen más de 240 mil delincuentes con estudios de licenciatura, maestría o doctorado en espera de utilizar la tecnología para robar datos e información.

El investigador y analista de Fraudes Cibernéticos, Oscar Manuel Lira indicó que cada vez que ingresamos a Internet existen mil millones de personas conectadas a la red, por lo que es riesgoso realizar operaciones financieras por este sistema.

A pesar de que existen sistemas que bloquean el ingreso de otros cibernautas a nuestras computadoras, son muy difíciles de detectar. “Los principales responsables de que continúen los robos de información son las empresas en fabrican antivirus, aunque los tengas actualizados tardan más de seis meses para que detecten un virus”.
“Quienes comenten fraudes cibernéticos no son personas ignorantes, no son personas comunes y corrientes, son profesionales, son personas estudiadas que tardan de seis meses a un año para realizar sus fechorías”.

En México existen leyes que castigan este tipo de fraudes pero por desgracia lo que falta es controlar los servicios por Internet, que es justamente donde se cometen estos ilícitos que tanto dañan a las empresas e industrias.
Según las estadísticas anualmente los bancos enfrentaron 3 mil 464 reclamaciones por fraudes bancarios por un monto acumulado de 478 millones de pesos. Cifras que han colocado a México como uno de los mercados objetivos de los ciberdelincuentes, al concentrar el 0.5 por ciento de los fraudes electrónicos que se generan en el mundo.

26 Septiembre 2008
Sandra Hernández Hernández

4.7 MEDIDAS PARA PREVENIR EL ROBO DE INFORMACIÓN

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización
Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
Confidencialidad: La información sólo debe ser legible para los autorizados.
Disponibilidad: Debe estar disponible cuando se necesita.
Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, que el usuario no puede negar dicha acción.

Además de enfatizar que las entidades financieras y bancarias jamás solicitan claves, cambios de ellas o información personal de los clientes a través del correo electrónico, es sumamente importante que los usuarios incorporen hábitos de navegación que permitan minimizar el impacto que provoca ser víctima de los ataques descriptos.

A continuación, se presenta una serie de consejos que ayudan a contrarrestar estas acciones maliciosas:

Mantener el sistema operativo, el navegador y el antivirus con las últimas actualizaciones de seguridad disponibles. Esto ayuda a mantener el sistema libre de todo tipo de códigos maliciosos, sobre todo, aquellos que aprovechan técnicas de inyección de código HTML y vulnerabilidades 0-Day (de día cero).

Instalar un antivirus con capacidades de detección proactiva. Debido a la gran variedad de malware, las técnicas de detección utilizadas por las mejores soluciones antivirus están basadas en la detección proactiva de los códigos maliciosos. De esta manera, a través de un análisis entiempo real, el antivirus puede indicar que determinado archivo es potencialmente peligroso, incluso sin que el mismo cuente aún con una firma que lo idefentifique.

Hacer caso omiso a correos electrónicos de origen desconocido o a nombre de entidades financieras o bancarias. Por lo general, los correos electrónicos con estas características suelen ser no deseados (spam) y

esconden potenciales ataques de phishing buscando propagarmalware como los descriptos. Del mismo modo, es conveniente no atender a mensajes escritos en idiomas que no son el nativo de quien los recibe.

Evitar introducir datos personales y/o financieros en sitios desconocidos. De esta manera, se minimiza la posibilidad de recibir correo electrónico no deseado, una de las principales vías por las que se diseminan los ataques de phishing y malware.

Escribir con el teclado, la dirección de la entidad en la barra de navegación. Es recomendable no acceder a sitios web por medio de enlaces incrustados en correos electrónicos, sino que es conveniente acceder a dichos sitios escribiendo directamente la dirección en la barra de navegación del navegador que se utilice.

No operar desde ambientes públicos. En lo posible, se debe evitar acceder a sitios de transacciones comerciales desde sistemas que se encuentren en lugares de acceso público como cibercafés, locutorios, aeropuertos, hoteles, etc. ya que, al ser utilizadas por cualquier persona, pueden conllevar a potenciales riesgos de robo de datos.

Verificar las medidas de seguridad del sitio Web. Otro buen hábito es verificar la existencia de un candado en el navegador utilizado, que permita visualizar el certificado digital del sitio al que se accede. Asimismo, verificar que la dirección web de la página de la institución financiera comience con “https”[21]. Esto indica que se está navegando bajo un protocolo seguro

Utilizar claves fuertes. Una de las medidas de seguridad implementada por las entidades es que la contraseña de acceso debe cumplir con determinados requisitos impuestos por la entidad en cuestión. Por ello, al momento de elegir la contraseña, es conveniente que sea fácil de recordar pero que además sea lo

[21] **HTTPS**: Protocolo seguro de transferencia de hipertexto (Hypertext Transfer Protocol Secure). Protocolo de comunicación que permite la transferencia de información de manera segura.

suficientemente robusta como para dificultar su descubrimiento por parte de usuarios malintencionados.

Bajo este escenario, las organizaciones o empresas de cualquier tipo no están exentas de ser víctimas de ataques de phishing o malware; por lo tanto, además de las pautas mencionadas, es necesario extremar las medidas de seguridad teniendo en cuenta aspectos como:

Elaboración de políticas de seguridad claras. Las mismas deben involucrar medidas que ayuden a combatir códigos maliciosos.
Ejecución de planes de seguridad. Los que deben incorporar medidas en materia de concientización de usuarios.
Implementación de soluciones antimalware. Implementar soluciones de seguridad antimalware con sistemas de detección proactiva que ayuden a prevenir la proliferación de códigos maliciosos que puedan afectar los activos de la compañía.

Robo de Información personal online
Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
26 de junio del 2008

4.8 ELEMENTOS PARA LA PROVISIÓN DE SERVICIOS DE SEGURIDAD

Servicios de seguridad: Protege las comunicaciones de los usuarios ante las posibles ataques.

Mecanismos de seguridad: Son utilizados para implementar un determinado servicio de seguridad o una combinación de ellos, se podría decir que son las piezas lógicas con los que se construyen los protocolos de seguridad los cuales son los encargados de proporcionar los servicios de seguridad.

Protocolo de seguridad: Consiste en un conjunto de reglas y formatos que determinan el intercambio de piezas de información en el que intervienen 2 o mas entidades.

Técnicas Criptográficas: En la actualidad los mecanismos de seguridad que han sido desarrollados son mecanismos criptográficos, esta permanente presencia de la criptografía y la indudable importancia que el comportamiento de los criptosistemas tienen en el resultado final.

Fig. 21 Elementos para la Provisión de Servicios de Seguridad

Seguridad en Redes Telemáticas
Justo Carracedo Gallardo
McGraw Hill
Madrid Marzo 2004

4.9 TÉCNICAS DE ASEGURAMIENTO DEL SISTEMA

- Codificar la información: Criptología,[22] **Criptografía** y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales .
- Vigilancia de red.
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones.

Técnicas para proteger la información: El cifrado y descifrado de los datos y las técnicas de firma digital son los medios mas efectivos para garantizar que los datos puedan ser comprendidos por los receptores deseados y que los transmisores de la información sean, realmente , quienes dicen ser.
Otras de las técnicas son la utilización de cuentas, contraseñas y sistemas de control de acceso, la palabra cuenta significa que para que una persona pueda obtener acceso al sistema, debe disponer de una identidad digital que haya sido configurada por la persona o departamento apropiado, y las cuentas deben disponer de contraseñas que no sean fáciles de determinar, el entorno debe poder garantizar que las contraseñas de los usuarios no se envíen a través de los medios de transmisión en una forma tal que pueda ser fácilmente captadas y descifradas por una persona no autorizada

En la criptografía, el mensaje que se quiere cifrar se denomina texto claro. Se utiliza este termino por que la información que contiene el mensaje puede ser leída fácilmente por cualquiera. El algoritmo para cifrar el texto en claro se párametrisa mediante una clave. El mensaje de texto claro que se haya sido cifrado utilizando una función de cifrado y una clave se denomina texto cifrado.

[22] **La criptología**: es el estudio de los criptosistemas: sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado (o nadie) pueda descifrarlo.

El cifrado, que implica siempre algún tipo de manipulación matemática de los datos, se le suela denominar genéricamente código de autenticación del mensaje (MAC, Message Authentication Code). Históricamente, hay dos categorías de métodos de cifrado, cifrado por sustitución y cifrado por transposición.

Cifrado de sustitución: Es simplemente un esquema en el que se utiliza un carácter o símbolo en lugar de una carecer real.

Redes de Computadoras
Austin Community College
Ed. Tittel, McGraw Hill, 2004

Cifrado de transposición: Se basa en la reordenación aplicada al texto original mediante una clave establecida. Al igual que en el primer método el descifrado se realiza mediante la clave y de nuevo la reordenación, presenta los mismos inconvenientes que el primer método.

La Criptografía moderna está basada también en los algoritmos de Sustitución y Transposición pero con distinta orientación

Libro electrónico "Seguridad Informática" cuarta edición
Versión v32 de Jorge Ramió Aguirre. Universidad Politécnica de Madrid
Seguridad: Criptografía Cristóbal Penalva Ivars 05/2006

5. CRIPTOGRAFÍA

La criptografía es la técnica, ciencia o arte de la escritura secreta. El principio básico de la criptografía es mantener la privacidad de la comunicación entre dos personas alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario; a esto debemos la autenticación, esto es, la firma del mensaje de modo que un tercero no pueda hacerse pasar por el emisor.

La palabra criptografía proviene de las palabras griegas "criptos" (oculto) y "grafos" (escritura). A la transformación del mensaje original en el mensaje cifrado (criptograma) le llamamos cifrado, y a la operación inversa, le llamamos descifrado; estos pasos se realizan mediante un conjunto de reglas preestablecidas entre los comunicantes a la que llamamos clave. El criptoanálisis es el conjunto de técnicas que intenta encontrar la clave utilizada entre dos comunicantes, desvelando así el secreto de su correspondencia.

Transparencias de clase
- Hackers 3. Stuart McClure y otros, Ed. McGraw Hill
- Libro Electrónico “Cripto-libro”, PFC desarrollado por Ana Mª Camacho Hernández de la U.P.M. 05-2000

5.1 HISTORIA DE LA CRIPTOGRAFÍA

La historia de la criptografía se remonta a miles de años. Hasta décadas recientes, ha sido la historia de la criptografía clásica — los métodos de cifrado que usan papel y lápiz, o quizás ayuda mecánica sencilla. A principios del siglo XX, la invención de máquinas mecánicas y electromecánicas complejas, como la máquina de rotores Enigma, proporcionaron métodos de cifrado más sofisticados y eficientes; y la posterior introducción de la electrónica y la computación ha permitido sistemas elaborados que siguen teniendo gran complejidad.

La evolución de la criptografía ha ido de la mano de la evolución del criptoanálisis — el arte de "romper" los códigos y los cifrados. Al principio, el descubrimiento y aplicación del análisis de frecuencias a la lectura de las

comunicaciones cifradas ha cambiado en ocasiones el curso de la historia. De esta manera, el telegrama Zimmermann provocó que Estados Unidos entrara en la Primera Guerra Mundial; y la lectura, por parte de los Aliados, de los mensajes cifrados de la Alemania nazi, puede haber acortado la Segunda Guerra Mundial hasta dos años. Hasta los años 70, la criptografía segura era dominio casi exclusivo de los gobiernos. Desde entonces, dos sucesos la han colocado de lleno en el dominio público: la creación de un estándar de cifrado público (DES); y la invención de la criptografía asimétrica.

Simon Singh, Los códigos secretos : el arte y la ciencia de la criptografía,
desde el antiguo Egipto a la era Internet,
Barcelona, Debate, 02-2000.

La escitala (siglo V a.C.) El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta, por parte de los lacedemonios. El cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo llamado escitala, de longitud y grosor prefijados. Aún sabiendo la técnica utilizada, si no se tenían las dimensiones exactas de la escitala, un posible interceptor del mensaje tenía muy difícil su criptoanálisis. El grosor y la longitud de la escitala eran la clave de este sistema:

Fig. 22 La escitala,

Cualquiera que desenrollara la tira se encontraría con:
AAC SIN ICT COA INL FLA RA AE BS

El cifrador de Polybios (siglo II a.C.)

Es el cifrador por sustitución más antiguo que se conoce. El método se basaba en una tabla secreta, en cuyos ejes se ponían diferentes combinaciones de

letras o números y dentro de la tabla las letras del alfabeto. Cada letra del mensaje a cifrar era sustituida por sus “coordenadas”. Se ve bastante más claro en el siguiente ejemplo:

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i/j	k
C	l	m	n	o	p
D	q	r	s	t	u
E	v	w	x	y	z

Fig. 23 Cifrado de polybios

Mensaje: Polybios es el rey
Criptograma: CECDCAEDABBDCDDC AEDC AECA DBAEED

Cifrado de César

En el siglo I a.C., Julio César presenta este cifrador cuyo algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro. Es un cifrador por sustitución monoalfabético, en el que las operaciones se realizan módulo n, siendo n igual al número de elementos del alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fig. 24 Cifrado de cesar

Alfabeto de cifrado del César para castellano módulo 27
Mensaje: Tu también, brutus?
Criptograma: wx wdoelhp euxwxv?

Aquí termina lo que hemos denominado historia antigua de la criptografía.
Después de el siglo primero antes de Cristo y hasta el siglo XV de nuestra era, no se conoce de ningún sistema critpgráfico de nueva invención (a esa época se la conoce como edad oscura, ya que hubo más retrocesos que avances en absolutamente todas las facetas del saber humano; y la criptografía no iba a ser una excepción).

Historia Moderna

Disco de Alberti En 1466, León Battista Alberti, músico, pintor, escritor y arquitecto, concibió el primer sistema polialfabético que se conoce, que emplea varios abecedarios, utilizando uno u otro cada tres o cuatro palabras. El emisor y el destinatario habían de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinara la correspondencia de los signos. Los diferentes abecedarios utilizados eran representados en uno de los discos, mientras que el otro se rellenaba con el abecedario normal, más los números del 1 al 4. Este disco define 24 posibles sustituciones dependiendo de la posición del disco interior.

Una vez establecida la correspondencia entre caracteres de ambos discos, se sustituye el texto en claro del disco exterior por cada una de las letras correspondientes del disco interior, cambiando al abecedario correspondiente (prefijado por los comunicantes) cada x palabras, habiendo sido x también prefijada por los comunicantes.

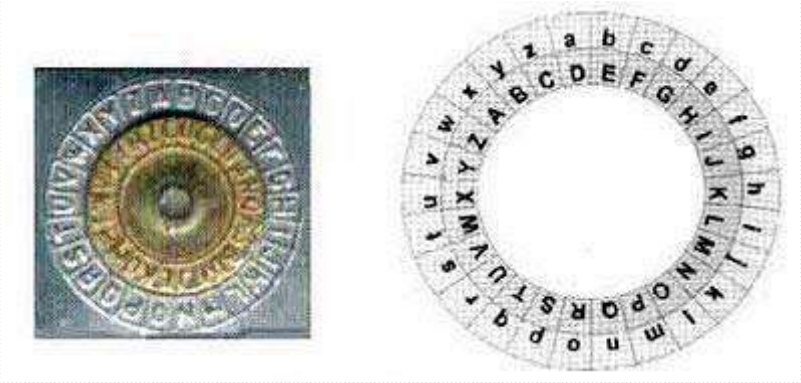


Fig. 25 Cifrado disco de Alberti

Rueda de Jefferson (1743- 1826), redactor de la declaración de independencia de Estados Unidos, aunque el primero en fabricarla en serie fue Ettiene Bazeries en 1891. El aparato consiste en una serie de discos que giran libremente alrededor de un mismo eje y llevan impresas las letras del alfabeto escritas en cada disco en diferente orden. El emisor mueve los discos hasta configurar el mensaje en claro, y elige otra línea que será el mensaje cifrado. Tras haber sido

transmitido, el receptor no tiene más que poner las letras recibidas en línea y buscar en otra línea el mensaje en claro.

Fig. 26 Cifrado rueda de Jefferson

Disco de Wheatstone El disco de Wheatstone (1802-1875) realiza una sustitución polialfabetica, muy parecida a la utilizada por Alberti. El invento consta de dos discos concéntricos: en el exterior se escriben, en orden alfabético, las 26 letras del alfabeto ingles más el espacio, y en el interior se distribuyen esas mismas 26 letras pero aleatoriamente. Sobre los discos hay dos "manecillas" como las de un reloj, de forma que a medida que avanza la mayor por el disco exterior, la menor se desplaza por el disco interior. Cuando el puntero grande recorre una vuelta, el pequeño da una vuelta más una letra. El mensaje en claro se cifraba "prohibiendo" al disco exterior ir en sentido antihorario siendo el mensaje secreto lo indicado por el puntero menor.

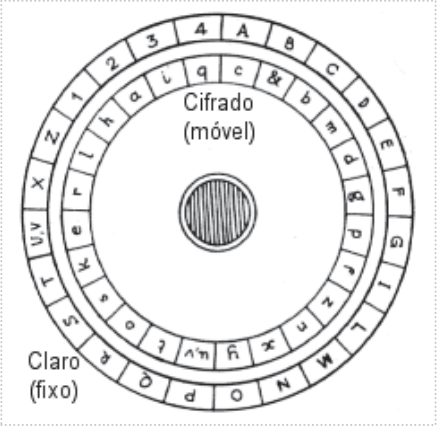


Fig. 27 Cifrado Disco de Wheatstone

Maquinas posteriores

A parte de estas máquinas relativamente sencillas, podemos encontrar algunos inventos más modernos de cuyo funcionamiento sería imposible hacer una descripción sin meternos de lleno en las leyes de la física que los rigen, por lo que hemos optado por simplemente enumerarlos. Algunos de estos inventos basan su cifrado en algunos de los sistemas que vamos a describir en los siguientes apartados. Fig. 28 Cronológicamente ordenados, los citados inventos son:

- *Maquina Enigma*: Inventada por Arthur Scherbius en 1923 y usada por los alemanes durante la II Guerra Mundial.

- *Maquinas de Hagelin:* Desarrolladas por el criptólogo sueco Boris Hagelin entre 1920 y 1930. Se basaban en el sistema de cifrado de Beaufort.

- *Maquina M-325:* Desarrollada por Frederick FriedMan en los años cuarenta del siglo XX. Es muy parecida a la maquina *enigma* alemana, ya que también se basa en rotores que realizan una sustitución polialfabética. *Enigma Hagelin M-32*

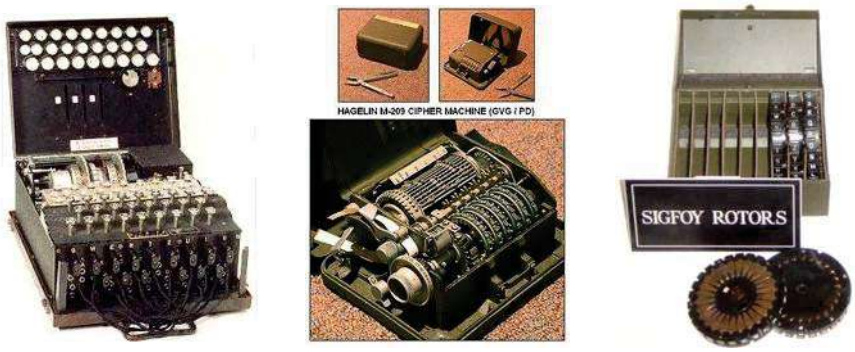


Fig. 28 Enigma , Hageli, M-325

Criptosistema de Vigènere: El sistema de cifrado de Vigenère es un sistema polialfabético o de sustitución múltiple, de clave privada o secreta. Este tipo de criptosistemas aparecieron para sustituir a los monoalfabéticos o de sustitución simple, basados en el Algoritmo de Cesar que hemos visto anteriormente, que

presentaban ciertas debilidades frente al ataque de los criptoanalistas relativas a la frecuencia de aparición de elementos del alfabeto.

Segundo Cifrado de Vigénere El segundo cifrado de Vigènere es igual que el primero, sigue utilizando la tabla anterior, salvo en la secuencia de caracteres que se utilizan como clave. En el primer cifrado esta secuencia clave era la repetición de la clave primaria. Sin embargo en este segundo algoritmo, la secuencia de caracteres utilizada como clave se obtiene del resto del mensaje original. En el ejemplo anterior, en vez de utilizar por segunda vez como clave la palabra *prueba* utilizaríamos el conjunto de caracteres *cifrad*; la tercera vez utilizaríamos *odevig*, y así hasta el final del mensaje.

Criptosistema de Beaufort Al igual que el cifrado de Vigènere, es una sustitución periódica basada en alfabetos desplazados, pero utilizando otra tabla diferente (mostrada a continuación), en la que se invierte el orden de las letras del alfabeto y luego se desplazan a la derecha.

Cifrado de Playfair (1854) El cifrado de Playfair en realidad fue inventado por Charles Wheatstone, para comunicaciones telegráficas secretas en 1854 (de hecho, es el sistema utilizado en el disco de Wheatstone); no obstante se le atribuye a su amigo el científico Lyon Playfair.
Utilizado por el Reino Unido en la Primera Guerra Mundial, este sistema, que ya no es polialfábetico sino poligrámico, consiste en separar el texto en claro en diagramas y proceder a su cifrado de acuerdo a una matriz alfabética de dimensiones 5 X 5 en la cual se encuentran representadas las 26 letras del alfabeto ingles, aunque para una mayor seguridad se puede agregar una palabra clave (añadiéndola a la matriz en lugar de las primeras letras).

Cifrado de Hill

Surge en 1929, tras la publicación de un artículo en Nueva York por parte del matemático Lester S. Hill, que propone utilizar las reglas del álgebra de matrices en las técnicas de criptografía.

El método es de sustitución monoalfabética y poligrámico, y consiste en asignar un valor numérico a cada letra del alfabeto. El mensaje en claro se dividirá en pares de letras y se colocará en una matriz 2x1, que se multiplicará por la matriz resultante de asignar un valor numérico a la clave que se quiere emplear de 2x2. El resultado de la multiplicación será un par de letras cifradas (una matriz de 2x2·2x1=2x1) Para descifrar basta con utilizar matriz inversa de la de la clave.

Transparencias de clase Hackers 3.
Stuart McClure y otros, Ed. McGraw Hill

5.2 SISTEMAS CRIPTOGRAFICOS

La criptografía ha sido usada desde muy antiguo, aunque modernamente, con el concurso de los computadores, resulta de más fácil uso y mucho más eficaz que la que se conseguía con los sistemas tradicionales.

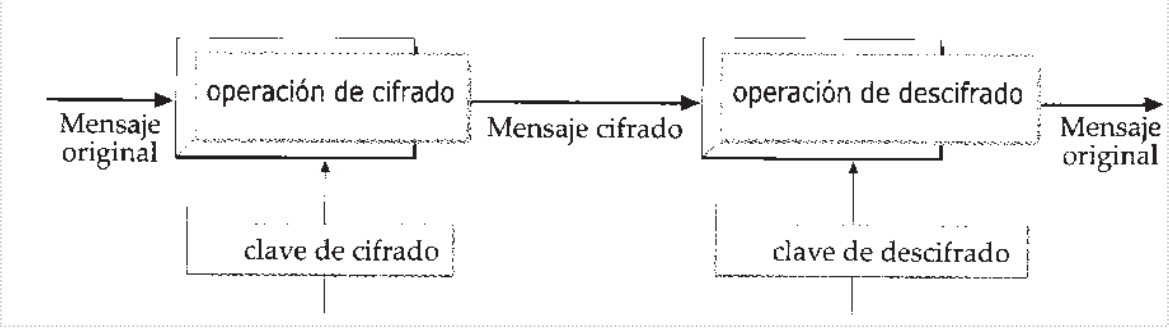


Fig. 29 Encriptación de un mensaje

En este sistema criptográfico, en el puede verse como un subsistema produce un mensaje cifrado a partir de un mensaje original, mediante la aplicación de una transformación de este que depende de un parámetro denominado clave de

cifrado. En el extremo opuesto, el mensaje original puede ser recuperado en otro subsistema mediante la aplicación de la clave de descifrado.

La gracia esta en encontrar los algoritmos23 adecuados para el proceso de cifrado y descifrado a si como el adecuado transporte y comparición de las claves por parte del usuario que emite el mensaje original y el usuario que recibe este en el extremo opuesto.

CRIPTOGRAFÍA MODERNA

Podemos considerar que la criptografía moderna asienta sus bases teóricas en el siglo XIX pero su verdadera aparición hay que situarla en la década de los 70s del pasado siglo, cuando aparecen algoritmos disponibles para usos civiles implementables mediante un programa de ordenador, la característica fundamental de esta criptografía moderna es que el algoritmo de cifrado debe de ser de conocimiento publico, y solo la clave debe permanecer secreta. La seguridad de los sistemas reside en la robustez del algoritmo y en la adecuada custodia de la clave para que solo sea conocida por las personas autorizadas para ello.

Dentro de la criptografía moderna puede distinguirse dos tipos de sistemas criptográficos:

Criptosistemas de clave secreta: En ellos la clave de cifrado y descifrado es la misma: es una clave secreta que comparte el emisor y el receptor del mensaje. Debido a esta característica son denominados también criptosistemas simétricos.

[23] **Algoritmo criptográfico:** De forma similar a cualquier otro algoritmo computacional, consiste en un conjunto de reglas que definen de forma precisa y no ambigua una secuencia de operaciones y transformaciones de los datos tal que dicha secuencia y termine en un tiempo finito, un algoritmo debe contemplar la operación de cifrado y la operación de descifrar.

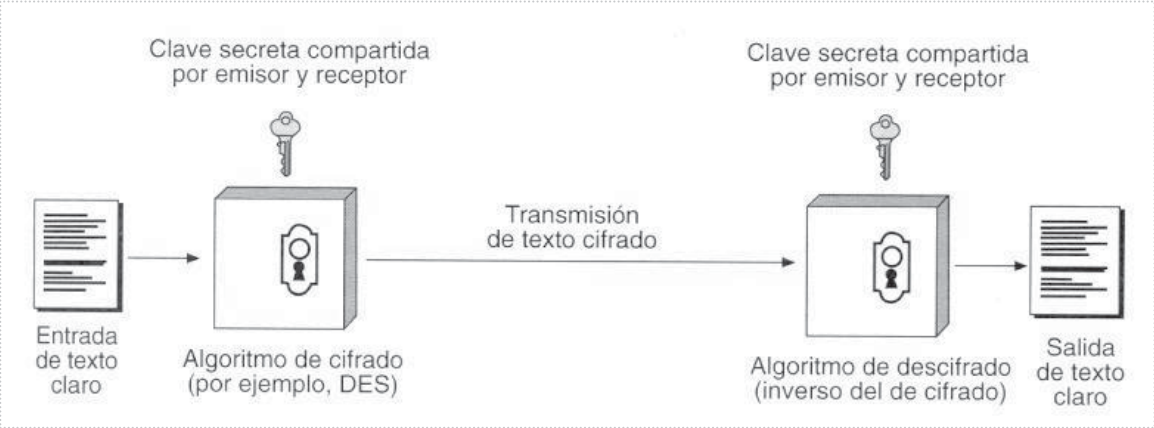


Fig. 30 Modelo de cifrado convencional (simétrico)

5.2.1 CRIPTOSITEMA SIMÉTRICO:

$$C = E_k (m)$$

Donde k es la clave secreta, E_k representa la operación de cifrado con esa clave y m es el mensaje en claro.

Simétricamente el proceso de recuperación del mensaje original, mediante la operación de descifrado, D_k, en el que se utiliza la misma clave secreta k, se representa como:

$$m = D_k (c)$$

La simetría del proceso se basa por tanto en que este tipo de cifradores se comporta tal que:

$$Dk\ [e2\ (m)] = m$$

El primer algoritmo significativo de clave secreta fue el DES, otros algoritmos importantes son el IDEA y el Rijndael.

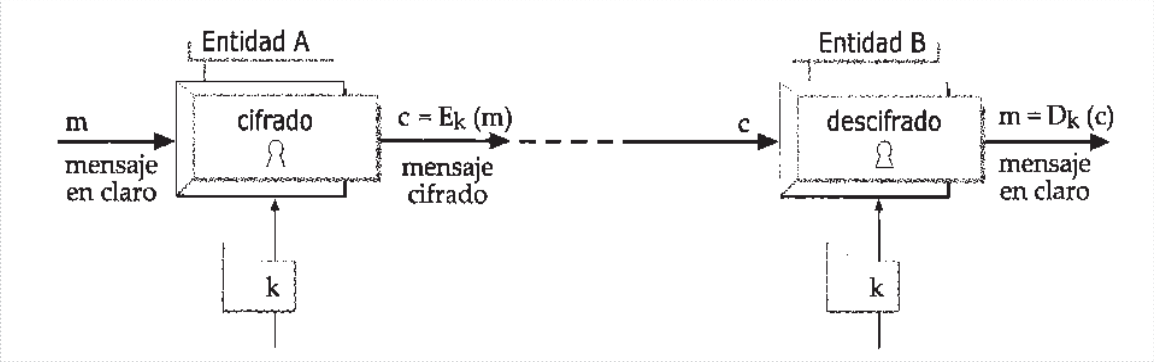


Fig. 31 Criptografía simétrica

Criptosistema DES: (Data Encryption Estándar), puede ser considerado como el primer algoritmo de la criptografía moderna usado masivamente en procedimientos civiles, tanto personales como comerciales. También conocido como DEA (Data Encription Algorithm) por ANSI y Normalizado por ISO como DEA-1, ha venido desempeñando desde 1977 un papel relevante en la implantación de la criptografía, en general. Aunque actualmente puede ser considerado como un algoritmo anticuado que ha sido vulnerado en múltiples ocasione, usado en determinadas condiciones, aun puede ser de utilidad en muchas aplicaciones.

Basado en un diseño de IBM, surgió como resultado de una propuesta de los organismos de normalización que buscaban un algoritmo con alto nivel de seguridad, que estuviese completamente especificado, susceptible de validado, cuya seguridad residiese solo en la clave, fácil de entender, disponible para todos los usuarios, económicamente accesible y fácil de implementar, IBM acorto el tamaño de la clave, que paso de los 112 bits que tenia en el diseño original a solo 64 y modificando asi su estructura de la parte mas sencible del algoritmo, las denominadas Cajas S. Esto genero controversia ante el temor de que el acortamiento de la clave facilitase la ruptura por parte de una organización con muchos recursos como en el caso de a NSA.

Algoritmo IDEA. Es un cifrador europeo que fue representado por sus autores, X.Lai y J.Massey en 1990 bajo el nombre de PEES (Proponed European Encryption Estándar) y que tras algunas mejoras, en 1992 paso a denominarse con el nombre de IDEA (International Data Encryption Estándar). Es un algoritmo muy robusto que se hizo popular por haber sido adoptado por PGP, una aplicación de correo electrónico seguro de uso muy extensivo.

Se trata de un cifrador simétrico en el que tanto el mensaje claro el criptograma se encuentran divididos en bloques de 64 bits, como en el DES, pero utilizando una clave de 128 bits, lo que representa un incremento notable del espacio de claves, que pasa de ser de 2^{128} =3,4 . $10^{38.}$ esta es ya una cifra muy elevada lo que conlleva un aumento considerado de su seguridad sise le compara con DES dificultando mucho un ataque exitoso por fuerza bruta.

RIJNDAEL (El herededo del DES): Después de una primera ronda se seleccionaron quince de los algoritmos presentados a la convocatoria AES, En una segunda conferencia en 1999 se seleccionaron cinco de ellos en base a las numerosas pruebas realizadas por criptoanalistas y especialistas de todo el mundo. Estos algoritmos seleccionados fueron:

- MARS de IBM
- RC6 de RSA Laboratory
- SERPENT de R. Anderson, E.Biham y L. Knudsen
- TWOFISH, de B. Schneider y otros.
- RIJNDAEL, de los belgas flamencos Joan Daemen y Vicent Rijmen

Es menester alabar aquí el procedimiento llevado a cabo para la evaluación de los algoritmos candidatos: ha estado presidido por una apertura hacia toda la comunidad científica.

Al fin, en octubre del 2000, el NIST anuncio la elección del RIJNDAEL como el algoritmo propuesto para AES, con lo cual se convertirá en el nuevo estándar de Estados Unidos para las próximas décadas. Dada la apertura existente en su definición y especificación, es de esperar que sea adoptado también por otros países y otras organizaciones.

El algoritmo ofrece mayores posibilidades que las exigidas en la convocatoria final, ya que tanto la clave como el tamaño del bloque se pueden elegir entre 128, 192 y 256 bits, aunque las opciones de mayor tamaño de bloque no estarán incluidas en el estándar debido a que el estudio criptoanalitico realizado durante el proceso de selección se baso en bloques de 128 bits.

Los criterios bajo los que se desarrollo el algoritmo [DaRi99] fueron los siguientes:

- Resistencia ante todos los ataques conocidos.
- Velocidad y código compacto en su implementación sobre una amplia gama de plataformas
- Simplicidad de diseño.
-

Algoritmo	Tamaño de clave (bits)	Tamaño de bloque (bits)	Número de etapas	Aplicaciones
DES	56	64	16	SET, Kerberos
Triple DES	112 o 168	64	48	Financial Key management, PGP, S/MIME
AES	128, 192 o 256	128	10, 12 o 14	Destinados a sustituir DES y 3DES
IDEA	128	64	8	PGP
Blowfish	Variable hasta 448	64	16	Varios paquetes de software
RC5	Variable hasta 2048	64	Variable hasta 255	Varios paquetes de software

Fig. 32 Algoritmos de cifrado convencional

5.2.2 CRIPTOSISTEMA DE CLAVE PÚBLICA (ASIMESTRICO)

Criptosistemas de llave publica: se distinguen por que cada usuario o sistema final dispone de dos claves: una privada, que debe mantener secreta y una publica, que debe ser conocida por todos las restantes entidades que va a comunicar con ella, se le conoce como criptosistemas asimétricos.

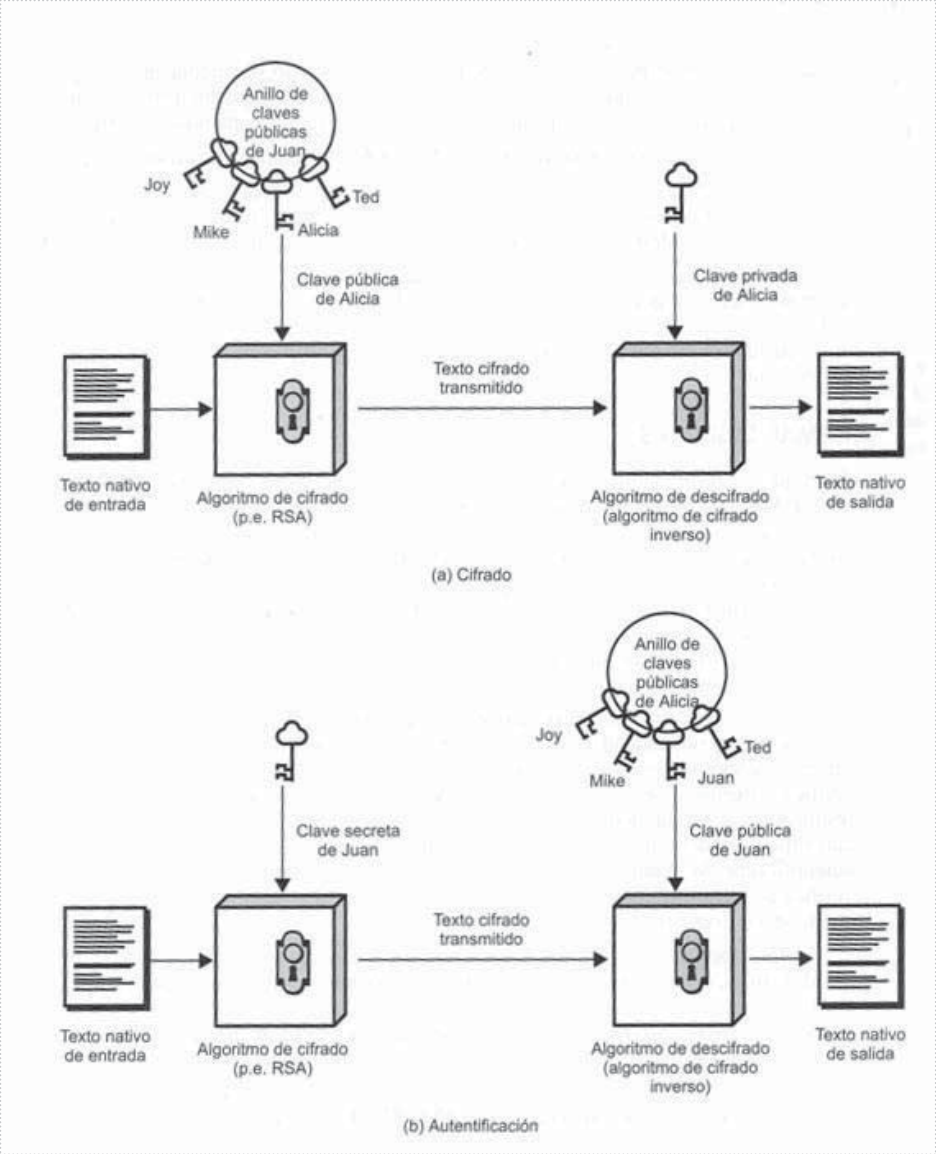


Fig. 33 Cifrado de llave publica

Una forma de cifrar la información consiste en utilizar una clave secreta que solo sea conocida por el trasmisor y el receptor. El nivel de secreto que es posible alcanzar con una clave se basa en la longitud de esta. Si una clave solo puede utilizar números decimales, entonces las claves de dos dígitos tendrán 100 posible combinaciones, si aumentaos la longitud hasta 3 dígitos, el numero de combinaciones será de 100 mientras que para seis dígitos en numero total de combinaciones es de 1, 000,000. Cuando el emisor este listo para trasmitir un mensaje hacia el receptor, cifra los datos la clave secreta y envía los paquetes a través del medio de trasmisión. El receptor descarga los mensajes del emisor mediante la clave secreta, con lo que será capaz de leer el contenido.

El cifrado del mensaje en el lado receptor implica otro proceso matemáticos para decodificar la información. La idea en que se basa esta estrategia consiste en hacer que los datos no puedan ser leídos por personas no autorizadas que pudieran interceptar los paquetes durante su viaje a través del medio, solo aquellos que posean las claves secretas correspondientes podrán descifrar los mensajes por su puesto que un emisor puede comunicarse con múltiples usuarios receptores, cada sistema puede albergar varias claves secretas.

En la criptografía de clave pública hay dos parejas de claves implicadas: *la clave pública y la clave privada*. El esquema de cifrado/descifrado no esta diseñado de tal manera que se puede deducir una de las dos claves a partir de la otra. En otras palabras, si una persona tiene una de las claves de la pareja, no puede deducir cual es la otra clave para tratar de romper el código. Tanto el emisor como el receptor almacenan dos claves cada uno, una de las cueles es conocida por ambos, mientras que la otra no lo es. La clave común es la clave pública y esta disponible para cualquiera que se desea comunicar con el emisor.

La clave privada exclusiva de cada sistema y solo la conoce el sistema especifico. Cuando un dispositivo envía un mensaje al receptor, el emisor cifra el mensaje con la clave pública y envía el mensaje cifrado al receptor. Para

descifrar el mensaje, el receptor debe usar su clave privada. El receptor no puede descifrar el mensaje con la clave pública. Cuando el receptor quiere devolver otro mensaje al emisor, cifrara dicho mensaje con la clave publica del emisor y lo enviara. Entonces, el emisor utilizara su propia clave privada para descifrar el mensaje del emisor no puede utilizar su clave publica para tratar de descifrar el texto.

Este tipo de cifrado/descifrado de doble clave hace que sea muy difícil, para alguien no autorizado, descifrar el mensaje. Los conjuntos de claves publica-privada utilizados por el emisor y el receptor son específicos y ni pueden utilizarse en otro mensaje de un sistema diferente.

Ejemplo: Si el sistema A se esta comunicando con el servidor B, Las claves publicas utilizadas por ambos sistemas están diseñadas para funcionar solo con las claves secretas asignadas a A y a B. Supongamos que la clave publica del sistema A es PubA y la clave privada del sistema A, guardada en secreto, es PrivA; suponga también que la clave publica del servidor Web es PubB y que la clave secreta correspondiente es PrivB. Cuando el sistema A este listo para enviar un mensaje al servidor B, lo cifrara con la clave PubB. Cuando el servidor Web reciba este mensaje, utilizara la clave PrivB, para descifrarlo. Una vez que este listo para enviar la respuesta al sistema A, el servidor Web cifrara el mensaje con la clave PubA y enviara la información ha dicho sistema.

El sistema A empleara la clave PrivA para descifrar el mensaje. Si otro sistema recibiera el mensaje enviado por sistema A, no podría descifrarlo, al no disponer de la clave privA. Utilizar dos claves, siendo una privada y la otra publica, es perfectamente seguro, por que las funciones del cifrado y de descifrado tienen una propiedad unidireccional. Puede utilizarse una de las claves para cifrar o descifrar el mensaje, pero lo que no se puede es utilizarse la misma clave para realizar ambas funciones con el mismo mensaje.

Un elemento enormemente crítico en la criptografía de clave publica es el modo en que se distribuyen las claves a los sistemas apropiados. Si yo enviara al lector su clave pública y su clave privada, alguien podría capturar los paquetes de información y extraer ambas claves. Además si yo estuviera enviando su clave privada, alguien podría capturar los paquetes de información y extraer ambas claves. Además, si yo le estuviera enviando la clave privada, también existiría la posibilidad de que retuviera una copia de la misma. Si mi sistema resultara comprometido, dicha clave privada ya no seria privada.
Para facilitar el intercambio de claves adecuado y poder generar las claves, se utilizan los servicios de una autoridad de certificación (AC). En algunos textos, la AC se denomina centro de distribución de claves (KDC; Key Distribution Center) de confianza.

La autoridad de certificación es una entidad interna o externa responsable de verificar quienes son el emisor y el receptor, de generar los conjuntos de claves publicas y privadas para las dos entidades, de subministrar las claves publicas a ambos interlocutores y de entregar las claves privadas a sus propietarios respectivos. Un ejemplo de autoridad de certificación externa es Verisign[24].

Muchos sistemas operativos de servidor o de red tienen la posibilidad de proporcionar autoridades de certificación internamente y algunos de ellos funcionan también con autoridades de certificación externa. Además de crear las claves, es necesario intercambiar las claves publicas entre las dos entidades y cada dispositivo debe tener la garantía de que la otra entidad es quien dice ser. Para permitir que las dos entidades que no se conocen intercambien las claves con seguridad, se utiliza el protocolo de intercambio de claves DIFFIE-Hellman[25].

[24] **Verisign:** Es una empresa de seguridad informática famosa por ser una autoridad de certificación reconocida mundialmente. Emite certificados digitales RSA para su uso en las transmisiones seguras por SSL.

[25] **Protocolo Diffie-Hellman**: Permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada).

Para distribuir claves publicas a personas individuales, se utiliza normalmente certificados digitales, los cuales suelen estar disponibles en las exploradores Web y en los sistemas de correo electrónico seguro. En estos casos, alguna autoridad de certificación emite un certificado que básicamente afirma que la clave publica contenida en el certificado pertenece, ciertamente a la persona o a la empresa indicados en le certificado.

Existen elementos de información obligatorios y otros opcionales, debiendo todos los certificados incluir la siguiente información:

- Nombre de la organización, empresa o entidad para quien se ha emitido la clave publica
- La clave publica de dicha organización, empresa o entidad indica en el certificado.
- El nombre de la Autoridad de certificación que ha emitido la clave publica
- Una firma digital

Redes de Computadoras
Austin Community College
Ed. Tittel, McGraw Hill, 2004

Podemos clasificar el uso de criptosistemas de clave pública en tres categorías: Cifrado/ descifrado: el emisor cifra un mensaje con la clave pública del receptor. Firma digital: el emisor firma un mensaje con su clave privada. Esto se consigue mediante un algoritmo criptográfico aplicado al mensaje o a un pequeño bloque de datos que es una función del mensaje Intercambio de llaves: dos partes cooperan para intercambiar una clave de sesión.

Hay distintas posibilidades que implican la clave privada de una o de las dos partes. Algunos algoritmos son adecuados para las tres aplicaciones, mientras otros sólo se pueden usar para una o dos de ellas. La tabla 2 indica las aplicaciones que soportan los algoritmos, la tabla también inclute el Estándar de Firma Digital (DSS) y la criptografía de curva eliptica.

Algoritmo	Cifrado/descifrado	Firma digital	Intercambio de clave
RSA	Si	Si	Si
Diffie-Hellman	No	No	Si
DSS	No	Si	No
Curva eliptica	Si	Si	Si

Fig. 34 Aplicaciones que soportan los algoritmos

Seguridad en redes
William Stallings (Prentice Hall)

Criptosistema RSA: La primera propuesta conocida acerca de los criptosistemas de llave publica es la de Diffie y Hellman en 1976. La primera propuesta que soporte dicho modelo fue realizada por Rivest, Shamir y Adlem RSA78, tres jóvenes profesores del MIt y se conoce bajo el nombre de Criptosistema RSA conforme a las iniciales de su nombre, desde su aparicion ha sido el sistema que se ha aceptado en todos los hambitos donde se opera con criptografía de clave publica y de forma especial, en los trabajos conducentes al diseño de los mecanismos de seguridad.

Su seguridad se basa en la dificultad de factorizar grandes números y en el hecho de que el calculo de logaritmos en aritmetica modular es un problema NP-Completo inabordable computacionalmente para bases de valor alevado. El mensaje a cifrar se divide en bloques de tal manera que tanto el mensaje a cifrar como el mensaje cifrados son números enteros comprendidos entre cero y n-1.

Seguridad en Redes Telemáticas
Justo Carracedo Gallardo
McGraw Hill, Madrid Marzo 2004

Un criptosistema de clave publica, un determinado usuario o sistema final A guarda su clave privada KS_A que solamente es conocida por el. Sin embargo, la clave pública KP_A puede ser perfectamente conocida por todos los demás usuarios pertenecientes a un determinado entorno de seguridad. El algoritmo se comporta de manera que si el mensaje se cifra usando una de las claves, se puede descifrar utilizando la otra.

Si A desea mandar un mensaje encriptada a B, de tal manera que pueda ser leido por B y solo por B, lo cifrara con la clave publica de B, KPb, obteniendo el criptograma c:

$$C= E_{KPB} (m)$$

En el extremo receptor, B, unico poseedor de KSB, Podra recuperar el mensaje original descifrando c con su clave privada:

$$M=D_{KSB} (c)$$

En la operación antes descrita se proporciona el servicio de confidencialidad, algunos algoritmos de clave publica el RSA tiene propiedades de las dos claves publica y privada.

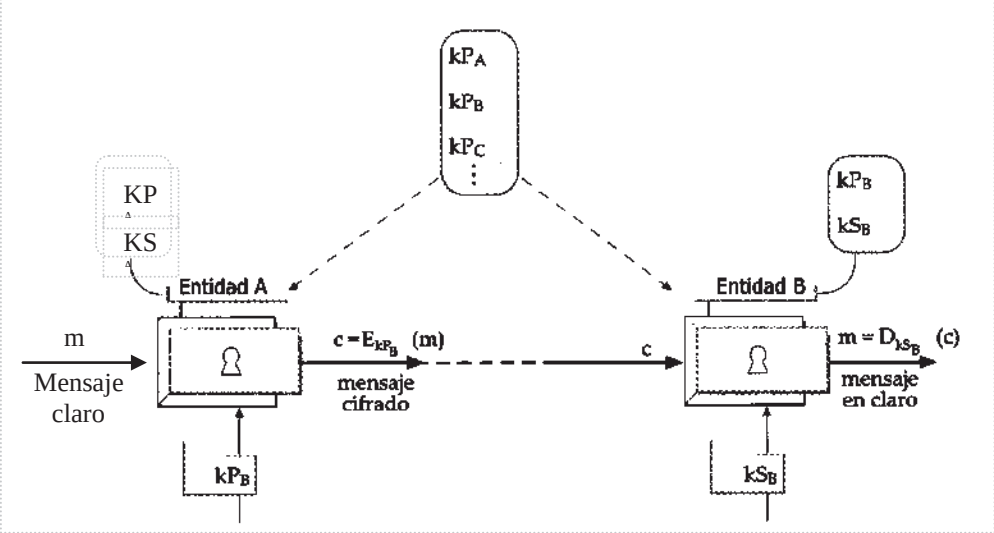


Fig. 35 Criptografía asimétrica

Redes de Computadoras
Austin Community College
Ed. Tittel, McGraw Hill, 2004

El algoritmo más popular en la familia de algoritmos simétricos es Advanced Encryption Standard, AES [2], ya que es el estándar que fue seleccionado en 2002 por NIST (National Institute of Standards and Technology, USA). Mientras que el algoritmo más popular en la familia de algoritmos asimétricos es RSA [3], nombre que proviene de las iniciales de los apellidos de sus inventores (Ron Rivest, Adi Shamir y Len Adleman).

La gran ventaja de los métodos asimétricos es que permiten iniciar las comunicaciones sin tener que haber acordado previamente, y de manera segura, una clave secreta. Sin embargo estos algoritmos son muy costosos desde el punto de vista computacional, por lo que se tiende a utilizar métodos simétricos. En la mayoría de las aplicaciones prácticas, se utilizan los métodos asimétricos para iniciar una comunicación segura durante la cual se establece una clave secreta generada aleatoriamente y se acuerda un algoritmo de cifrado simétrico a partir de las preferencias de los dos interlocutores. A partir de ese momento la comunicación tiene lugar por medio de algoritmos simétricos que son más eficientes.

V. Delgado, R. Palacios: "Introducción a la Criptografía: Tipos de algoritmos", *Anales de Mecánica y Electricidad*,Vol. LXXXIII, Fascículo I, pp. 42-46, 2006.

5.2.3 FIRMA DIGITAL: Es a un mecanismo criptografico donde lo que realmente se cifra con la clave privada del signatario o firmante, es una muestra reducida, un resumen o hash[26] de tamaño fijo (120 0 160 bits según el algoritmo) e independientemente del tamaño del mensaje a firmar. El Receptor del mensaje firmado, mediante unas operaciones de comparación, puede adquirir suficientes garantías acerca de quien es el autor de la firma y sobre la integridad del mensaje recibido.

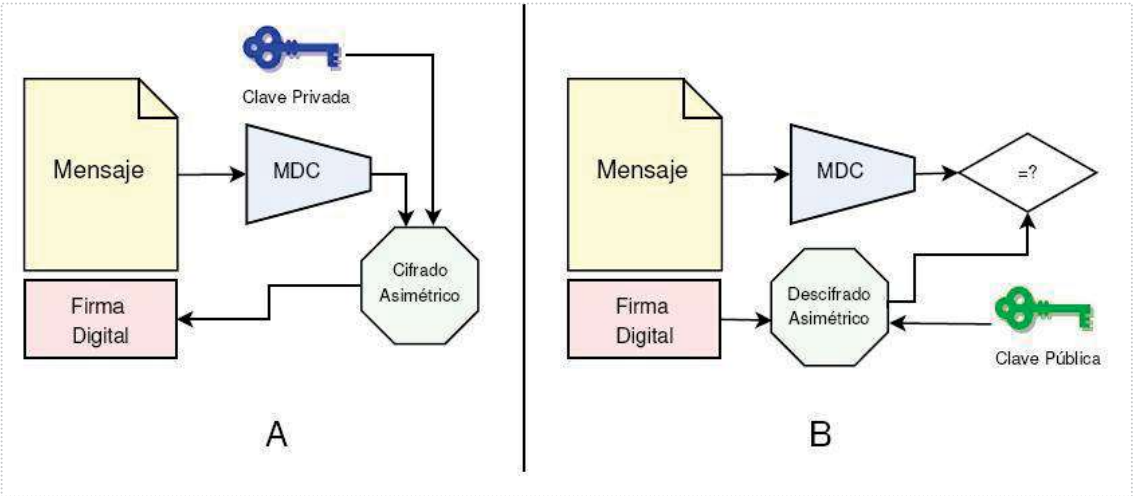


Fig. 36 Esquema de firma digital

[26] **Hash**: se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo,

5.2.4 CERTIFICADO DIGITAL: Es una pieza de información, un documento de capital importancia, en el que se asocia el nombre de una entidad con su clave publica durante un determinado periodo de validez. El certificado es emitido por una TTP[27] especial denominada Autoridad de certificación CA.

El talón de Aquiles de los criptosistemas de clave publica consiste en que si alguien se le engaña acerca del valor de la clave publica de otro usuario, la seguridad se viene abajo, en realidad la clave publica solo hay que darla a conocer a los miembros del dominio de seguridad de que se trate, pero como su conocimiento no tiene nada de reservado, no importa que sea conocida por quienes no tengan nada que ver con ese entorno, lo que si hay que garantizar de algún modo es su validez.

La solución a este problema consiste en garantizar la propiedad y validez de la clave publica mediante la generación de un certificado de la clave publica firmado digitalmente por una autoridad de certificación, CA (. La CA es una tercera parte de confianza (TTP) en la que confían los participantes en la comunicación que son miembros del dominio de seguridad de que se trate.

El certificado digital es una pieza de información en la que se asocia el nombre de una entidad con su clave publica durante un periodo de validez.

Este certificado simplificado de la entidad A consta de dos partes: la primera contiene los datos en los que se aporta la información necesaria, y la segunda parte es la firma de esos datos con la clave privada de la CA. LA siguiente nomenclatura CA<<A>> significa certificado de A generado o expedido por la CA.

[27] **TTP (Trusted Third Party):** Es una autoridad de seguridad, de confianza para otras entidades con respecto a actividades relativas a la seguridad. Con el fin de asegurar los requisitos de seguridad de una comunicación, las TTPs pueden estar involucradas en el protocolo de diferentes maneras.

Es importante hacer notar que el certificado es una pieza de información segura por si misma que, en principio, puede ser reconocida por todos sin ningún género de restricciones, su fortaleza la obtiene de la firma de la CA correspondiente y de la confianza que el receptor del cerificado tienen en esa CA.

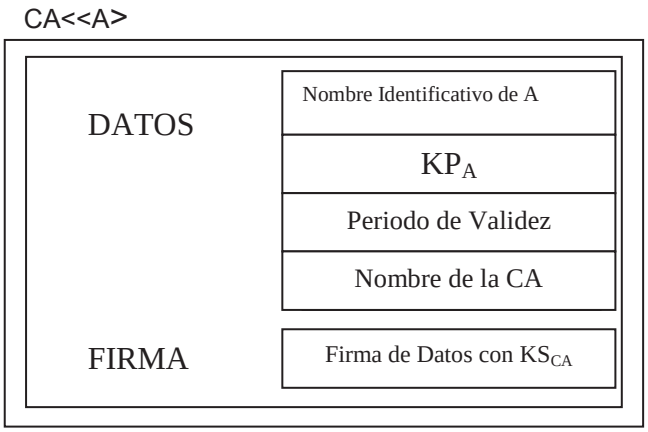


Fig. 37 Firma Digital

Seguridad en Redes Telemáticas
Justo Carracedo Gallardo
McGraw Hill, Madrid Marzo 2004

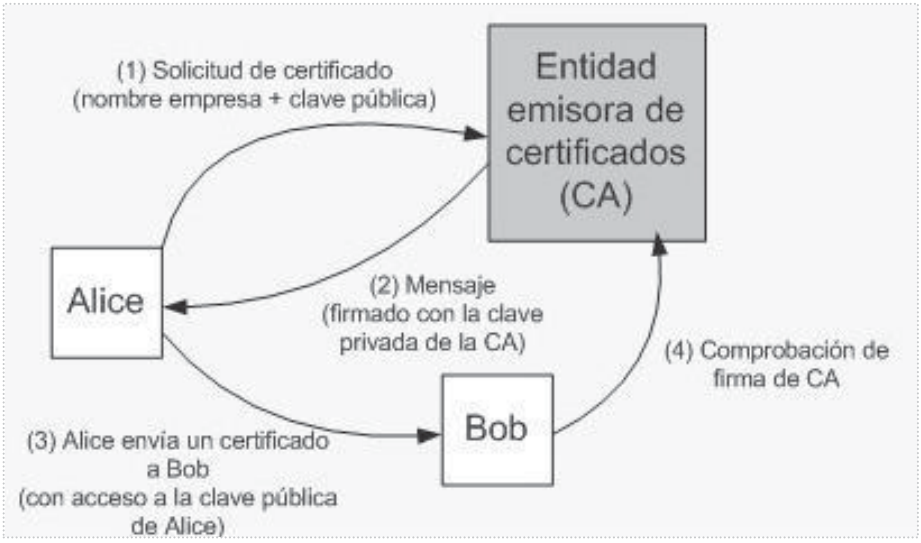


Fig. 38 Proceso de certificación digital

La secuencia de eventos que se muestra en la ilustración 1 es la siguiente:

1. Alice envía a una entidad emisora de certificados una solicitud de certificado firmado que contiene su nombre, su clave pública y quizás alguna información adicional.
2. La entidad emisora de certificados crea un mensaje a partir de la solicitud de Alice. La entidad emisora de certificados firma el mensaje con su clave privada, creando de este modo una firma independiente. A continuación, devuelve el mensaje y la firma a Alice. En conjunto, el mensaje y la firma forman el certificado de Alice.

3. Alice envía el certificado a Bob para darle acceso a su clave pública.

4. Bob comprueba la firma del certificado mediante la clave pública de la entidad emisora de certificados. Si la firma resulta ser válida, acepta la clave pública del certificado como la clave pública de Alice. Como en el caso de la firma digital, cualquier destinatario con acceso a la clave pública de la CA puede determinar si la firma del certificado procede de una entidad emisora de certificados concreta. Este proceso no requiere ningún tipo de acceso a datos secretos.

En el escenario anterior se supone que Bob tiene acceso a la clave pública de la entidad emisora de certificados. Tiene acceso a dicha clave si posee una copia del certificado de la CA que contiene la clave pública.

El formato de los Certificados Digitales es estándar, siendo X.509 v3 el recomendado por la Unión Internacional de Comunicaciones (ITU) y el que está en vigor en la actualidad. El aspecto de los certificados X.509 v3 es el siguiente:

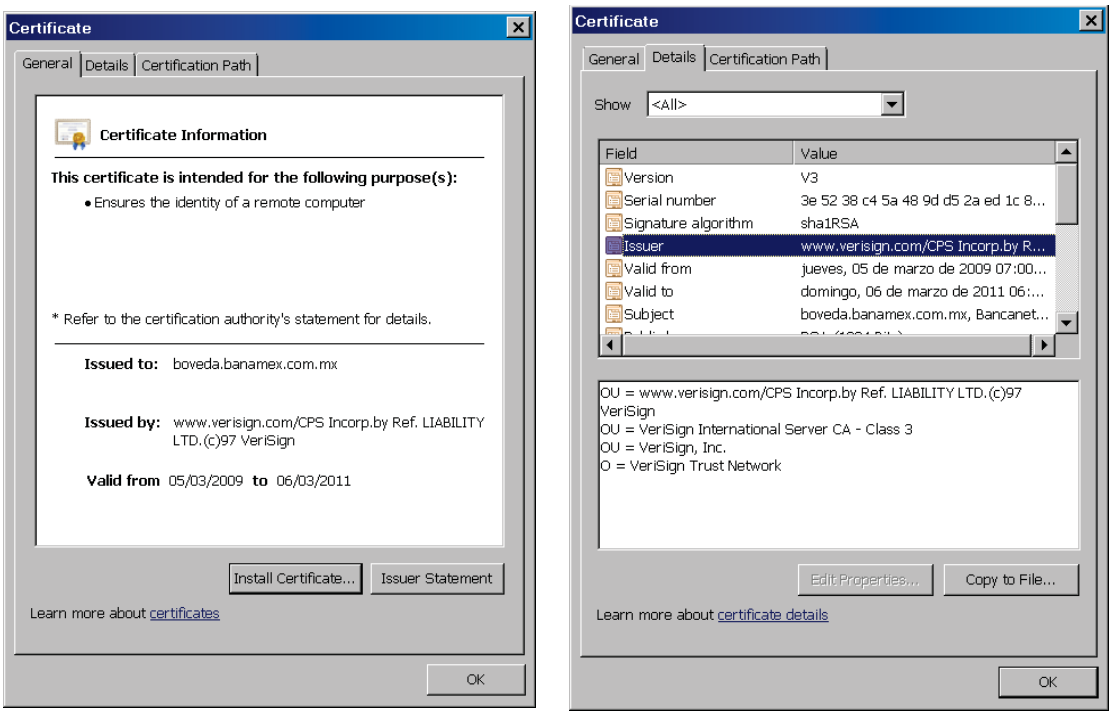


Fig. 39. Formato de los certificados digitales

Los datos que figuran generalmente en un certificado son:

1. Versión: versión del estándar X.509, generalmente la 3, que es la más actual.

2. Número de serie: número identificador del certificado, único para cada certificado expedido por una AC determinada.

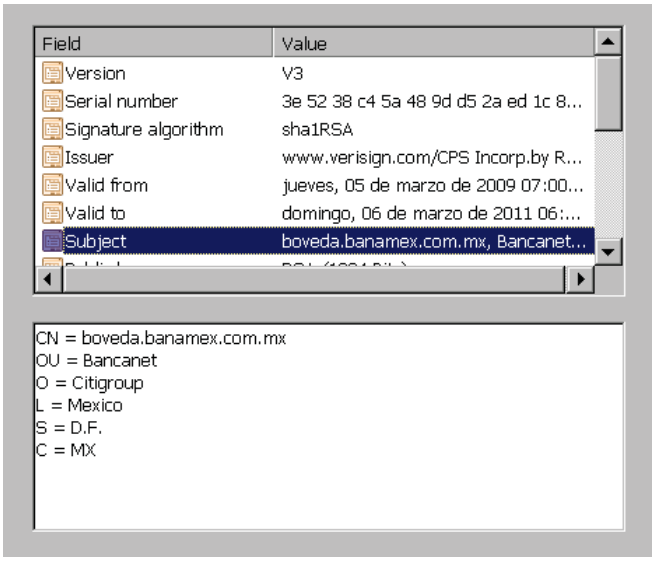
3. Algoritmo de firma: algoritmo criptográfico usado para la firma digital.

4. Autoridad Certificadora: datos sobre la autoridad que expide el certificado.

5. Fechas de inicio y de fin de validez del certificado. Definen el periodo de validez del mismo, que generalmente es de un año.

6. Propietario: persona o entidad vinculada al certificado. Dentro de este apartado se usan una serie de abreviaturas para establecer datos de identidad.

Un ejemplo sería:



CN	Nombre común del Usuario
OU	Información Varia
O	Organización
L	Ciudad
S	Estado
C	País
E	Correo electrónico
UID	ID de usuario

Fig. 40 Datos del certificado digital

En general, podemos decir que una entidad confía en otra entidad cuando la anterior asume que la segunda entidad se comportará exactamente como la anterior espera. Es decir, las entidades involucradas en una comunicación electrónica depositan un cierto grado de confianza en una TTP, que consiste en el hecho que esta TTP actuará tal y como el protocolo establece.

Las TTPs proporcionan una amplia gama de servicios de confianza, tales como certificados de clave públicos, generación y recuperación de claves, emisión de dinero electrónico, servicios de notaria, archivo o registro de evidencias, Realmente, han aparecido distintos tipos de TTPs que proporcionan el mismo servicio, debido a que se han propuesto diferentes soluciones para un mismo servicio. Por tanto tenemos una variedad de TTPs, como las Autoridades de

Certificación, Autoridades de Registro, Bancos Electrónicos, Notarios Electrónicos, Jueces Electrónicos

En muchos casos, los servicios de seguridad requieren una política de seguridad común; es decir, las autoridades de seguridad deben definir un juego de reglas para controlar la manera de usar los servicios de seguridad.

Macià Mut Puigserver; Josep L. Ferrer Gomilla; Llorenç Huguet Rotger
Septiembre de 2002

Hashes Criptográficos

Los hashes criptográficos fueron creados para generar un número aleatorio de un tamaño determinado produciendo el mismo resultado cada vez que los datos que se usan de entrada sean exactamente iguales, o sea, si generamos un hash de un archivo de texto y luego agregamos una letra al texto, el hash cambiaría completamente. Los hashes son generalmente usados para procesar claves y para la verificación de archivos. Por ejemplo, si usted quisiera verificar una claves, la tendría que pasar por el algoritmo del hash y obtendría una lista de números, ahora sin importar cuántas veces usted haga el mismo proceso, si la entrada fuese la misma la salida también sería la misma.

La seguridad de los hashes está basada en que es absolutamente imposible obtener la entrada original que fue utilizada para generar el hash, esto es debido a que los hashes tienen una salida de tamaño constante. O sea si tu usas de entrada para un hash la letra “s”, el hash tendrá el mismo tamaño que si tu usas 700gb de datos, además de esto se puede adherir que es prácticamente imposible generar una colisión (que un grupo de datos cree la misma salida que otro grupo de datos).
Últimamente se ha descubierto que SHA-1 y MD5 tienen colisiones, esto significa que es más “fácil” el crear una entrada que tenga la misma salida que otra entrada.
Por lo demás, la seguridad de los algoritmos fue sólo disminuida, lo que aún nos permite dormir bien a quienes usamos hash para la verificación de claves.

5.3 CRIPTOGRAFÍA EN INTERNET

¿Por que es importante la criptografía en Internet*?* Básicamente toda la estructura del comercio electrónico depende de ella. Recordemos que aunque actualmente los volúmenes de las transacciones en línea no supera los 500 millones de dólares por año las perspectivas más modestas apuestan a que esa cifra suba hasta los 22.000 millones de dólares para el final del milenio. Nicholas Negroponte, uno de los mas reconocidos gurús de Internet, considera montos por cien mil millones de dólares. Pero si, como todos sabemos Internet nacio hace mas de veinte años como una red militar, por que es insegura para transacciones comerciales?

La razón, como la explican los mexicanos Daniel German y Alejandro López Ortiz en su artıculo, ¿Es la red lo suficientemente confiable?, es que"desde sus inicios se decidió que la seguridad de la información que se transmitía no era una prioridad, lo mas valioso en ese momento era interconectar computadoras de forma tal que pudiera resistir fallas severas, posiblemente resultado de un ataque nuclear contra los Estados Unidos".

El protocolo principal por el cual se transmite la información que viaja por la red (TCP/IP, Transfer Control Protocolo/Internet Protocolo) no ha variado en su esencia desde la creación de Internet. Esta información se divide en paquetes mas pequeños a los cuales se llama datagramas. Estos datagramas son enviados por la red sin ningún orden específico. Así cuando enviamos un mensaje que contenga, por ejemplo, las letras ABCD, este se dividirá en cuatro datagramas, cada uno con una letra. Estos datagramas viajaran de modo independiente, para luego recomponerse en la computadora de destino, sin que el receptor final pueda saber que ruta tomo cada uno de ellos. Sin embargo, ninguno de estos datagramas esta encriptado y cualquiera que los tome en su recorrido puede leerlos sin problema. Y aquí es donde entra la criptografıa como aliada del comercio en lınea. La idea es encontrar un sistema en donde los datos comerciales y financieros puedan viajar de un modo seguro por la red.

5.3 COMERCIO ELECTRÓNICO

Cualquier forma de transacción comercial en la que las partes interactúa electrónicamente, en lugar de hacerlo por intercambio o contacto físico directo

El comercio electrónico es tecnología para el cambio, y comienza a transformarse en una herramienta crucial para la sociedad moderna y el desarrollo económico, por lo cual un crecimiento masivo en este campo parece inevitable. El comercio electrónico se convierte en una necesidad estratégica dentro de los negocios, tanto en los sectores privados como públicos, constituyéndose en un factor clave para reducir los costos, incrementar la competencia y enfrentar la alta velocidad de demanda de los consumidores. Las empresas que lo miren como un "complemento" a su forma habitual de hacer negocios, obtendrán sólo beneficios limitados, siendo el mayor beneficio para aquellas que sean capaces de cambiar su organización y sus procesos comerciales para explotar completamente las oportunidades ofrecidas por el comercio electrónico.

Ventajas y oportunidades.

El comercio electrónico le permite al empresario:

- Desaparecer los límites geográficos para su negocio.
- Estar disponible las 24 horas, 7 días a la semana, todos los días del año.
- Reducción de un 50% en costos de la puesta en marcha del comercio electrónico, en comparación con el comercio tradicional.
- Hacer más sencilla la labor de los negocios con sus clientes.
- Reducción considerable de inventarios.
- Agilitar las operaciones del negocio.
- Proporcionar nuevos medios para encontrar y servir a clientes.
- Incorporar internacionalmente estrategias de relaciones clientes-proveedores.
- Reducir el tamaño del personal de la fuerza.
- Menos inversión en los presupuestos publicitarios.
- Reducción de precios por el bajo coste del uso de Internet.
- Cercanía a los clientes y mayor interactividad y personalización de la oferta.
- Desarrollo de ventas electrónicas.

- Globalización y acceso a mercados potenciales de millones de clientes.
- Implantar tácticas en la venta-productos para crear fidelidad en los clientes.
- Enfocarse hacia un comercio sin el uso del papel, es posible a través del EDI.
- Bajo riesgo de inversión en comercio electrónico.
- Rápida actualización en información de productos y servicios de la empresa
- Obtener nuevas oportunidades de negocio, con la presencia en el mercado.
- Reducción del costo real al hacer estudios de mercado.

Además el comercio electrónico brinda grandes ventajas y oportunidades al cliente como:

- Un medio que da poder al consumidor de elegir en un mercado global.
- Brinda información pre-venta y posible prueba del producto antes de comprar.
- Inmediatez al realizar los pedidos.
- Servicio pre y post-venta on-line.
- Reducción de la cadena de distribución, lo que le permite adquirir un producto a un mejor precio.
- Mayor interactividad y personalización de la demanda.
- Información inmediata sobre cualquier producto, y disponibilidad de acceder a la información en el momento que así lo requiera.

5.3.1 RIESGOS DEL COMERCIO ELECTRÓNICO

El comercio electrónico puede resultar de alto beneficio para la reducción de los costos de las organizaciones y en sus negocios, y crear oportunidades en nuevos y mejores servicios a los clientes. Sin embargo, los sistemas electrónicos y la infraestructura que le da soporte al comercio electrónico son susceptibles de situaciones de abuso, mal uso y fallas en muchas de sus formas

El comercio electrónico en Internet y otras redes públicas pone de manifiesto algunos aspectos críticos:

- La demanda de los consumidores para acceder de forma segura al comercio y otros servicios es muy alta.
- Los comerciantes quieren métodos simples y de bajo costo para manejar las transacciones electrónicas.

- Las instituciones financieras requieren de los proveedores de software soluciones competitivas en precio, manteniendo altos niveles de calidad.
- Las instituciones financieras, las empresas de medios de pago, las administradoras de tarjetas y los propietarios de marca necesitan diferenciar el comercio electrónico, sin afectar significativamente sus infraestructuras.

Factores críticos dentro de la estrategia de implantación del comercio electrónico, el papel y responsabilidad de las empresas de medios de pago, las instituciones financieras, y los comerciantes es crucial para establecer especificaciones que permitan, mínimamente, los objetivos de:

- Proporcionar confidencialidad en las comunicaciones
- Proporcionar *confidencialidad* en las comunicaciones.
- *Autenticar* todas las partes involucradas.
- Garantizar la *integridad* de las instrucciones de pago.
- *Autenticar* la identidad del usuario y el comerciante.

Desde la perspectiva del negocio, las consecuencias más comunes del abuso, el mal uso y las fallas, pueden incluir:

- **Pérdidas financieras como resultado de un fraude***:* alguien puede transferir fondos, en forma fraudulenta, de una cuenta a otra, o destruir importantes registros financieros.
- **Pérdidas de información confidencial de valor:** una intrusión puede revelar información a partes no autorizadas para su conocimiento, resultando en un daño muy importante.
- **Pérdidas de oportunidad de negocio a través de discontinuidad del servicio***:* los servicios comerciales, electrónicamente dependientes, pueden ser interrumpidos por largos o inaceptables períodos de tiempo, como resultado de ataques deliberados o eventos accidentales. El costo puede ser catastrófico.

- ***Utilización no autorizada de los recursos:*** un ataque externo puede generar acceso a los recursos no autorizados, y hacer uso de la información para el beneficio propio.
- ***Pérdida de confidencia o respeto del cliente****:* una organización puede sufrir pérdidas significativas como resultado de la publicidad negativa de una intrusión o falla.

5.3.2 LA CRIPTOGRAFÍA APLICADA AL COMERCIO ELECTRÓNICO

Procesos típicos del comercio electrónico:

- Envío de la orden de pedido al comerciante, junto con información sobre el instrumento de pago.
- Solicitud de autorización del comerciante a la institución financiera del comprador
- Confirmación de la orden por parte del comerciante
- Solicitud de reembolso del comerciante a la institución financiera del comprador

Esta es una secuencia de procesos que se distingue poco de la utilizada en el comercio convencional, lo que constituye una de las premisas para su desarrollo. La característica principal es la ausencia del *cara a cara* entre el comerciante y el comprador, sin embargo, el comercio electrónico permite la "*identificación*" y "*autenticación*" de las partes intervinientes.

Por tanto, los procesos definidos en las transacciones de comercio electrónico, dentro de los límites establecidos, son:

- Proporcionar la *autenticación* necesaria entre compradores, comerciantes e instituciones financieras
- Garantizar la *confidencialidad* de la información sensible (número de tarjeta o cuenta, fecha de caducidad, etc.)

- Preservar la *integridad* de la información que contiene tanto la orden de pedido como las instrucciones de pago

Aunque estos aspectos son importantes en cualquier red de transmisión de datos, su vulnerabilidad causa una preocupación mucho mayor cuando se relacionan con Internet u otra red pública de datos, por su ubicuidad y desconocimiento de todas las partes actuantes.

Cómo se logra la implementación, en los procesos, de *autenticación, confidencialidad e integridad* enunciados anteriormente:

- La *confidencialidad* (no vulnerabilidad de la información conteniendo los datos necesarios para realizar el pago, tales como el número de cuenta o tarjeta y su fecha de caducidad) se alcanza mediante la encripción de los mensajes
- La *integridad* de los datos conteniendo las instrucciones de pago, garantizando que no han sido modificados a lo largo de su trayecto, se consigue mediante el uso de firmas digitales
- La *autenticación* del comprador, como usuario legítimo de la tarjeta o cuenta sobre la que se instrumenta el pago del bien o servicio adquirido, se consigue mediante la emisión de certificados y la generación de *firmas digitales*
- La *autenticación* del comerciante, garantizando que mantiene una relación comercial con una institución financiera que acepta el pago mediante tarjetas, se consigue mediante la emisión de certificados para el comerciante y las correspondientes *firmas digitales*

Los algoritmos criptográficos empleados para los procesos de encriptación, emisión de certificados y generación de firmas digitales son de doble naturaleza. Por un lado, se define un algoritmo de clave privada, de fortaleza contrastada y excelente rendimiento: DES (Data Encryption Standard), en uso desde 1977. Por otro lado, se hace imprescindible contar con un algoritmo que permita el

intercambio de claves en una red pública, con total seguridad, entre múltiples participantes sin ninguna relación previa; un algoritmo como el descrito se define de clave pública, y generalmente se emplea el diseñado por Rivest, Shamir y Adleman, cuyas iniciales componen su nombre: RSA.

Esencialmente, cada algoritmo criptográfico permite la implementación de una función determinada. DES se emplea para garantizar la confidencialidad de los mensajes transmitidos; RSA se emplea para garantizar la integridad de los datos y la autenticidad de los participantes. RSA desempeña todavía una función adicional, posible gracias a su definición como algoritmo de clave pública (también se conoce como algoritmo asimétrico, por emplear dos claves diferentes, una para la encriptación y otra para la desencriptación): permite la distribución y utilización de una clave secreta entre participantes sin ninguna relación previa y, lo que es más importante, sobre canales (vínculos de comunicación) no asegurados

Information Systems Control Journal, Volume 6, 2000
By Marcelo Héctor González, CISA, ASS

Las ventajas del comercio electrónico son evidentes. El comprador puede ver de manera rápida todo el escaparate electrónico y no tiene que ir tienda por tienda en busca del producto deseado. Se optimiza también el tiempo de atención al cliente, que no tiene que esperar largas colas para ser atendido.

Uno de los objetivos fundamentales de la criptografía, es proporciona al comercio electrónico las herramientas necesarias para garantizar, dado el caso, el carácter secreto de la información intercambiada (confidencialidad), así como la no manipulación de la misma entre el origen y el destino (integridad).

Hoy día existen diferentes protocolos como el SET (Secure Electronic Transaction) o el SSL (Secure Sockets Layer) que se ocupan de que este tipo de transacciones a través de redes informáticas sean lo más seguras posibles.

Miguel Ángel Sarasa López
Boletín del Criptonomicón
Año I, nº 25, 28 de octubre de 1998

PROTOCOLO SET: Transacciones Electrónicas Seguras (Secure Electronic Transaction o SET) es un protocolo estandarizado y respaldado por la industria, diseñado para salvaguardar las compras pagadas con tarjeta a través de redes abiertas, incluyendo Internet. El estándar SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras.

El 19 de diciembre de 1997 Visa y MasterCard formaron SET Secure Electronic Transaction LLC (comúnmente conocida como "SETCo") para que implantase la especificación. En cuanto el protocolo SET 1.0 fue finalizado, comenzó a emerger una infraestructura basado en el mismo para dar soportar su uso a gran escala. Ya existen numerosos fabricantes de software que han empezado a crear productos para consumidores y comerciantes que deseen realizar sus compras de manera segura disfrutando de las ventajas ofrecidas por SET.

Gonzalo Álvarez Marañón, CSIC
2007

Proceso de pago con SET

El proceso de pago en una transacción electrónica usando el protocolo SET admite un grán número de opciones diferentes pero, básicamente, consta de los siguientes pasos:

1. El cliente, trás seleccionar los artículos a comprar en el sitio web del vendedor, envía a éste un formulario de pedido, siendo respondido por el comerciante con el envío de su certificado digital y el de la pasarela de pago.

El cliente comprueba la validez de los certificados y envía entonces al comerciante una orden de pago, que está dividida en dos secciones o documentos diferentes: la Información de pedido (OI), en la que figuran los datos de los productos comprados, su precio y las demás informaciones necesarias para la compra, y la Instrucción de compra (PI), en donde se describen sus datos bancarios y se dan instrucciones para el pago a la entidad vendedora.

2. Esta orden de pago se firma digitalmente por medio de un algoritmo especial, denominado Firma Dual, que se realiza concatenando primero los resúmenes hash de los dos documentos generados y encriptándo esta concatenación después con su llave privada, para seguidamente encriptar la Firma Dual mediante una clave simétrica generada por su software SET. Por último, se encriptan la clave simétrica generada y el número de la trajeta de crédito con la llave pública de la pasarela de pago.
De esta forma el vendedor no puede conocer los datos bancarior del comprador, y el banco no puede conocer la información sobre los productos comprados, a pesar de que ambos documentos están ligados por la misma firma. En ciertos casos es posible realizar la transacción sin esta firma dual, estableciéndose mediante un protocolo inicial qué metodo se va a usar.

3. El vendedor recibe la orden de compra y la firma dual del ciente, se queda con la descripción de la compra y trás comprobar la auntenticidad del comprador, utilizando para ello la firma digital de éste y su certificado, y la integridad de los datos recibidos envía los datos financieros a la Pasarela de Pago encriptados con la clave pública de la misma.

4. La Pasarela de Pago comprueba la autenticidad del comprador y la integridad del PI del mismo, y con el mensaje del vendedor comprueba la relación existente entre la descripción de la compra enviada al vendedor y la usada para la firma dual recibida.

5. Si todo es correcto, la Pasarela de Pago envía mediante las redes de comunicación bancarias el PI al banco del vendedor y solicita autorización para el pago, mediante un documento denominado Petición de autorización de pago.

6. El banco del vendedor comprueba entonces que la tarjeta de crédito es válida y permite el cargo del importe de la compra, enviando entonces un documento a la pasarela, denominado Autorización de pago, autoriza el proceso de compra.

7. Una vez informado el vendedor de la autorización procede al envío de los artículos comprados al cliente, y después de la entrega física del producto pide el importe de la venta a la Pasarela de Pagos, proceso que se conoce con el nombre de Solicitud de pago.

8. Entonces la Pasarela de Pagos pide al banco del comprador la transferencia del importe de la venta al banco del vendedor, petición que recibe el nombre de Solicitud de compensación. Entonces se le hace efectivo al vendedor el importe, con lo que se cierra el proceso total de compra.
Todos los documentos implicados en el proceso anterior deben llevar un número identificador único de transacción, conocido como ID.

Fig. 41 Proceso completo de pago mediante SET

Protocolos de uso general y particulares

PROTOCOLO	*PROPOSITO*
CyberCash	Transacciones electrónica de Fondos
DNSSEC	Sistemas de Dominio de Nombres
IPSec	Encripción a nivel de paquete
PCT	Encriptamiento a nivel de TCP/IP
PGP	E-Mail
S/MIME	El desplegado de WEB
Secure RPC	Llamadas a procedimientos remotos
SET	Transacciones electrónica de Fondos
SSL	Login Remoto
TLS	Encriptamiento a nivel de TCP/IP

Fig.42 Protocolos y sus Propósitos

Algunos fueron diseñados para seguridad en módulos específicos de comunicación, tales como el e-mail y el login remoto. Otros son generados, proveen servicios de criptografía para múltiples nodos de comunicación.

Applied Cryptography,
Bruce Scheneier Addison-Wiley

5.3.3 ENCRIPTACION CON MD5 EN PHP

Hoy en día la mayoría de las páginas web utilizan bases de datos para poder desarrollar portales dinámicos y así hacerlos más atractivos a la vez que útiles. Pero esta información que se guarda en la base de datos tiene que tener algún tipo de protección. Es por ello que algunos campos se guardan encriptados en la base de datos, principalmente cuando una página requiere el nombre de usuario y contraseña, esta última se encripta y se guarda en la Base de datos.

En PHP se utiliza la función MD5 (Message Digest 5), que es una función hash irreversible (de un sólo sentido), es decir, encripta el password tecleado por el usuario y es imposible que partiendo desde la cadena encriptada se vuelva a la contraseña origen. Por esto mismo no hay problema de que alguien pueda acceder al campo encriptado de la base de datos.

Como en la base de datos se guarda la contraseña encriptada, cuando un usuario quiere acceder, habrá que realizar una comparación entre el password que introduce encriptado en MD5, y lo que tenemos en la base de datos, (que es la contraseña encriptada en MD5), si coincide se le permite el acceso, si no, se rechaza.

MD5 se utiliza también para que cuando un usuario olvida su password, si quiere recuperar la contraseña se le pide que introduzca por ejemplo el correo, y se le envía un mail con una URL tal que si entra en ella genere una nueva contraseña que se le indica al usuario y se reescribe en md5 en la base de datos (borrando la anterior contraseña).

Hay que tener en cuenta que esto no es 100% seguro, puesto que la contraseña se encripta en el servidor, entonces al enviar la contraseña desde el cliente al servidor podría ser interceptada.

Para hacernos una idea, el algoritmo MD5 convierte el mensaje en un bloque múltiplo de 512 bits, (si hace falta añadirá bits por el final). Luego coge el primer

bloque de 512 bits del mensaje y realiza diversas operaciones lógicas con los 128 bits de cuatro vectores iniciales ABCD de 32 bits cada uno. (Dichos vectores tendrán el valor inicial que nosotros queramos).

Como resultado obtiene una salida de 128 bits que se convierte en el nuevo conjunto de los 4 vectores ABCD. Se repite el algoritmo hasta procesar el último bloque del mensaje. Al terminar, el algoritmo devuelve los últimos 128 bits de estas operaciones.

5.4 SEGURIDAD WEB

La seguridad en web tiene 3 etapas* primarias:

- **Seguridad de la computadora del usuario**: Los usuarios deben contar con navegadores y plataformas seguras, libres de virus y vulnerabilidades. Tambiéndebe garantizarse la privacidad de los datos del usuario.

- **Seguridad del servidor web y de los datos almacenados:** ahí Se debe garantizar la operación continua del servidor, que los datos no sean modificados sin autorización (integridad) y que la información sólo sea distribuida a las personas autorizadas (control de acceso).

- **Seguridad de la información que viaja entre el servidor web y el usuario:** Garantizar que la información en tránsito no sea leída (confidencialidad), modificada o destruida por terceros. También es importante asegurar que el enlace entre cliente y servidor no puede interrumpirse fácilmente (disponibilidad).

Eduardo Espina
Segridad de la web

Cuando se creo por primera vez la Web no podía imaginarse el modo que iba a crecer y los tipos de información que atravesarían Internet hoy en día. A medida que las empresas fueron inaugurando sus escaparates Web en Internet empezó a quedar claro que era necesario implantar protocolos y procedimientos para proteger la trasferencia de información sensible, como por ejemplo las datos de las tarjetas de crédito, números de carnet de identidad y de la seguridad social y otro tipo de datos de identificación personales dentro de un explorador.
La primera solución popular para proporcionar autentificación, integridad y privacidad para las transacciones fue SSL (Secure Sockets Layer, nivel de conectores seguros). SSL fue desarrollado originalmente por Netscape y ahora es gestionado por IETF (Internet Enginnering Task Force). La IETF renombro el protocolo denominado TLS (Transport Layer Security seguridad de nivel de trasporte). Pero es muy probable que continúe el lector encontrando referencias a SSL en la literatura y en general puede considerarse que SSL Y TLS son idénticos. Una de las características mas adecuadas de SSL/TLS es que se puede ser empleado por otros protocolos además de http.

El protocolo seguro esta situado entre el protocolo de trasporte y el protocolo de nivel de aplicación y para los servicios de nivel superior. TLS aparece como si fuera un protocolo de trasporte normal. La aplicación no necesita hacer nada especial para crear los mecanismos adicionales de seguridad, por que estos son gestionados por un protocolo de nivel inferior. Además de las funciones seguras, TLS también proporciona todas las funciones de tipo TCP, como el control de flujo, el control de congestión y la fiabilidad.

Cuando se utiliza http en conjunción con TLS, se lo suele denominar HTTPS (http seguro), especificándoselo como tal en la dirección URL, Por ejemplo, para conectarse al servidor Web de Texas Stars con una conexión http segura, LA dirección URL seria Https://www.texas-star.com.
Se utiliza (HTTPS) en lugar de http. Esta conexión utiliza un puerto IP diferente de las conexiones HTTP estándar, que emplea el puerto 80. De manera predeterminada, HTTPS utiliza el puerto 443. Una gran ventaja de utilizar un

protocolo seguro que sea independiente de las aplicaciones y de los protocolos de nivel superior es la posibilidad de permitir trasmisiones interactivas seguras en tiempo real. Para proporcionar conversaciones seguras interactivas. TLS esta dividido en dos partes: 1 protocolo de negociación y 1 protocolo de registro.

El protocolo de negociación: TLS se utiliza para negociar y establecer los parámetros para la conexión. Entre estos parámetros de configuración podemos citar elementos tales como la clave de sesión y los algoritmos de cifrado. Si los parámetros de conexión especifican el uso de certificados, el protocolo de negociación gestiona el intercambio de los mismos. Este tipo de certificados garantizan que el receptor obtenga una copia confiable de la clave publica de su interlocutor. Una vez instalado el certificado en el explorador del usuario el servidor Web puede verificar los mensajes procedentes del usuario, utilizando para ello su clave privada.
El protocolo de registro: Se encarga de la trasferencia de datos a través de la conexión HTTPS. Gestiona los procedimientos necesarios para realizar la fragmentación o precomposición de los mensajes de nivel de aplicación. Además puede trasmitir los datos en formato comprimido. La compresión no añade seguridad, pero puede contribuir a la acelerar la trasferencia de los datos.

El protocolo TLS proporciona la capacidad de continuar con una sesión interrumpida. Esto resulta particularmente útil para las transacciones Web, en la que se trasmiten diferentes tipos de información al usuario. TCP crea una nueva conexión por cada archivo trasferido. Por tanto si una pagina Web contiene vínculos a varios elementos gráficos, se abrirá una nueva conexión TCP de trasferencia de datos separada para cada una de las imágenes graficas. Con TLS, establecer una nueva sesión para cada trasferencia de archivo requerirá una gran cantidad de tiempo y de recursos. En lugar de ello, si el servidor dispone todavía de una sesión activa con el mismo usuario, se empleara el mismo ID de sesión para todas las trasferencias de archivos hacia el explorador.
¿Cómo podemos saber si una conexión se está realizando mediante SSL?. Generalmente los navegadores disponen de un icono que lo indica,

generalmente un candado en la parte inferior de la ventana. Si el candado está abierto se trata de una conexión normal, y si está cerrado de una conexión segura. Si hacemos deble click sobre el candado cerrado nos aparecerá el Certificado Digital del servidor web seguro.

Además, las páginas que proceden de un servidor SSL vienen implementadas mediante protocolo HTTP seguro, por lo que su dirección, que veremos en la barra de direcciones del navegador, empezará siempre por https, por ejemplo:

https://www.htmlweb.net

Redes de Computadoras
Austin Community College
Ed. Tittel, McGraw Hill, 2004

Asegurar paginas Web con los exploradores de la Web funciona para crear un sistema de seguridad casi impenetrable que protege los datos que envía por la Internet. Cuando se envía la información esta puede pasar a través de muchas computadoras antes de alcanzar su destino. Si no esta conectado a una pagina Web asegurada, otras personas en Internet pueden visualizar la información.

Cuando se visita una pagina Web asegurada, su explorador por lo general mostrara un candado o llave en la pantalla para indicar que la pagina esta asegurada, muchos exploradores también muestran un cuadro de dialogo alertándolos de que esta a punto de visualizar una pagina Web asegurada.

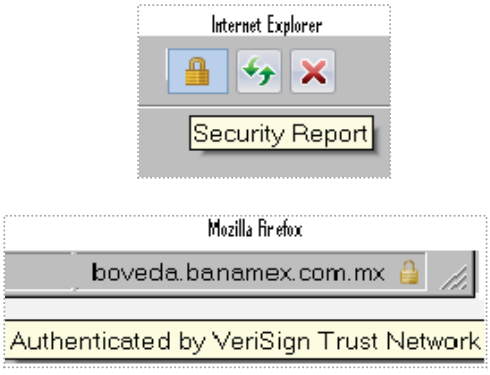


Fig. 43 Conexión segura mediante SSL

Aprenda Internet y la World Wide Web
Kelleigh Wing, Paul Whitehead, Ruth Maran
2da Edición, From MaranGraphics
2001 pos ST Editorial Inc.

5.4.1 RECOMENDACIONES PARA GESTIONAR SERVIDORES WEB.

- Sitúe sus servidores Web en una zona desmilitarizada. Configure el cortafuegos para eliminar todas las conexiones al servidor Web en todos los puertos, Excepto http (puerto 80) o HTTPS (puerto 443).
- Elimine todos los servicios no necesarios de su servidor Web, manteniendo FTP (solo si lo necesita) y una capacidad de inicio de sesión seguro, como por ejemplo una Shell[28] segura. Todo servicio no necesario se convierte en un posible punto de ataque.
- Desactive las posibilidades de administración remota, a menos que esta se realice utilizando una contraseña de un solo o un enlace cifrado.
- Limite el número de personas que tengan acceso de administrar o de nivel raíz.
- Registre toda la actividad de los usuarios y conserve dichos registros en forma cifrada en el servidor Web o almacénelos en una maquina independiente dentro de su intranet.
- Monitoree los registros del sistema de forma regular, en busca de actividades sospechosas. Instale macros de captura para detectar los ataques que se produzcan contra el servidor. Cree macros que se ejecuten cada hora, aproximadamente, y que compruebe la integridad de las contraseñas y de otros archivos críticos. Cuando esas macros detectan algún cambio, debe enviarse un mensaje de correo electrónico al administrador del sistema.
- Elimine todos los archivos innecesarios, como pdf, del directorio de scripts /cgi-bin.
- Elimine los árboles de documentos predeterminados incluidos en servidores Web tales como IIS y EXAir. Aplique todos los parches de seguridad relevantes tan pronto como sean anunciados.

[28] **Shell**: es un programa informático que actúa como interfaz de usuario para comunicar al usuario con el sistema operativo mediante una ventana que espera órdenes escritas por el usuario en el teclado.

- Si necesita utilizar una interfaz grafica de usuario en la consola, elimine los comandos que arrancan automáticamente el gestor de ventanas de directorios de arranque.
- Si la maquina debe ser administrada remotamente, exija que se utilice algún tipo de mecanismo seguro, como por ejemplo una Shell segura para realizar la conexión, no permita las conexiones Telnet o FTP anónimas hacia esta maquina desde ningún sitio de Internet que no sea de confianza.
- Ejecute el servidor Web en una parte del arbol del directorio configurada para que el servidor no pueda acceder a los archivos reales del sistema.
- Realice todas las actualizaciones desde la intranet. Mantenga los originales de las paginas Web en un servidor de la intranet y realice ahí todos los cambios y actualizaciones. Después, cargue dichas actualizaciones en el servidor publico mediante una conexión SSL. Si hace esto cada hora evitara que un servidor corrupto quede expuesto durante un periodo de tempo prolongado.
- Analice su servidor Web periódicamente con herramientas tales como ISS (busca vulnerabilidades).
- Haga que el software de detección de intrusiones monitorice las conexiones efectuadas con el servidor, configure el detector para que proporciones una alarma al detectar ataques conocidos y actividades sospechosas y para que capture dichas sesiones con el fin de revisarlas periódicamente.

5.4.2 SEGURIDAD EN CORREO ELECTRÓNICO.

Cuando se envía un mensaje de correo electrónico a una persona situada en una ubicación diferente, el mensaje a través de diversos encaminadores y equipos de red, hasta llegar al receptor. En cualquier parte del camino, el mensaje puede ser captado por alguna persona y los contenidos de este leídos.

Además la persona no autorizada que lea el mensaje puede volver a insertarlo en el medio de trasmisión en forma modificada y/o puede respondernos en

forma tal que pensemos que la respuesta es legitima y que esta proviene de receptor al que destinábamos el mensaje, para proporcionar un entorno que haga el correo electrónico mas difícil de leer al ser capturado por un hacker, las personas y las aplicaciones utilizan técnicas de cifrado para codificar los mensajes de correo electrónico, entre los mas populares se encuentran PGP (Pretty Good Privacy) y PEM (Privacy Enhanced E-mail).

Pretty Good Privacy: Puede utilizarse para cifrar cualquier tipo de datos. Este sistema fue desarrollado por Phil Zimmermann y proporciona lo siguiente:

- Privacidad
- Autenticación
- Firmas digitales
- Compresión

Algunos productos comerciales utilizan PGP, la estructura de PGP se basa en RSA, en IDEA(International Data Encrypyion Algorithm, algoritmo de cifrado de datos internacional, y en MD5. Cuando un usuario Implementa PGP por primera vez para enviar un mensaje, PGP efectúa un compendio del mensaje mediante MD5[29] y luego cifra el resultado con la clave RSA privada del usuario.

EL mensaje original y el compendio cifrado se incorporan en un único mensaje y se comprimen utilizando ZIP. La tecnología Zip utiliza el algoritmo de IV-Lempel para comprimir los datos. El programa PGP del sistema del emisor solicitara que se introduzcan algunos datos aleatorios. Utilizando esa entrada aleatoria y la velocidad de escritura en el teclado del emisor; se utiliza IDEA para producir un mensaje de 128 bits que actúa como clave de sesión. A continuación, la clave de mensaje se utiliza para cifrar los datos comprimidos del emisor. Finalmente, el mensaje se vuelve a cifrar con la clave pública del receptor.

[29] **MD5, *Message-Digest Algorithm 5***: Algoritmo de Resumen del Mensaje 5: es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Los datos componentes resultantes de las operaciones realizadas por PGP se convierten a Base64 y se envían en forma de mensaje con formato MIME. El receptor invierte la codificación de Bit Base64 y descifra el mensaje con su clave privada. Después, descomprime la información y extrae el texto en claro del compendio cifrado.

Después, se descifra el compendio utilizando la clave pública del emisor. El receptor lleva a cabo los cálculos MD5 con el texto en claro y si concuerda con el compendio añadido al mensaje, el receptor sabrá que el mensaje es correcto y el emisor autentico.

Pretty Good Privacy: Proporciona soporte para tres diferentes longitudes de claves RSA dependiendo del tipo de organización que este usando PGP:

- 126 bits Esta longitud esta diseñada para el suso ocasional y no debe emplearse por parte de organizaciones o empresas que estén intercambiando información sensible.
- 512 bits Esta longitud de clave esta diseñada para el uso comercial y puede ser descifrada por organizaciones o personas que dispongan los suficientes recursos financieros, es decir, de un montón de dinero o recursos.
- 1024 bits Este tamaño de clave esta diseñado para uso militar y es esencialmente imposible de romper en un plazo de tiempo comparable al tiempote vida de un ser humano.

Redes de Computadoras
Austin Community College
Ed. Tittel, McGraw Hill, 2004

La diferencia entre Criptografía y seguridad informática

En un modelo criptográfico típico, existen dos puntos: "a" y "b", que se consideran fiables y, entre ellos, se transmite información mediante un canal no fiable. La Criptografía se ocupa de los problemas relacionados con la transmisión confidencial y segura por el medio no fiable, en tanto la seguridad informática se ocupa de asegurar la fiabilidad de los nodos "a" y "b".

Limitaciones de la Criptografía

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encripción se hacen más fáciles de quebrar debido al avance de la velocidad y potencia de los equipos de computación. Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta-tratar sistemáticamente con cada posible clave de encripción, buscando colisiones para funciones hash, factorizando grandes números, etc.- la fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo.

En 1977 Martin Gardner escribió que los números de 129 dígitos nunca serían factorizados, en 1994 se factorizó uno de esos números. Además de la fuerza bruta, avanzan las matemáticas fundamentales que proveen nuevos métodos y técnicas de criptoanálisis.

Ing. *Yran Marrero Travieso*, El 18/09/l 2003.
Centro Provincial de Información de Ciencias Médicas.
La Habana

5.5 FUTURO DE LA CRIPTOGRAFÍA

Quantum Cryptography, Cifrado cuántico). La criptografía cuántica es la criptografía que utiliza principios de la mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida. Las actuales técnicas de la criptografía cuántica permiten a dos personas crear, de forma segura, una clave secreta compartida que puede ser usada como llave para cifrar y descifrar mensajes usando métodos de criptografía simétrica.

La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas.

En teoría el cifrado cuántico es imposible de vulnerar porque la información es codificada normalmente en **fotones** que no pueden ser intervenidos sin destruir el mensaje. En tanto los algoritmos de cifrado usados actualmente están basados en teorías matemáticas y, en principio, pueden ser vulnerados si se tiene la suficiente capacidad de cálculo computacional.

La delincuencia informática parece que va más rápida que su seguridad. Dentro de 30 años, muchos de los secretos que guarda el mundo moderno bajo potentes algoritmos criptográficos, como los datos médicos o la información clasificada de los gobiernos, correrán un peligro real de saltar por los aires. La criptografía cuántica se encargará de que su descifrado sea un juego de niños, susceptible de caer en manos de terroristas o criminales.

Quien realizó tal profecía no fue un simple agorero, sino respetables investigadores como Martin Hellman, coinventor de la criptografía de clave pública, y el criptólogo argentino Hugo Scolnik, durante sus intervenciones en el Día Internacional de la Seguridad de la Información en la Universidad Politécnica de Madrid.

Hellman y Scolnik sostienen que la criptografía cuántica está aún en un estado embrionario y hasta dentro de 30 años no se verán sus primeras aplicaciones prácticas, que romperán con facilidad los actuales sistemas de cifrado. Mientras tanto, ha

empezado una carrera paralela para proteger la información que debería seguir siendo secreta cuando irrumpa la criptografía cuántica.

Hellman aseguró que está preocupado por si cae en malas manos. De momento, los investigadores trabajan en una de las pocas soluciones a su alcance: cifrar las cosas por duplicado, combinando criptografía simétrica y asimétrica, de forma que si la cuántica rompe la asimétrica, quede aún en pie la simétrica. El problema, dijo, es que "es muy caro, por lo que sólo puede usarse para información realmente valiosa".

El riesgo de que esta novedosa tecnología se use con fines perversos no es ninguna utopía, ya ha sucedido con los programas informáticos, como demostró Sergio de los Santos, consultor de seguridad de Hispasec Sistemas: "En el código malicioso hemos pasado del romanticismo al todo por la pasta, gente organizada que presta especial atención a atacar la banca en línea". Como ejemplo de su creciente poder, mostró fotos de una lujosa fiesta en Praga que reunió a algunos de estos nuevos criminales

MERCÈ MOLIST 17/01/2008

Computación cuantica: Aunque en la realidad no pasa de ser una formulación teórica con reducida demostraciones practicas, es posible que dentro de no muchos años se desarrolle un tipo de computadores basados en la dualidad de la materia y onda presente en la física cuantica, representara una drástica disminución en el volumen de los componentes y en el conocimiento de la velocidad de calculo.

Los ordenadores cuanticos procesan los datos codificados en formas de onda que son tratadas apoyándose en determinadas propiedades físicas de esta forma de energía de energía (se habla de q-bits, bits cuanticos) lo que permite diseñar algoritmos (criptografía cuantica) que pueda resolver en un tempo razonable problemas numéricos actualmente inabordables.

Seguridad en Redes Telemáticas
Justo Carracedo Gallardo
McGraw Hill, Madrid Marzo 2004

6. CASO PRÁCTICO

La mayoría de las empresas que se dedique a la venta de productos o servicios requieren del comercio electrónico y es por esto que al involucrarse en este proceso requieren métodos de seguridad que certifique y garanticen en envío y recepción de la información, así como de salvaguardar la información de nuestras bases de datos, ya que de lo contrario las perdidas monetarias y de información serán enormes.

En nuestro Pagina Web ofrecemos servicios y productos a través del comercio electrónico, los cuales son una forma practica y eficaz de llevar a cabo una venta, esto permitirá que los usuarios en la comodidad de su casa o trabajo puedan hacer compras por medio de tarjetas de crédito para ello necesitamos un servicio que nos garantice que esa transacción se va a llevar acabo en tiempo y forma y con seguridad para las dos partes, ya que en la actualidad hay muchas personas que buscan interceptar estos datos y a si robar la información de la tarjetas para después hacer robos o/y fraudes. Es por esto que hay empresas con mucha experiencia y renombre internacional que se dedican a realizar servicios de compra-venta las cuales están certificadas para realizar transacciones seguras, lo cual garantiza el envío y recepción de los datos y así poder llevar acabo el proceso de forma integra, esto da confianza y seguridad a los usuarios y a las empresas.
También necesitamos acciones de seguridad que nos permitan tener integra la información de nuestras bases de datos, es por esto que utilizamos técnicas de encriptación para poder accesar a nuestro sistema de usuarios y catálogos que manejamos evitando que hackers puedan burlar las claves y robar nuestra información.

Por seguridad generamos un sistema que nos permite encriptar la contraseña de los usuarios que registremos para accesar al sistema y puedan manejar la información cuando se requiera.

6.1 PAGINA WEB

6.1.1 DISEÑO

La forma en que los usuarios envían información confidencial a través del comercio electrónico utilizando la criptografía como medio. En nuestra pagina principal de pelucas y postizos, la cual se dedica a la venta de productos de cabello natural y sintéticos como son: pelucas, extensiones, chongos, donas en sus diferentes presentaciones, así como joyería de fantasía y otros productos para el cabello.

Fig. 44. Pagina Principal

En muestro menú principal tenemos los enlaces de los productos y servicios que ofrecemos, ubicación, historia, así como la opción de compras y comentarios de la pagina, además en la parte inferior de la pagina existe un enlace hacia nuestro sistema de administración de usuarios y productos la cual nos permite administrar nuestra información de nuestra pagina Web.

6.1.2 MENÚ DE PRODUCTOS. Muestra todos los productos que se manejan, en esta sección manejamos las extensiones de cabello, al dar clic sobre cualquier articulo nos desplegara la descripción de cada articulo, una vez que el cliente ha visto sus características y desea hacer una orden se podrá hacer en la opción carrito de compra, así como regresar al menú de los productos y seguir buscando mas artículos. De la misma forma funcionan los rubros de: Pelucas, Postizos, Extensiones, Bolsas, Accesorios para el cabello y la joyería de fantasía, de esta forma los clientes podrán buscar todos los productos de forma practica y rápida.

Menú Productos – Extensiones

Fig. 45 Pagina Productos

Al ingresar a los diferentes Menús, nos desplegara su contenido, en la opción productos proporciona un submenú de los diferentes artículos que la tienda oferta, así como algunas promociones que se estén manejando en ese momento, las diferentes opciones de productos y marcas, al seleccionarlo nos mostrara una descripción de sus características como son: nombre, color, medida.

6.1.3 MENÚ SERVICIOS.

Muestra una lista de los servicios que se ofrecen: tales como: colocación de extensiones de cabello, pestaña, unas y cortinas de extensiones, además algunas promociones de estos servicios. Una vez que seleccionamos alguno, nos da la descripción de cómo se coloca cada uno de los productos, así como las diferentes formas de aplicación, los colores y marcas que se manejan. En la opción contacto están los datos de la tienda para que el cliente realice sus citas.

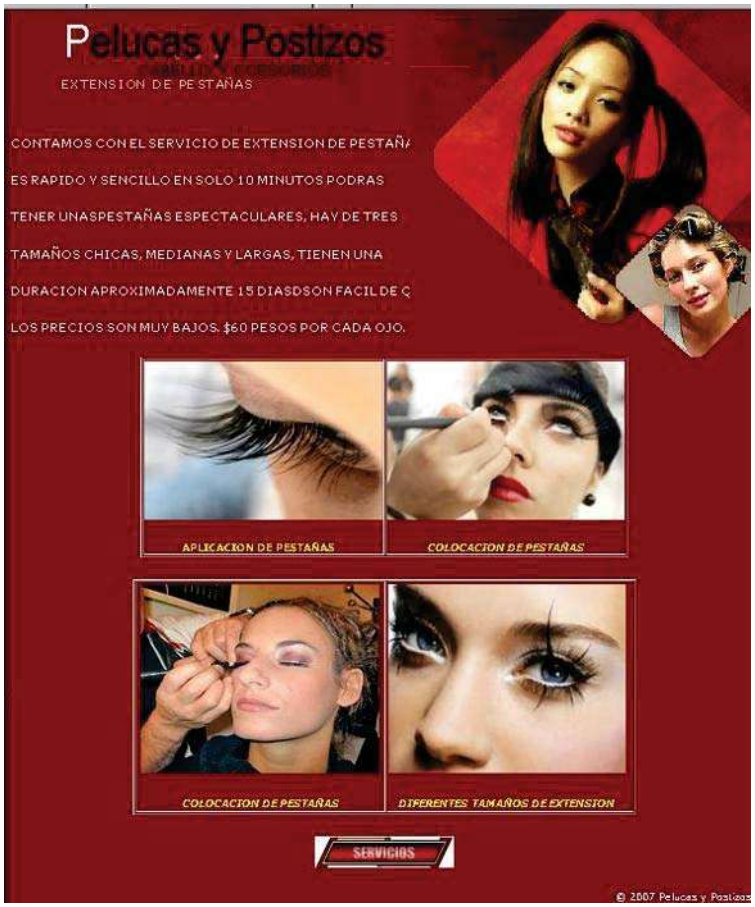


Fig. 46. Pagina Servicio

6.1.4 HISTORIA, UBICACIÓN Y CONTACTO.

Se describe la historia de la tienda, sus inicios y como se ha ido creciendo al incursionar en nuevos productos y servicios, utilizando marcas de primera calidad, detallamos la ubicación, los teléfonos para que los clientes puedan visitar el lugar así como solicitar información en general y las formas de compra que se ofrecen.

Fig. 47. Pagina Historia

6.1.5 EVALUACIÓN DE LA PÁGINA.

Nos permite saber que es lo que opinan nuestros cliente sobre nuestros productos y servicios es por esto que invitamos a todos ellos para que nos hagan una critica, algún comentario, que nos permita ir cambiando o agregando funciones, artículos o servicios, métodos de compra lo cual nos hará crecer y ser mas eficientes en lo que realizamos y lo mas importante que nuestros clientes estén conformes con los servicios y productos que ofrecemos.

Una vez llenado el formulario el cliente lo envía y se almacena la información en nuestra base de datos, ahí el administrador podrá ver el reporte que se haya hecho y analizar la retroalimentación que el cliente ha realizado sobre nuestros productos y servicios.

Fig. 48. Pagina Evaluación

6.1.6 COMPRAS (Opción Deposito Banco)

Tenemos opciones para nuestros clientes al hacer sus compras, en esta opción es a través de un deposito en el banco, nos envían información de los productos o servicios que necesiten, llenan el formulario con todos los datos que necesitamos, una vez que ellos nos envía la información se quedara registrada en nuestro sistema de información, se revisan los datos durante el día y verificamos cuantos pedidos existen, una vez revisado sus datos se genera su pedido, se comunican con el cliente y se le notifica la cantidad a depositar, al

momento de su deposito nos envían un fax con el deposito y se procede a enviar la mercancía.

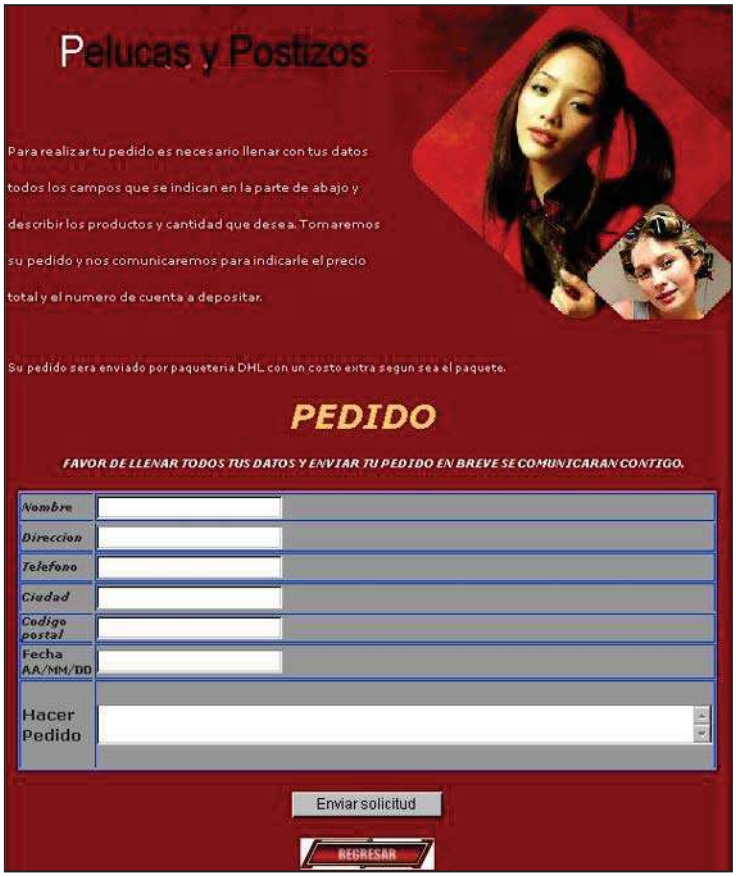


Fig. 49. Pagina Pedido

Menú Compra (Carrito de Compra)

En la pagina se puede comprar directamente agregando productos al carrito y poderlos pagar a través de las tarjetas de crédito, una vez que el cliente este navegando por las diferentes paginas podrá ir agregando artículos.

Al estar viendo la descripción de los artículos en la opción carrito-compras no enlaza al catalogo de los productos que estemos visualizando en ese momento.

Fig. 50. Opción Regresar Menús

Catalogo Productos

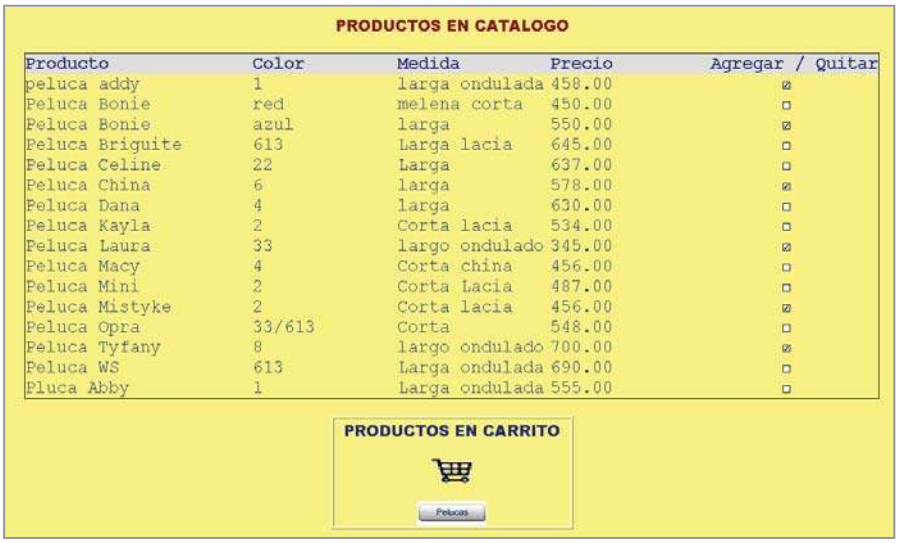


Fig. 51. Catalogo Productos

Al agregar productos al carrito nos muestra un catalogo de todos los Artículos de un determinado menú, despliega la lista de todas las existencia en ese momento con sus características a si como el precio, agregamos o quitamos dependiendo de lo que necesitemos comprar, si se desea agregar mas podemos regresar a los menú anteriores y poder seleccionar mas productos.

Una vez agregado varios de ellos, nos muestra todas las características de lo que se va a comprar como son: el nombre del producto, color, medida, precio

Fig. 52. Descripción Venta-Productos

Una vez seleccionados los productos se van contabilizando y nos muestran cuantos se han agregado para comprar, la cantidad de productos si es que se quiere comprar mas de uno, el total de la compra, tenemos la opción de borrar o actualizar para quitar algún articulo, o agregar unidades.

Fig. 53. Modificación de Unidades

Al determinar el total de los productos, las unidades y el precio total, seleccionamos pago con tarjeta, se llenara la información personal del cliente, para que se registre en nuestra base de datos y verificar la compra que esta haciendo así como realizar el envío de mercancía,

Seleccionamos siguiente para agregar los datos de las tarjetas o regresar si se requiere según sea el caso.

Fig. 54. Envío Información Venta-tarjeta

Se requiere contratar un servicio de Banamex u otra empresa que se dedique al sistema de pago por Internet, que nos permita hacer el cargo a nuestra cuenta, una vez realizado esto el cliente podrá seleccionar el tipo de tarjeta, se podrá seleccionar las tarjetas visa o mastercard, esta empresa utiliza un método criptográfico para las transacciones SSL[30]. Este método criptográfico es el mas usado y nos permitirá hacer una transacción segura.

Fig. 55 Pagina selección de tarjeta

Una vez seleccionado alguna opción se podrán ingresar los datos de los números de la tarjeta, los códigos de seguridad, la fecha de vencimiento, la empresa verificara los datos de la tarjeta y supervisara si son reales, de lo contrario no podrá seguir con el proceso de compra, los datos que el usuario envía son encriptadas a la bases de datos de la empresa, en nuestro caso Banamex, utilizando medios criptográficos de seguridad de primer nivel, ofreciendo confianza al cliente y a la empresa que en el momento de la compra-venta no intervendrán personas ajenas a esta transacción.

[30] **SSL:** Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA.

También es importante verificar algunos aspectos importantes en una transacción, por ejemplo el candado de nuestro navegador donde nos indica que certificado de autenticidad de la página, esto nos da la tranquilidad de que estamos navegando o interactuando en un sitio seguro y que podemos hacer operaciones sin riesgos.

Fig. 56 Introducción de datos confidenciales.

Este ejemplo mostrara como funciona el encriptada: ejemplo de la tarjeta anterior ponemos el número de tarjeta, fecha vencimiento y código de seguridad.

Tarjeta no. 1245 2564 9878 9856
Fecha vencimiento: 05 09
código de seguridad: 589

Al viajar esto en texto plano, es posible ver los datos tanto en tránsito como en el servidor de esta pagina Piensen que un hacker logró entrar al servidor y tiene acceso a toda esta información.

Ahora, si yo codifico este mismo texto usando un método criptográfico como el SSL:

-----BEGIN PGP MESSAGE-----
Version: SSL

hQIOA47ca7Y9fNCaEAf/XPeug0IY9cLLM/Zs0qXtncgJ6j2CLKSzFZn5dL32IVJY
EvdVYU+go8fjnV26Tn8Qc70V+8ObO3xf2+UBMDrPcn/Xmxj1n3q4K54Xce/OsZxL
FeCfv7mwV4yEhhHQPVtTIamXccphBT9ylmlS1iW8e7w4N3rJ87y6sdSZ2J7zT4wl
Hs4wX1b760Sh5C0NKAno2qnvtkJEbsjgljog3LxlK7sf9vHbMu2F9XcpetIolHvt
MAr8m/mQlxUBqIsRz5qcA0GrmHUrK0pJXTomDbSPgVxZa4frb0KH2gbxJnP9mvV4
sOasljNZhzsx6DRbPEaACOunyOlVblJiWPo+ljwAZgf6Ase86SOkRWhvasOXGiFD
qHDKdeF0n0cSzBWk/qUsiChNN8cyagVEq+zmHhessrD1gfiLssTXn3YNraipzBUC
HDUTDZsWpIT46aYVA58/l9GboYOcBRy8sNyyLc5c60GMoPDT/OXvHDi6VqqbyN5X
zM1PjQhCxeJrlsObGmeqoEUkfjdtjsv/V1AOwvMBET13A5PTeTAymD+Nt8umEbNQ
7kCrj3xo+OQdJm+vj3Q0u1I9m1oAg+rTG18EMou7q0G3NmBScPhHQgORp+6l05qk
xBIs59iB+L6z9HfTVi1FH2HoLXFLHOIlxFbPOind2aXNcKe7sZSvXM+MuHv5nEvG
OtKLAdIKsNOFA/kZu20YDkhJyaZBFp96sT/CeiI+oev8Phaspt7NZgz/VGnzpXYq
TIx9lR1jLqX3TnzYk/oojsh8aA6xUqwfMhfv5RWploeG/BGOuts3jinAkEkzL/FG
2Y1x6gOKt9vZ8uudELbQ5qTAIl6Wjy7Q+c73Eg83BDlpoda9d8UMDvDlDOf5FQ==
=9b8R
-----END MESSAGE-----

Esto es algo ilegible, es lo que vería un hacker en la red, con estos métodos todas las empresas que utilicen el comercio electrónico, realicen transacciones bancarias y demás movimientos en la red con información confidencial, se recomienda utilizar algún método criptográfico para asegurar que nuestros datos lleguen a su destinatario sin ser descubiertos por maliciosos expertos informáticos.

6. 2 SISTEMA DE INFORMACION

Una vez que tenemos nuestra página Web funcionando al mismo tiempo podemos administrar nuestra información de los usuarios y catálogos que utilizamos, en la página principal de la Web en la parte inferior hay un enlace:

Al dar clic nos enlazamos a la interfaz principal del sistema donde nos pide que nos identifiquemos para poder accesar, nombre y clave:

Fig. 57. Entrada al Sistema de Información

Es de importancia generar un password confiable que nos dará la tranquilidad de que nadie podrá accesar al sistema excepto el administrador u otros que tengan derechos para hacerlo, el sistema genera passwords encriptados de esta manera tenemos una protección mas segura y difícil de hackear.

6.2.1 MENÚ PRINCIPAL DEL SISTEMA

Una vez validado nuestro nombre y clave, ingresamos a la interfaz principal, ahí nos muestra un menú de usuarios, productos y reportes, donde podemos administrar nuestra información, ya sea agregar, eliminar, modificar, usuarios y productos así como generar los reportes necesarios para la empresa.

Fig.58. Menú Principal

El sistema nos permite fácil enlace a las diferentes interfaces, ya sea cerrar la sesión o regresar a la pagina Web dependiendo de las necesidades de cada usuarios, es flexible y fácil de ingresar a todos sus paginas. Una de las características importantes es que podemos accesar y administrar nuestra información desde cualquier parte del mundo, al tener una conexión a Internet el usuario ingresara con su clave y password, una vez dentro, podrá revisar pedidos, ventas, así como ingresar o eliminar productos de los catálogos, las acciones necesarias para tomar decisiones que le permitan ser eficientes y lograr los objetivos de la empresa.

6.2.2 ADMINISTRACION DE USUARIOS

En esta ventana podemos agregar, modificar, buscar, y eliminar usuarios dependiendo de las necesidades, manejamos dos tipo de usuarios: administrador tiene todos los privilegios para manipular la información, y el usuario que solo puede accesar a ciertas ventanas que el administrador o dueño de la empresa crea convenientes. De esta manera los usuarios solo puedan ver o manejar datos que se les autorice.

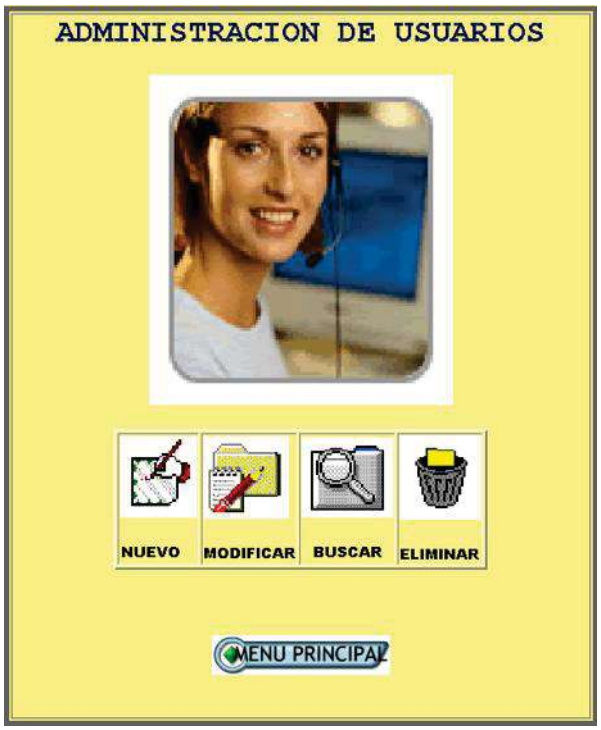


Fig. 59. Administración de Usuarios

Al oprimir en cada botón nos permitirá realizar diferentes acciones en la misma interfaz por ejemplo al dar clic en nuevo podremos llenar los siguientes campos: nombre, clave, password, dirección, perfil, sexo, Al seleccionar crear usuario, agregaremos un nuevo registro, lo importante de agregar un pasword es que el sistema genera una clave encriptada esto nos permite mayor seguridad, utilizamos sha1 y md5 que son algoritmos criptográficos seguros. De esta manera si el intruso obtiene los passwords, el texto no será plano si no una serie de caracteres encriptados que será imposible descifrar.

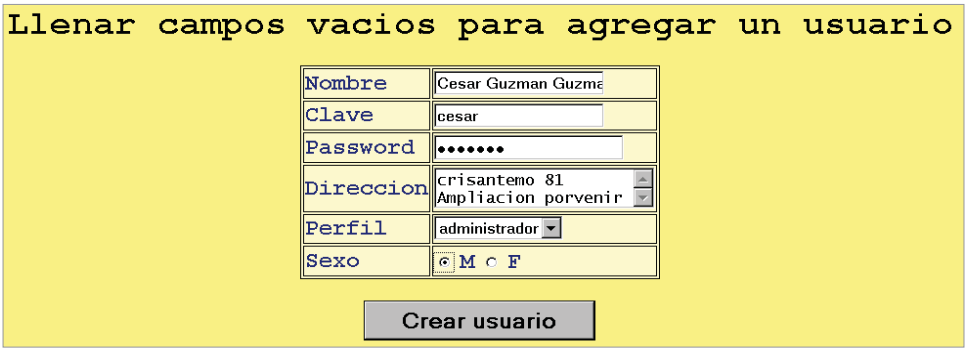


Fig. 60. Agregar un nuevo usuario

Permite modificar los registros agregados en la base de datos, solo seleccionamos modificar y buscamos el usuario, podremos cambiar información de cualquiera de sus campos.

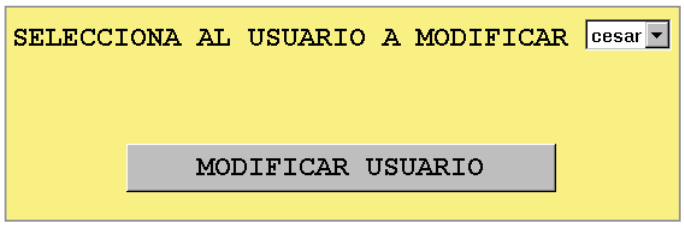


Fig. 61. Modificar usuarios

La opción buscar muestra todos los registros de los usuarios que tiene el sistema, hay dos opciones para buscar alguno de ellos, si se maneja mucha información, debemos utilizar formas para obtenla de una forma rápida, utilizamos buscar por nombre o por perfil.

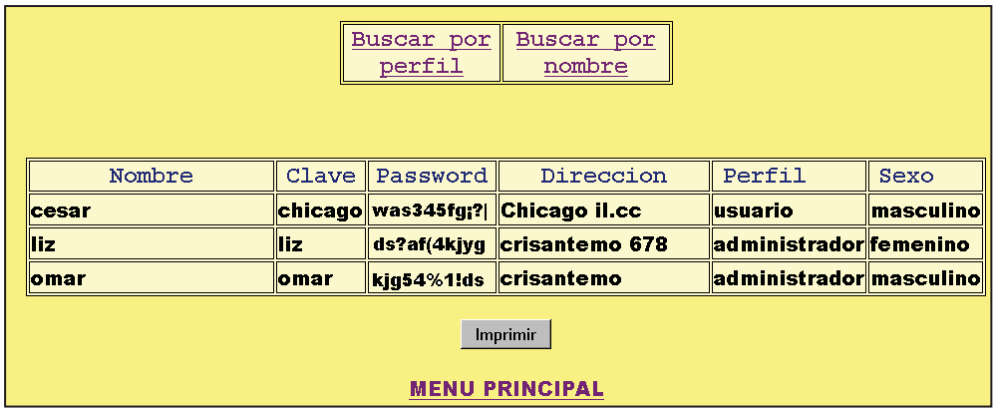


Fig. 62. Mostrar usuarios del sistema

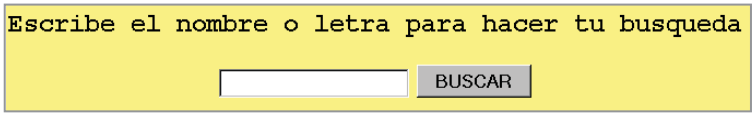


Fig. 63. Buscar usuarios por Nombre

A si mismo podemos eliminar algún registro de un usuario que ya nos se requiera, ubicamos el nombre del usuario, lo seleccionamos y se borra, utilizamos un mensaje de advertencia por seguridad para verificar si realmente se quiere eliminar dicho registro para siempre del sistema.

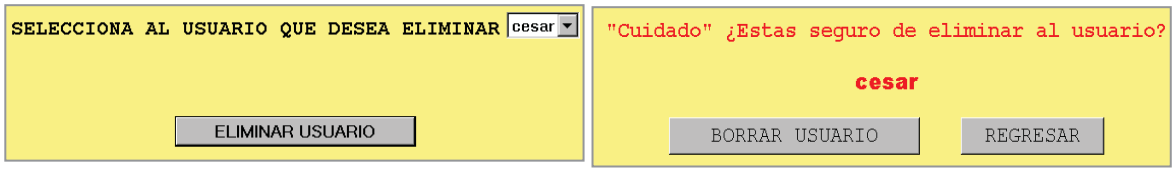


Fig. 64. Eliminar Usuarios

6.2.3 MENÚ CATALOGOS

Nos muestra los diferentes catálogos que la empresa maneja, a través de ellos podemos agregar, modificar, visualizar o eliminar registros de productos que se manejan, al seleccionar algunos de los ellos permitirá realizar cambios que se verán reflejadas en la pagina Web, cuando el cliente visualice los diferentes productos y al momento de hacer su compra podrá ver su existencia y variedad de ellos.

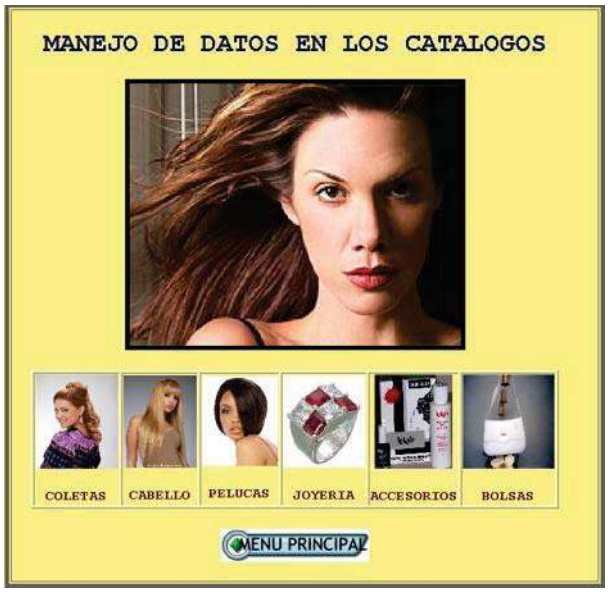


Fig. 65. Menú Principal Catálogos

Al seleccionar un catalogo, nos enviara a la ventana la cual mostrara los iconos con las diferentes opciones para ejecutar alguna acción que se requiera, de la misma forma se maneja y administra la información de los otros productos, además tendremos opción de regresar a los menús anteriores si se desea es muy practico y fácil de navegar.

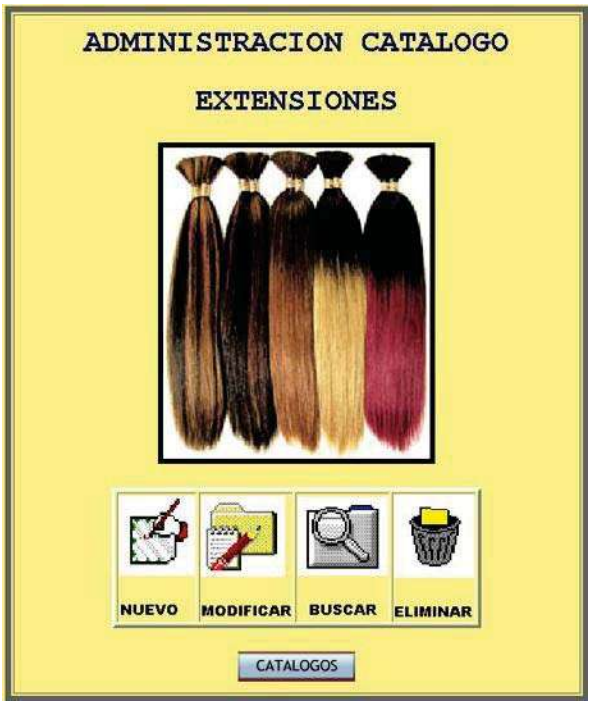


Fig. 66 Administración de Productos-Extensiones

La opción nuevo permite agregar un nuevo registro de algún producto, utilizamos los campos siguientes: id, producto, color, medida, precio, con estos campos describimos los productos que damos de alta en el catalogo.

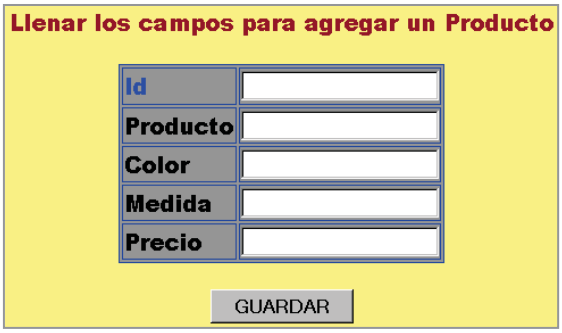


Fig. 67 Agregar un nuevo Producto

Si existiera algún error en los registros, podemos modificar cualquier campo en los diferentes catálogos, seleccionamos la opción modificar, buscamos el nombre del producto y lo modificamos.

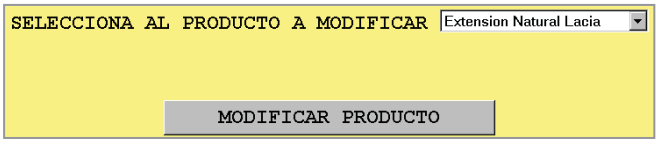


Fig. 68. Modificar un producto

Al manejar muchos dato es necesario tener una opción de búsqueda que nos permite verificar esa información, en todo los catálogos utilizamos una opción de búsqueda rápida por nombre de los productos que manejamos, esto dará mas rapidez a las consultas que se necesiten realizar.

Las extensiones encontradas son:

Buscar por nombre

Id	Nombre	Color	Medida	Precio
1	Extension Natural Lacia	1	18 Pulgadas	1200.00
2	Extension Natural Lacia	2	18 Pulgadas	1200.00
3	Extension Natural Lacia	1B	18 Pulgadas	1200.00
4	Extension Natural Lacia	4	18 Pulgadas	1200.00
5	Extension Natural Supreme	8	18 Pulgadas	1200.00
6	Extension Natural Supreme	16	18 Pulgadas	1200.00
7	Extension Natural Supreme	22	18 Pulgadas	1200.00
8	Extension Natural Supreme	613	18 Pulgadas	1300.00
9	Extension Natural Supreme	27	18 Pulgadas	1200.00
10	Extension Natural Supreme	1	20 Pulgadas	1400.00
11	Extension Natural Supreme	2	20 Pulgadas	1400.00
12	Extension Natural Lacia	4	20 Pulgadas	1400.00
13	Extension Natural Lacia	613	20 pulgadas	1400.00

Fig. 69 Mostrar todos los productos

Al dar clic en la opción buscar por nombre, nos muestra una ventana donde nos permite seleccionar algún nombre de los productos que hay en existencia y al ubicar uno de ellos nos mostrara toda la información de los registros encontrados.

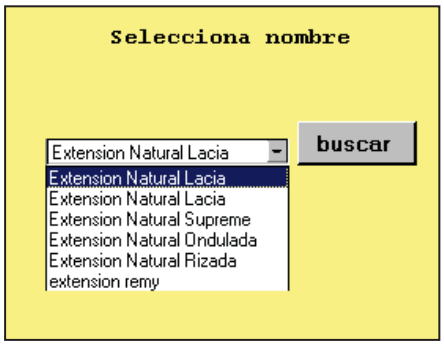


Fig. 70. Buscar Productos por Nombre

Se podrá eliminar algún registro que no se requiera en los diferentes catálogos, seleccionamos el nombre del registro y se borra.

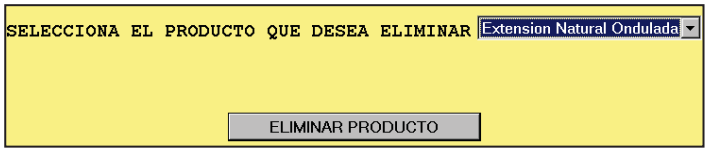


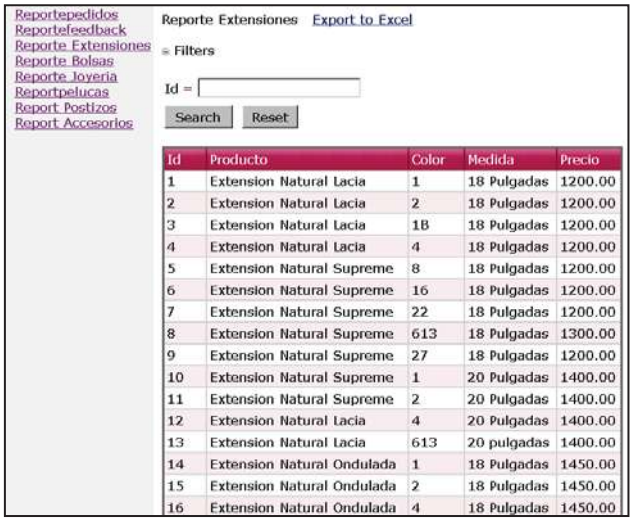
Fig. 71. Eliminar un producto

6.2.4 REPORTES

En esta sección se ubican todos los informes de nuestros productos, la lista de toda las existencia en los catálogos, así como los pedidos y ventas que se haya realizado en un periodo determinado, es importante tener al día nuestros informes ya que día a día se requiere enviar mercancía a los clientes, de esta manera se puede revisar la información recabada en el día.

Fig. 72. Menú Reportes

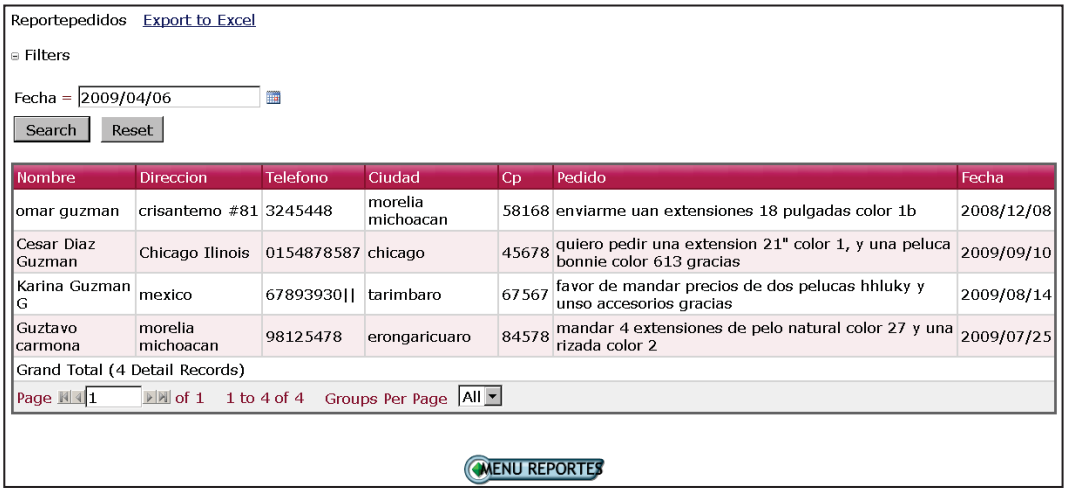
Al seleccionar cualquiera de los reportes nos enviara a una ventana donde nos mostrara la descripción de la información que hay almacenada en nuestra base de datos, de los productos, ventas, pedidos y comentarios que nuestros cliente han realizado.



Id	Producto	Color	Medida	Precio
1	Extension Natural Lacia	1	18 Pulgadas	1200.00
2	Extension Natural Lacia	2	18 Pulgadas	1200.00
3	Extension Natural Lacia	1B	18 Pulgadas	1200.00
4	Extension Natural Lacia	4	18 Pulgadas	1200.00
5	Extension Natural Supreme	8	18 Pulgadas	1200.00
6	Extension Natural Supreme	16	18 Pulgadas	1200.00
7	Extension Natural Supreme	22	18 Pulgadas	1200.00
8	Extension Natural Supreme	613	18 Pulgadas	1300.00
9	Extension Natural Supreme	27	18 Pulgadas	1200.00
10	Extension Natural Supreme	1	20 Pulgadas	1400.00
11	Extension Natural Supreme	2	20 Pulgadas	1400.00
12	Extension Natural Lacia	4	20 Pulgadas	1400.00
13	Extension Natural Lacia	613	20 pulgadas	1400.00
14	Extension Natural Ondulada	1	18 Pulgadas	1450.00
15	Extension Natural Ondulada	2	18 Pulgadas	1450.00
16	Extension Natural Ondulada	4	18 Pulgadas	1450.00

Fig. 72. 1 Reporte Productos

Nuestro sistema de reportes nos permite tener un menú donde instantáneamente podemos ubicar cualquier informe que sea requerido, permite utilizar filtros para ubicar información especifica por ejemplo por fechas y mostrara solo datos que se haya manejado ese determinado día, de esta forma podemos estar al tanto de las ventas, pedidos, entradas y salidas de la información en nuestro sistema.


Reportepedidos Export to Excel

Filters

Fecha = 2009/04/06

Search Reset

Nombre	Direccion	Telefono	Ciudad	Cp	Pedido	Fecha
omar guzman	crisantemo #81	3245448	morelia michoacan	58168	enviarme uan extensiones 18 pulgadas color 1b	2008/12/08
Cesar Diaz Guzman	Chicago Ilinois	0154878587	chicago	45678	quiero pedir una extension 21" color 1, y una peluca bonnie color 613 gracias	2009/09/10
Karina Guzman G	mexico	67893930||	tarimbaro	67567	favor de mandar precios de dos pelucas hhluky y unso accesorios gracias	2009/08/14
Guztavo carmona	morelia michoacan	98125478	erongaricuaro	84578	mandar 4 extensiones de pelo natural color 27 y una rizada color 2	2009/07/25

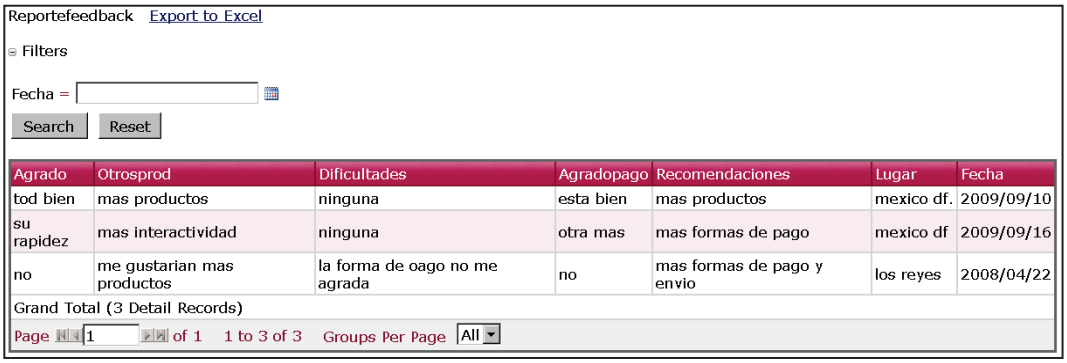
Grand Total (4 Detail Records)

Page 1 of 1 1 to 4 of 4 Groups Per Page All

MENU REPORTES

Fig. 72.2 Reporte Pedidos

Una de las características importantes que tiene nuestro sistema de reporte es que nos permite exportar información a Excel, una herramienta practica, que nos ayudara a poder generar mayor cantidad de filtros, graficas y de mas estadísticas que sean necesarias para el control de la información que manejamos.


Reportefeedback Export to Excel

Filters

Fecha =

Search Reset

Agrado	Otrosprod	Dificultades	Agradopago	Recomendaciones	Lugar	Fecha
tod bien	mas productos	ninguna	esta bien	mas productos	mexico df.	2009/09/10
su rapidez	mas interactividad	ninguna	otra mas	mas formas de pago	mexico df	2009/09/16
no	me gustarian mas productos	la forma de oago no me agrada	no	mas formas de pago y envio	los reyes	2008/04/22

Grand Total (3 Detail Records)

Page 1 of 1 1 to 3 of 3 Groups Per Page All

Fig. 73.3. Reporte Feed-back.

CONCLUSIONES

A través de este trabajo de investigación me he dado cuenta la importancia que tiene la información para las empresas, cuales has sido las ventajas y desventajas de ingresar al mundo del Internet, nos damos cuenta que cada día que pasa existen mas personas maliciosas tratando de apoderarse de la información que manejan las empresas y los usuarios, datos valiosos como: cuentas de bancos, contraseñas, información confidencial entre muchas mas con la finalidad de robar dinero y hacer mal uso de ellos.

Es sorprendente las cifras de robo de información, de distintas formas, en el mundo por parte de los expertos informáticos (hackers) que solo piensan en la manera fácil de obtener beneficios.

Es por eso que todos en general que hacemos uso de los servicios de Internet debemos realizar ciertas acciones para que no seamos blanco de extorsiones o robo de información, ya que en la red esta plagada de mucho malware que buscan la manera de cometer su acto ilícito.

Pero a nivel empresarial nos damos cuenta que deben estar al día con todos los métodos de seguridad para que para sus sistemas de información estén a salvo de los cibercriminales que día a día buscan nuevas alternativas para hacer fraudes.

Las empresas optan por utilizar métodos a través de la criptografía los cuales les permitan realizar envíos y recepción de información de forma segura con la seguridad de que si cae en manos de malas personas no pueda ser descubierto el mensaje original.

GLOSARIO

Sistemas: Un sistema de información (SI) es un conjunto organizado de elementos, estos elementos son de 4 tipos: Personas, Datos, Actividades o técnicas de trabajo, Recursos materiales en general, Todo ese conjunto de elementos interactúan entre si para procesar los datos y la información

Auditabilidad: La facilidad con que un sistema de información puede ser examinado y verificado

wíreless: USB es un protocolo de comunicación inalámbrica por radio con gran ancho de banda que combina la sencillez de uso de USB con la versatilidad de las redes inalámbricas.

LAN: Una red de área local, red local o LAN (del inglés Local Area Network) es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de hasta 200 metros.

10Base5: es un estandar para la conexión de una red utiliza cable coaxial grueso utiliza la topologia de bus.

10Base2: es un estandar para la conexión de una red, utiliza cable coaxial delgado y es mas sencilla de instalar.

Red informática: es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

Ethernet: Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de *ether*.

Fast Ethernet: Fast Ethernet o Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps.

Gigabit Ethernet: Es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

Gigabits: Un gigabit es una unidad de medida de almacenamiento informático normalmente abreviada como Gb o a veces Gbit, que equivale a 10^9 bits.

TICs: son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno.

PYMES: pequeñas y medianas empresas.

Spam: Se llama *spam*, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario.

Home banking: servicio del banco a través de la red.

Malware: es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades maliciosas.

Virus: es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Spyware: Los programas espías o spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. Hackers utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática.

Internet: Es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Sitio: es un conjunto de páginas web, típicamente comunes a un dominio de Internet o subdominio en la World Wide Web en Internet.

WWW: Red Global Mundial es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet

Ofuscación: Técnica que consiste en dificultar la lectura del texto.

URL: significa *Uniform Resource Locator*, es decir, localizador uniforme de recurso.

Direccion IP: Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

Pagina Web. también conocida como página de Internet, es una fuente de información adaptada para la World Wide Web (WWW) Las páginas web pueden consistir en archivos de texto estático, o se pueden leer una serie de archivos con código que instruya al servidor cómo construir el HTML

DNS. Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Virus: Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

Host: Aquel dispositivo de la red que ofrece servicios a otros ordenadores conectados a dicha red.

HTTPS: Protocolo seguro de transferencia de hipertexto (Hypertext Transfer Protocol Secure). Protocolo de comunicación que permite la transferencia de información de manera segura.

Criptologia: Es el estudio de los criptosistemas: sistemas que ofrecen medios seguros de comunicación en los que el emisor oculta o cifra el mensaje antes de transmitirlo para que sólo un receptor autorizado (o nadie) pueda descifrarlo.

Protocolo: conjunto de estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

SSL: El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation. Se encuentra en la pila OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA.

Algoritmo criptográfico: De forma similar a cualquier otro algoritmo computacional, consiste en un conjunto de reglas que definen de forma precisa y no ambigua una secuencia de operaciones y transformaciones de los datos tal que dicha secuencia termine en un tiempo finito, un algoritmo debe contemplar la operación de cifrado y la operación de descifrar.

Criptoanálisis: Arte y ciencia de romper mensajes cifrados, descubriendo la clave, el mensaje en claro o ambos.

Criptologia: Rama de las matemáticas que abarca la criptografía y criptoanálisis. Por lo general, se usa el término criptografía con esta misma aceptación o sistema que sirve para cifrar.

Criptógrafo: Persona que se dedica al estudio y practica de la criptografía, se usa también para denominar a una maquina o sistema que sirve para cifrar.

Criptoanalista: Persona que se dedica al criptoanálisis.

Mensaje en claro: Mensaje o documento original que va hacer sujeto de cifrado.

Mensaje cifrado (criptograma): Mensaje o documento cifrado.

Cifrado, cifrar: Operación de transformación de un mensaje en claro en un mensaje cifrado.

Descifrado, descifrar: Operación de transformación de un mensaje cifrado en un mensaje claro.

Criptosistema: Un criptosistema utiliza un algoritmo criptografico para cifrar y descifrar los mensajes, se trata por tanto, de un sistema que implementa un algoritmo.

Encriptada, encriptar: Equivale a cifrar.

Desencriptado, desencriptar: Equivale a descifrar.

Codificar, descodificar (decodificar): Podría entenderse como una técnica de cifrado por medio de códigos

Fuerza bruta: Tecnica que consiste en intentos reiterados de accesar por medio de los controles de acceso legitimos, buscando algún password debil.

MDC: (Message Detection Code, Código de detección de mensajes) se emplean para asegurar la integridad de los datos.

URL: (Localizador de Recurso Uniforme) El URL de una pagina comienza con http (protocolo de trasferencia de híper texto y contiene el nombre de la computadora, nombre del directorio y nombre de la pagina. http://www.whitehouse.gov/wh/servicios

Protocolo TCP/IP: es el que se encarga de garantizarla comunicación fiable entre equipos y para cada uno de los servicios proporcionados por Internet, se ha desarrollado un protocolo especifico: http para el world wide Web, https para el World wide Web seguro, smtp para el correo Electronic, nntppara el acceso a grupos de noticias (news).

Hostear: El término Host, es usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red. En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc.

BIBLIOGRAFIA

PAGINAS WEB

- Que es la Información, Recuperado el 14/09/2008 en http://www.avizora.com/publicaciones/comunicacion/textos/0109_que_es_informacion.htm
- Formas de Comunicación. Recuperado el 14/09/2008 en http://www.agmediatica.com/index.php?area=1&p=static&page=formas_de_comunicacion
- Julio Cesar Casares, Que es una Idea, Recuperado el 20/09/2008 en http://web.jet.es/amozarrain/que_es_una_idea.htm
- Prusak y Davenport, Dato, Información, Conocimiento, Recuperado el 20/09/2008 en Http://www.gestiondelconocimiento.com/conceptos_diferenciaentredato.htm
- GA. Miller Procesamiento de la Información. Recuperado el 25/09/2008 en http://www.terra.es/personal3/tmc000/inv/suite.html.
- José Camilo Daccach T. Características de la Información Recuperado el 25/09/2008 en http://www.gestiopolis.com/delta/prof/PRO197.html
- Sergio Alejandro Martínez De La Cruz, Importancia de los sistemas de información para las pequeñas empresas, (11-2005) Pequeñas y medianas empresas, PyME Recuperado el 01/10/2008 en http://www.gestiopolis.com/canales5/emp/imposiste.htm
- Manuel Peralta, Sistemas de Información, Recuperado el 01/10/2008 en http://www.monografias.com/trabajos7/sisinf/sisinf.shtml
- Marcelo Gimenez, (Viernes 5 de Septiembre de 2008) La Importancia de la Seguridad en las Empresas Recuperado el 05/09/2008 en http://www.lasegunda.com/ediciononline/ciencia_tecnologia/detalle/index.asp?idnoticia=432018
- Tipos de Sistemas de Informacion, Recuperado el 6/10/2008 en http://tecnomaestros.awardspace.com/tipos_sistemas.php
- Sergio Etcheverry G., (03-06-2005) Clasificación de los Sistemas de Información, Recuperado el 6/10/2008 en http://www.unap.cl/~setcheve/siiqq/Page32.html
- Proceso del Manejo de Información, Recuperado el 10/10/2008 en http://iteso.mx/~ogla/manejoinf.htm
- Gómez, A.- Suárez, C., (01/2006), Sistemas de Información, Recuperado el 10/10/2008 de http://www.agapea.com/libros/Sistemas-de-Informacion-Herramientas-practicas-para-la-gestión-empresarial-2-Edicion-isbn-8478976833-i.htm
- Álvaro Domínguez (11/09/2001) Importancia de la Seguridad en las empresas, Recuperado el 27/10/2008 en http://www.transmedia.cl/noticia23=id190108.htm
- Métodos mas habituales para robar (03/2007), Recuperado el 27/10/2008 en http://www.cavaju.net/2007/03/los-mtodos-ms-habituales-para-robar.html
- La Jornada. (08/06/2007) Seguridad de los Usuarios en Internet, Recuperado 27/10/2008 en http://www.e-aprendizaje.gob.mx/wb2/eMex/eMex_24550_not859_plantea_la_un 27
- Rubén Aquino Luna, Gustavo Alberto Gutiérrez Ramí, (Noviembre de 2008), Crimen en línea Recuperado el 07/11/2008 en http://www.enterate.unam.mx/artic/2007/septiem/art4.html de

- Jorge Mieres, Cristian Borghello (junio 2008), Robo de información personal online Recuperado el 07/11/2008 http://www.eset-la.com/press/informe/robo_informacion_online.pdf.
- Seguridad Informática, Recuperado el 08/11/2008 en http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- 3 Stuart McClure, Historia de la Criptografia, Recuperado el 22/11/2008 en http://www.24flotilla.com/A11/otros/Historia%2520Criptografia.pdf
- Criptografia, Recuperado el 22/11/2008 en http://www.uv.es/~montanan/redes/trabajos/
- Encriptacion, Recuperado el 12/12/2008 en http://aplicaciones.virtual.unal.edu.co/drupal/files/criptologia.pdf
- Mercè Molist (17/01/2008) El desarrollo de la criptografía cuantica. Recuperado el 12/12/2008 en http://www.elpais.com/articulo/red/desarrollo/criptografia/cuantica/descifrara/todas/claves/actual/es/elpeputeccib/20080117elpcibenr_3/Tes
- Red Informática, Recuperado el 13/01/2009 en http://www.terra.es/personal/lermon/cat/articles/evin0405.htm
- Gonzalo Álvarez Marañón , CSIC (1998) Secure Socket Layer, Recuperado el 19/01/2009 en http://www.iec.csic.es/CRIPTonOMICon/ssl.html
- Marcelo Héctor González, CISA, ASS, (6,2000), Comercio Electrónico Recuperado el 20/05/209 en http://www.isaca.org/Template.cfm? Section=Home&CONTENTID =16658& TEMPLATE=/ContentManagement/ContentDisplay.cfm.
- Seguridad en Tics, Recuperado el 08/06/2009 en http://revista.seguridad.unam.mx
- Seguridad en Internet, Portal seguridad en Internet / Sistema Nacional e-Méxic, Recuperado el 08/06/2009 en http://www.e-mexico.gob.mx/wb2/eMex/eMex_Seguridad_en_Internet
- México a la cabeza en Malware, Recuperado el 10/06/2009 en http://www.comtodo.com/index.php?option=com_content&view=article&id=136:mexico-a-la-cabeza-en-malware&catid=53:noticias-&Itemid=128
- (11/02/2008) México Seria Fuente de Malware, Recuperado el 10/06/2009 en http://www.infomarket.com.mx/newsItem.asp?ID=454
- Aumentan Fraudes electrónicos. Recuperado el 11/06/2009 en http://www.radiotrece.com.mx/2008/09/26/aumentan-fraudes-electronicos
- Reguridad Informatica, Recuperado el 16/06/2009 en http://revista.seguridad.unam.mx/rs_unam_04/index.html
- Set, Recuperado el 12/06/2009 en www.iec.csic.es/set.
- Aplicaciones Cliente-servidor ASAyC Recuperado el 20/07/2009 en http://www.asayc.com/administracion/cliente.htm
- Modelo Cliente-Servidor , Recuperado el 25/08/2009 en http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/cliente-servidor.html
- Villalobos, Encriptación Md5 en Php, Recuperado el 14/09/2009 en http://php.ciberaula.com/articulo/encriptacion_md5_php/

LIBROS

Justo Carracedo Gallardo. (Marzo 2004)
Seguridad en Redes Telemáticas
Madrid: McGraw Hill

McGraw Hill. (2004)
Redes de Computadoras
Austin Community College: Ed. Tittel

William Stallings (2000)
Comunicaciones y Redes de Computadores
6ta edición. Ed. Prentice Hall

Kelleigh Wing, Paul Whitehead, Ruth Maran (2001)
Aprenda Internet y la World Wide Web
2da Edición
From MaranGraphics
ST Editorial Inc.

Alvaro Gomez Vieites, Carlos Suarez Rey (2004)
Sistemas de Información
Herramienta practica para la gestión empresarial
Alfaomega Grupo editor Ra-ma