

UNIVERSIDAD NACIONAL DEL NORDESTE

**FACULTAD DE CIENCIAS EXACTAS Y
NATURALES Y AGRIMENSURA**



Seguridad



Informática y Criptografía



¿Por que la Seguridad?.

Internet.

Comercio Electrónico.

Definición de Seguridad.

Pilares fundamentales de la Seguridad.

Factores que atacan a la Seguridad.

Seguridad Física y Seguridad Lógica.

Estrategias de Seguridad.

Criptografía.



Por que la seguridad?

La masiva utilización de las computadoras y redes como medios para *almacenar, transferir* y *procesar* información se ha incrementado en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual.*

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar.*

INTERNET



* Son abiertas y accesibles

* Permiten intercambios rápidos y eficientes a nivel mundial y a bajo costo.

Este concepto hace posible nuevas formas de funcionamiento de la sociedad actual que se ve dificultada por las inseguridades que van dejando al descubierto.

Por ejemplo:

- Los mensajes pueden ser Interceptados y manipulados.
- NO se puede garantizar la identidad de los participantes de una comunicación.
- NO se puede garantizar la integridad de los datos transmitidos.
- Los datos personales pueden ser ilegalmente almacenados,
- Etc.





Datos Interesantes

Internet ha pasado de tener miles de usuarios en 1983 a más de 800 millones de usuarios en el mundo en el 2004 y 1000 millones en el 2005.

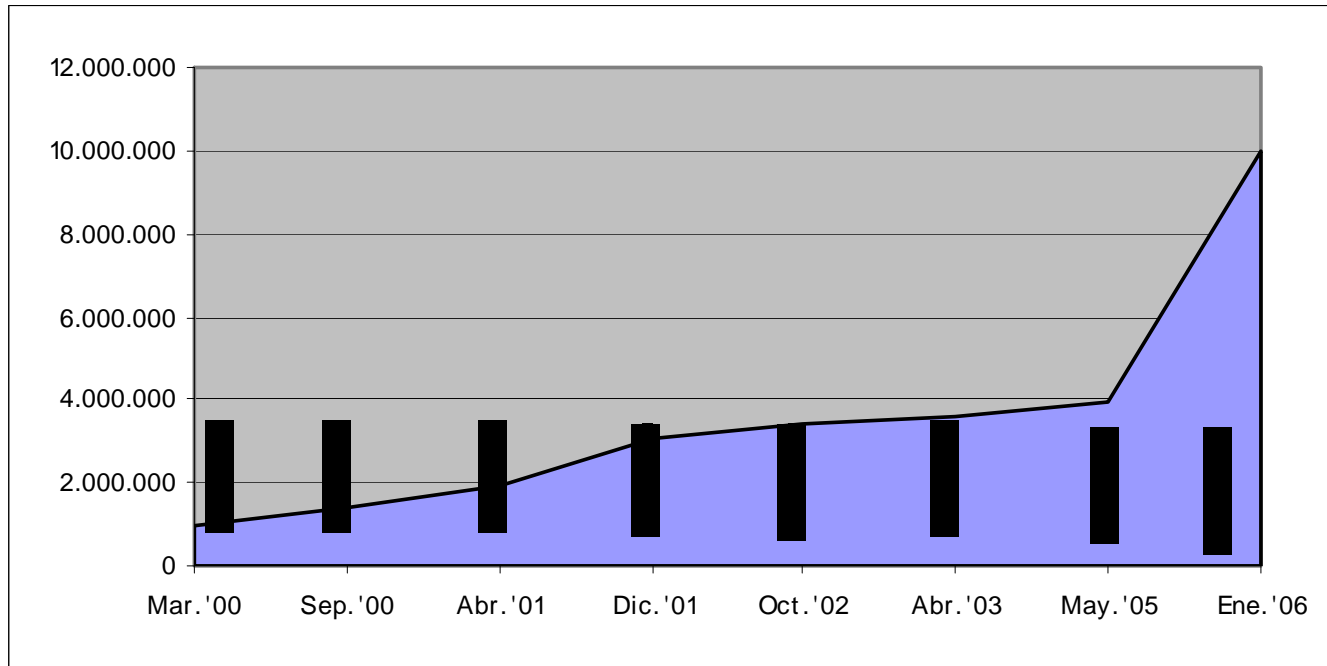
PROGRESION DE USUARIOS EN EL MUNDO	
AÑO	Nº Usuarios
1990	0,7-1 millón
2000	300-400 millones
2002	400-500 millones
2003	500-600 millones
2004	800 millones
2005	1.000 millones

Fuente: Angus Reid Group



- De acuerdo a un estudio realizado por una consultora, Internet fue uno de los indicadores que continuó creciendo durante la crisis en Argentina durante el 2002.
- Si bien la tasa de crecimiento fue menor que en tiempos anteriores, en el año 2005, la cantidad de Usuarios de Internet en el país llegó a los 3.900.000 (10% población).
- Mientras que hoy hay mas de 10 millones de usuarios, lo que representa aproximadamente, el 26% de la población.

Cantidad de usuarios de Internet en Argentina



Fuente: D'Alessio IROL Tracking sobre penetración de Internet 2003



Ventajas

Constituye un canal virtual vital para realizar negocios con los clientes actuales y futuros.

Desventajas

Internet representa riesgos de seguridad importantes que las empresas ignoran o subestiman.



Comercio electrónico


En el pasado, la posibilidad de conectarse con millones de clientes las 24 horas al día, los 7 días de la semana, era solamente posible para las grandes corporaciones.

Ahora, incluso una compañía con recursos limitados puede competir con rivales más grandes ofreciendo productos y servicios por Internet con una inversión modesta.




Los servicios de comercio electrónico son muy llamativos para:

- **Los consumidores** que no quieren pasar su tiempo libre limitado en los almacenes minoristas tradicionales,
- Sentirse restringidos por el horario normal de atención al público o,
- Hacer largas filas para pagar en la caja.




Los clientes no solamente compran fácilmente sus productos, sino que las compañías también han innovado el uso de conceptos como **“personalización”** para crear relaciones exclusivas e individuales con los clientes.

Las compañías que utilizan la personalización pueden identificar a sus clientes virtuales por el **nombre**, ofrecerles productos basados en **hábitos de compra previos** y almacenar de manera segura la información de la dirección del domicilio para agilizar las compras en línea.



Surgen nuevos desafíos que las empresas deben superar para tener éxito:

“Deben ofrecer servicios fáciles de utilizar y totalmente seguros porque guardan información confidencial como **direcciones** o **números de las tarjetas de crédito personales**”.



El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción ***a conductas antisociales y delictivas*** manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de ***cometer delitos tradicionales en formas no tradicionales.***



El Papel del Gobierno

Por su parte, los gobiernos han comenzado a crear reglamentaciones diseñadas para garantizar que las empresas implementen suficientes controles de seguridad.

Están muy interesados en conocer la forma en la que las empresas protegen su información e infraestructura.

En Estados Unidos, este interés se ha traducido en las recientes legislaciones **Sarbanes-Oxley**, HIPAA y GLBA . *






Definición Formal:

Se entiende por seguridad de los sistemas de información al conjunto de recursos:

- **metodologías,**
- **planes,**
- **políticas,**
- **documentos,**
- **programas ó dispositivos físicos,**
encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.



La Seguridad
Informática debe
vigilar
principalmente por
las siguientes
propiedades:

- *Confidencialidad*
- *Integridad*
- *Control*
- *Disponibilidad*
- *Autenticación*



Confidencialidad:

“Condición que asegura que la información no puede estar disponible por o para personas o entidades no autorizadas”.



Integridad:

“Condición que garantiza que la información es modificada, incluyendo creación y borrado por el personal autorizado”. (saldos en un sistema bancario).



Control:

“Permite asegurar que sólo los usuarios autorizados puedan decidir cuando y como permitir el acceso a la misma”.



Disponibilidad:

“Grado en el que un dato esta en el lugar, momento y forma en el que es requerido por el usuario autorizado”.



Autenticación:

“Mecanismo que permite conocer si la persona que esta accediendo es realmente quien debe ser y no un extraño”.



Amenazas para la seguridad





Para tener en cuenta:

- Se sabe que los empleados internos que tienen acceso a los sistemas, causan el 80% del total de violaciones a la seguridad.
- La gran mayoría de los problemas internos no son maliciosos, sino que son causados por errores de buena fe.
- Es importante que las empresas establezcan políticas de seguridad y programas para la toma de conciencia sobre la seguridad con el fin de educar a los empleados.



Las amenazas pueden ser analizadas en tres momentos:

- La prevención (antes)
- La detección (durante)
- La recuperación (después)





Prevención:

“Mecanismos que aumentan la seguridad o fiabilidad del sistema durante su funcionamiento normal”.(encriptar)

Detección:

“Mecanismos orientados a revelar violaciones a la seguridad”. (firewall)

Recuperación:

“Mecanismos que se aplican cuando la violación de un sistema ya se ha detectado”.(backup)

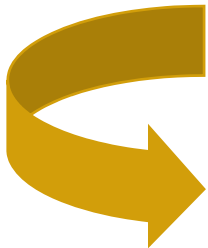


Seguridad Física:

“Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos o información confidencial”.

Seguridad Lógica:

“Aplicación de barreras y procedimientos que resguarden el acceso a los datos y accedan a ellos sólo personas autorizadas”.



“Todo lo que no está permitido debe estar prohibido”.


Estrategias de seguridad

1) Crear una política global de seguridad.

2) Realizar un análisis de riesgo.

3) Aplicar las medidas correspondientes de seguridad.





Los programas de seguridad de la información no son para implementar y luego dejar en “**piloto automático**”.

Se debe revisar objetivamente el estado del programa de seguridad empresarial cada **6** ó **12** meses.

En especial, se debe hacer una evaluación inicial de su situación actual, que incluya analizar cuidadosamente los componentes.



La evaluación inicial revisa las partes vitales del programa de seguridad: **personal, procesos y tecnología.**

El resultado de la evaluación señalará, las deficiencias y establecerán las recomendaciones sobre cómo puede mejorar la efectividad general del programa de seguridad.



1. **El personal:** Certificaciones y educación continuada.

El campo de la tecnología de la información en general y de la seguridad de la información **cambia** rápidamente.

Muchas cosas pueden suceder en el mundo de la seguridad de la información en el transcurso de un **año** incluso en **seis meses**.



Por ello nos deberíamos hacer la siguiente pregunta:

¿Conoce el personal de seguridad los temas de seguridad más recientes, tales como la prevención de intrusos, las nuevas tendencias en seguridad de las aplicaciones y la importancia de solucionar las vulnerabilidades inmediatamente?

Así como las amenazas a la seguridad y la tecnología **nunca** se detienen, la curva de aprendizaje de los empleados tampoco debe estancarse.



Por ejemplo, se debe promover la formación en seguridad para actualizar el conocimiento en el sector, lo cual podría hacerse:

- Ofreciendo entrenamiento al personal,
- Asistiendo a conferencias o a certificaciones fuera de la empresa,
- Trayendo al lugar de trabajo educadores de seguridad externos,
- etc.



Es importante que los miembros clave de su equipo tengan certificaciones en seguridad no sólo porque éstas reflejan comprensión y conocimiento práctico de los problemas de seguridad, sino también porque la mayoría de certificaciones exige cursos de educación continuada para conservar la certificación.

Esto garantiza que el personal certificado refresca de manera activa sus conocimientos para que esté actualizado sobre las últimas amenazas, tecnología y mejores prácticas de seguridad.



Certificaciones más conocidas

Certified Information Systems Security Professionals (CISSP).

Certified Information Security Manager (CISM)

Certified Information Systems Auditor (CISA).

SANS Global Information Assurance Certifications (GIAC)



2. La tecnología: Auditoría independiente y pruebas de penetración.

Siempre es recomendable que un auditor externo realice anualmente un análisis independiente de su programa de seguridad.

Los resultados mostrarán de manera precisa y objetiva cómo está el programa de seguridad.

Como parte del análisis, el auditor podrá evaluar los procesos de seguridad que el equipo ha implementado, como la administración de cuentas y la tecnología adoptada como la configuración de los firewalls.



Pruebas de Penetracion

Otra forma importante de evaluar la efectividad de la tecnología de la seguridad es realizar una ***prueba de penetración***.

En estas pruebas, un consultor de seguridad independiente se dispone a "ciegas" a averiguar todo sobre sus sistemas y procede a utilizar esa información en su contra para intentar penetrarlos.

El consultor no recibe ninguna información detallada sobre la infraestructura de su red de manera que confía en la información pública para ver hasta donde puede llegar.



Los resultados señalarán las zonas donde existe peligro y le ayudarán al equipo a saber cómo configurar la tecnología adecuada donde antes no existía.

Los análisis independientes y las pruebas de penetración son dos formas muy efectivas de identificar las zonas de alto riesgo y los puntos débiles antes de que sean aprovechados, lo que le permite a su equipo prevenir y hacer ajustes a la tecnología y a las normas de seguridad.




3. El proceso: Revise las políticas de seguridad y toma de conciencia

- Finalmente, se recomienda que realice un análisis periódico de sus políticas de seguridad y de los procesos que ha implementado para educar a los empleados y establecer los parámetros.
- Revisión y actualizaciones de la política de seguridad rutinaria: ¿Cuándo fue la última vez que evaluó las políticas de seguridad adoptadas para garantizar que aún son relevantes y que están actualizadas?



- Si no se han revisado sus políticas hace más de un año, ahora es el momento de hacerlo.
- Las políticas de seguridad nunca deben considerarse estáticas.
- Se recomienda realizar una revisión anual de todas las políticas - incluyendo la administración de cuentas, el acceso remoto, control de vulnerabilidades y respuesta a incidentes.
- En la medida que cambian los entornos operativos, los planes comerciales, las reglamentaciones y la economía de su empresa, y que surgen nuevas amenazas a la seguridad y nueva tecnología, se deben actualizar las políticas para reflejar estos cambios.

- 
- Se debe pensar en la cobertura de las políticas que existen actualmente.
 - *¿Son completas?*
 - ¿Es efectivo su programa de toma de conciencia sobre la seguridad?
 - ¿Qué conocimiento tienen los empleados de su empresa sobre las políticas de seguridad que su equipo ha implementado?
 - ¿Son conscientes de la importancia de la seguridad de la información?



- ¿Saben a quién recurrir si encuentran algo sospechoso en el equipo?
- ¿Para qué sirve tener políticas de seguridad si los empleados no las conocen?.
- Es necesario que se cumplan las políticas a nivel empresarial para que sean efectivas, aunque no se cumplirán a menos que su equipo de seguridad inicie y desarrolle una campaña de toma de conciencia de la seguridad en la empresa.
- Una revisión anual de las políticas reducirá el nivel de riesgo y evitará que su empresa se exponga innecesariamente.

Criptografía

- Para subsanar problemas relativos a la seguridad, surgieron distintos métodos o estrategias, siendo uno de los más antiguos pero actualmente utilizados: la criptografía.
- Proviene del griego ***kryptos*** (esconder) y ***gráphein*** (escribir), es decir “Escritura escondida”



Métodos Antiguos

- Uno de los algoritmos antiguos tuvo su origen durante el Imperio Romano, en la época de Julio César.
- César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales.



Por ejemplo:

A



M

B



N

C

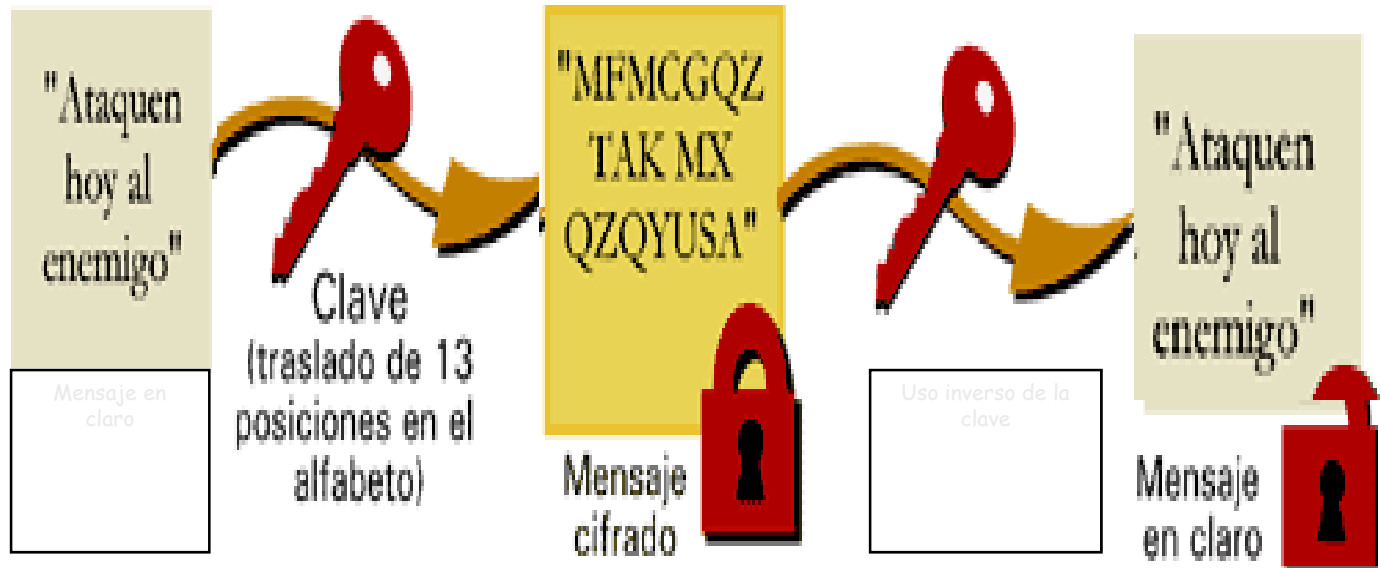


O

13

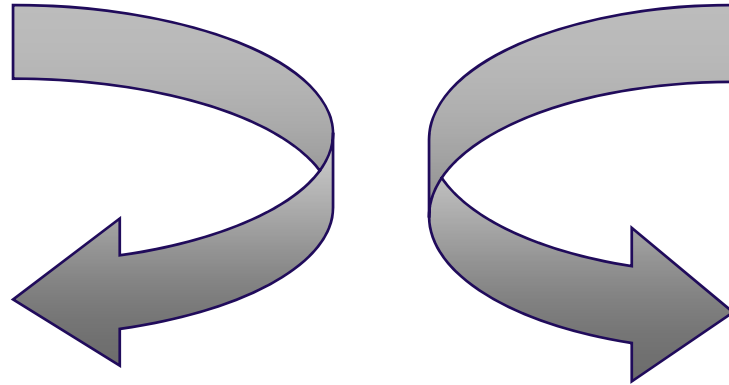


El método de cifrado introducido por Julio César introduce el concepto de "clave criptográfica".



Básicamente la criptografía se divide en dos ramas:

CRIPTOGRAFIA:

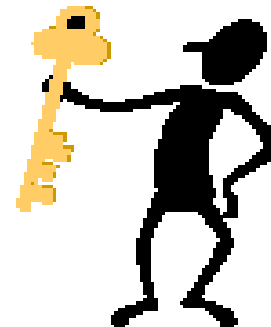
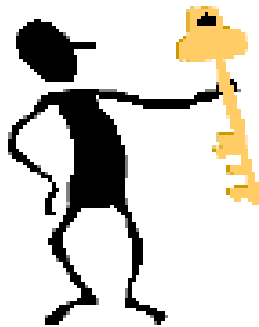


**1) CLAVE
PRIVADA O
SIMÉTRICA**

**2) CLAVE PÚBLICA
O ASIMÉTRICA**

1) Criptografía Simétrica:

- Conjunto de métodos que permite una comunicación segura entre las partes componentes.
- Siempre y cuando previamente se haya intercambiado una clave que llamaremos clave simétrica,
- La simetría se refiere a que las partes usan la misma llave para cifrar, como para descifrar.



D.E.S.: DATA ENCRYPTION STANDARD: ESTÁNDAR DE ENCRIPCIÓN DE DATOS:

- Es un sistema Criptográfico Simétrico.
- Es uno de los sistemas utilizados por las agencias del gobierno de EE.UU. no relacionadas con la seguridad nacional.
- Fue creado por IBM partiendo del proyecto Lucifer y propuesto al NBS (National Bureau of Standards), hoy NIST (National Institute of Standards and Technology), que lo adoptó en 1977 al igual que el ANSI (American National Standards Institute).
- Está disponible en "chips" pero su exportación está controlada por el departamento de estado de EE.UU.





*D.E.S.: DATA ENCRYPTION STANDARD:
ESTÁNDAR DE ENCRIPCIÓN DE DATOS:*

- Cifra bloques de 64 bits en bloques de 64 bits:
 - Modificación del NBS, inicialmente eran 128.
- Utiliza una clave de 64 bits (8 de paridad, el último bit de cada byte):
 - Modificación del NBS, inicialmente eran 128.
- Divide los datos o mensajes en bloques de 64 bits y los cifra por separado.
- Utiliza un “dispositivo” denominado **SBB** (standard building block o constructor estandar de bloques):
 - Requiere como entrada un bloque de 64 bits y una clave de 48 bits.
 - Produce una salida de 64 bits.
 - Requiere 16 dispositivos sbb.



D.E.S.: DATA ENCRYPTION STANDARD: ESTÁNDAR DE ENCRIPCIÓN DE DATOS:

- En 1988 se demostró que un ataque por *fuerza bruta* contra el algoritmo DES ya era posible:
 - Gracias al avance de la informática paralela, entre otras cosas.
- La *debilidad* no está en el algoritmo, sino en la *clave*:
 - La clave no posee suficiente longitud.
 - Si se aumenta la clave el des sigue siendo seguro.
- También se conocen claves débiles y semidébiles para este algoritmo:
 - Su número es tan pequeño en comparación con el total de claves posibles que no supone un gran problema.

Variantes del DES:

- *DES múltiple*:
 - consiste en aplicar el algoritmo des, con diferentes claves, varias veces.
 - aumenta la seguridad ya que el des *no* posee estructura de grupo (algebraico):
 - si la poseyera significaría que:
 - habría una tercer clave que produciría el mismo resultado logrado al aplicar dos veces el des con dos claves diferentes.
 - no se habría incrementado la seguridad.
 - para un algoritmo con estructura de grupo:

$$E(E(m, k_2), k_1) = E(m, k_3)$$

Variantes del DES:

- *La variante más utilizada es el triple-des (3des):*
 - *Se eligen dos claves k_1 y k_2 , el procedimiento es el siguiente:*

$$C = E_{K_1}(D_{K_2}(E_{K_1}(M)))$$

- *La clave en este caso tendrá 112 bits y 16 de paridad (128 en total).*



2) Criptografía Asimétrica:

- Utiliza complicados algoritmo matemáticos con números primos grandes y curvas elípticas.
- Cada usuario ha de poseer una pareja de claves:
 - * **Clave privada;**
 - * **Clave pública.**

CIFRAR



ENVIAR



DESCIFRAR



Criptosistema RSA

- Las siglas provienen de su inventor (Rivest, Shamir, Adleman).
- Emplea las ventajas proporcionados por las propiedades de los n° primos, ya que su robustez se basa en la facilidad para encontrarlos.
- **DES** implementado en software es 100 veces más rápido que **RSA**. Por tanto para mensajes cortos se debe utilizar RSA y para los largos DES.
- Desde el punto de vista de la confidencialidad los algoritmos asimétricos proporcionan una mayor seguridad que los simétricos a costa de una mayor carga computacional. Es por esta razón que generalmente se emplea una combinación de ambos.





Firmas digitales

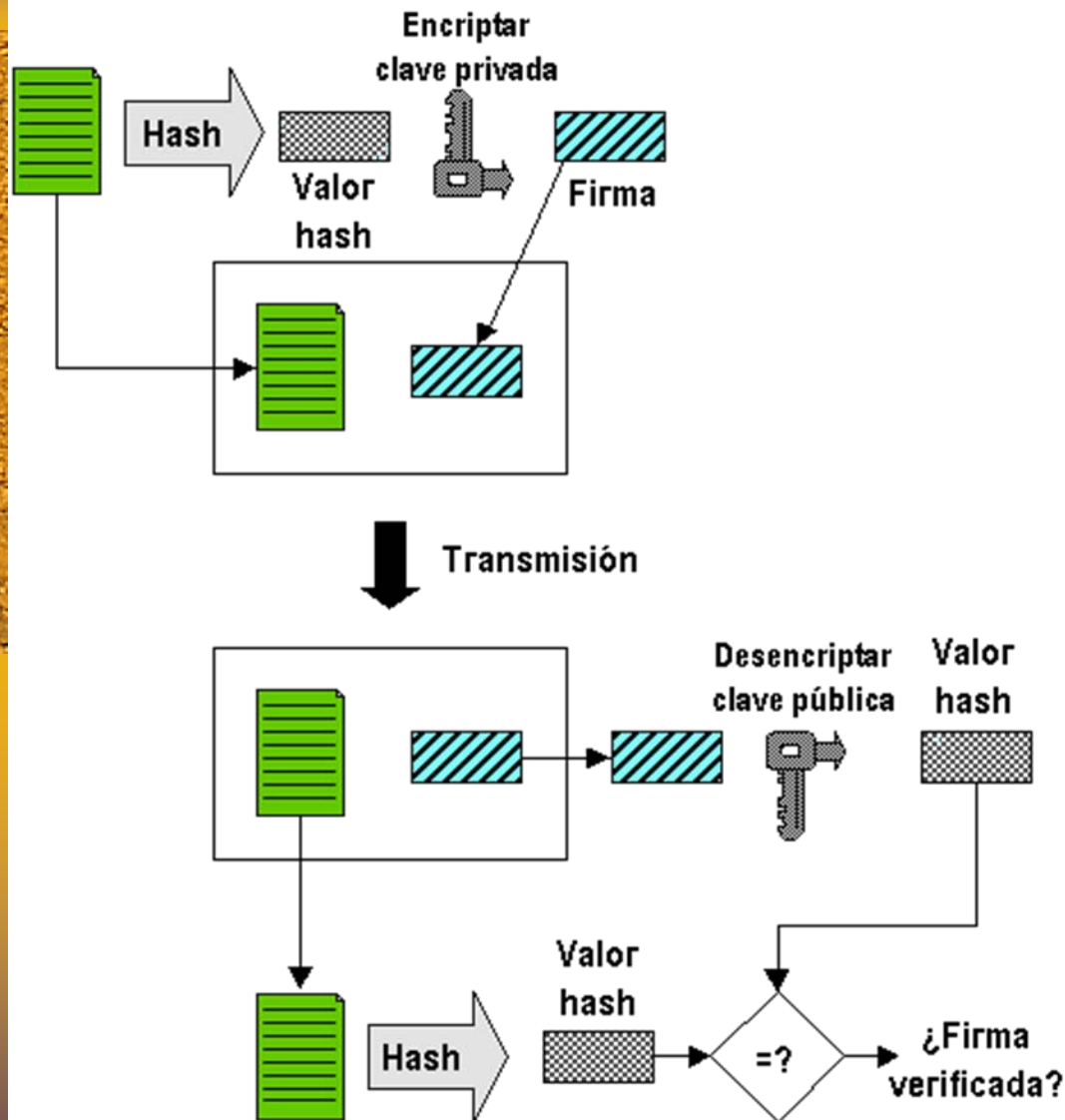
Permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

Son una solución que ofrece la criptografía para verificar:

- La integridad de documentos.
- La procedencia de documentos.



- Se basa en la criptografía de clave pública o asimétrica.
- Se puede definir una función Hash como aquella que reduce el mensaje a un conjunto de datos, denominado resumen, de longitud mucho menor que el mensaje, usualmente 128 ó 254 bits y que viaja junto con el mensaje original.



1. E genera un resumen del documento.
2. E cifra el resumen con su clave privada, firmando por tanto el documento. Este resumen es su firma digital.
3. E envía el documento junto con el resumen firmado (la firma digital) a R.
4. R genera un resumen del documento recibido de E, usando la misma función unidireccional de resumen.
5. Después R descifra con la clave pública de E, que es conocida, el resumen firmado (firma digital de E).
6. Si el resumen firmado coincide con el resumen que él ha generado, la firma digital es válida.



Algunas aplicaciones de la firma digital

Se puede aplicar en las siguientes situaciones:

- E-mail.
- Contratos electrónicos.
- Procesos de aplicaciones electrónicos.
- Formas de procesamiento automatizado.
- Transacciones realizadas desde financieras alejadas.
- Transferencia en sistemas electrónicos.
- En aplicaciones de negocios, un ejemplo es el (EDI).
intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios.

Software

CryptoForge es un software de encriptación para seguridad personal y profesional.

kryptel es una utilidad que permite encriptar y desencriptar ficheros de una forma sencilla y rápida, impidiendo así que sean vistos por personas no autorizadas.

Encrypt-It es una utilidad que permite encriptar ficheros de la manera más segura.





Conclusión

- Finalmente debemos mencionar que no existe un sistema computarizado que garantice al 100% la seguridad de la información, por la inmensa mayoría de diferentes formas con las cuales se pueden romper la seguridad de un sistema.
- Sin embargo realizando una buena planeación de estrategias de seguridad se podrían evitar importantes pérdidas y lograr la salvación de una organización o la obtención de grandes ganancias directas.



- Las actuales amenazas a Internet pueden encontrar puertas de acceso vulnerables a la red empresarial más rápido que nunca y los atacantes hoy en día tienen mayores destrezas para aprovechar las vulnerabilidades.

- Un año es una eternidad en el mundo de la seguridad en Internet puesto que muchas cosas pueden cambiar en ese lapso de tiempo.



- Una empresa proactiva, consciente de la seguridad es menos probable que sufra de enlaces débiles o zonas vulnerables.
- Como ejecutivo a cargo de la seguridad, sus empleados le tendrán como el ejemplo a seguir. Dé ejemplo mediante un esfuerzo concertado para evitar caer en la trampa de ejecutar un programa de seguridad desactualizado.



Información es conocimiento y como tal debemos atribuirle la importancia que merece.

- Esta importancia incluye estudiar y lograr la forma de protegerla.
- Esto plantea una paradoja:
- Si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.
- Si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

BIBLIOGRAFIA

- Firma Digital - Master en Dirección de Empresas - Universidad del Salvador (Argentina) – Universidad de Deusto (España) – 2002. www.hfernandezdelpech.com.ar
- Criptografía y Seguridad en Computadores, 3º Edición – 2002 - Manuel J. Lucena López mlucena@ujaen.es
- Tesis de Seguridad Informática sus Implicancias e Implementación – UTN - Borghello, Cristian – 2001. www.Segu-info.com.ar





Herramientas:

<http://www.mail-abuse.com/lookup.html>

<http://www.spamhaus.org>

<http://openrbl.org/client>

<http://www.spamanti.net>

<http://rbls.org>

<http://www.tracert.com/cgi-bin/ping.pl>

<http://www.freshtech.com/ping.htm>

<http://www.tracert.com/cgi-bin/trace.pl>

<http://www.geektools.com/traceroute.php>

<http://www.traceroute.org>

<http://www.traceroute.nl>

<http://www.opus1.com/www/traceroute.html>

<http://www.visualroute.com/server.html>

<http://www.traceroute.org/#Looking Glass>

<http://www.traceroute.org/#Route Servers>

phaster.com

Privacy:

<http://www.securitywire.com>

<http://www.privacy.net/analyze>

<http://www.junkbusters.com/cgi-bin/privacy>

<http://www.privacy.net/cookies>

<http://www.privacy.net/track>

<http://www.spychecker.com>

<http://www.gemal.dk/browserspy>

<http://www.anti-trojan.net/en/onlinecheck.aspx>

nonymouse.com

WWW:

codeflux.com

codeflux.com

codeflux.com

<http://www.submitpilot.com>

