UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

RECINTO UNIVERSITARIO “RUBÉN DARÍO”

FACULTAD DE CIENCIAS PURAS

DEPARTAMENTO DE COMPUTACIÓN

TEMA: Seguridad en Internet

Trabajo de Seminario Monográfico
optar al título de Licenciatura en Computación

Elaborado Por:

Br. Karla María Duarte Rivera

Br. María del Carmen López García

Tutor : **Msc. Eman Hussein Yousif**

Febrero 2008

APLICACIONES
DE
CORREOS SEGUROS

DEDICATORIA

A mi madre Mercedes García Quintana, quien ha sido mi impulso a mejorar día a día, me ha motivado a ser perseverante y esforzada, con su amor y sacrificio ha hecho de mí una persona de bien, con mucho ánimo de ayudar a los demás.

María del Carmen López García

A mi padre quien me impulsó a recibir el seminario, aunque no estés conmigo físicamente, siempre te recordaré.

Karla María Duarte Rivera

AGRADECIMIENTO

Agradezco a Dios antes que todo por haberme dado la oportunidad de llevar a cabo este trabajo, por haberme regalado años de vida hasta el momento para realizar uno de mis sueños y cumplir una de mis múltiples metas en esta vida.

De la misma forma agradezco a mi familia especialmente a mi madre por haberse sacrificado por mí toda la vida, haberme inculcado el espíritu de superación y perseverancia, por haber creído en mi, por haberme ensenado que a pesar de los obstáculos que nos encontramos en la vida, no debemos darnos por vencido y con mucha fuerza de voluntad y ayuda de Dios podemos superarlos.

También agradezco a mis amigos, que a lo largo de mi vida me han apoyado incondicionalmente, siendo estos amigos mas que hermanos y con su gran ayuda muchas veces salimos adelante, en especial a mis amigos Darwing Jaime Vallejos y su esposa Luz Morena Mejía.

María del Carmen López García

Doy infinitas gracias a Dios por la vida y el camino que he recorrido en el transcurso de la misma.

Gracias a mi hijo por ser mi fuerza y razón para concluir este trabajo.

A Sergio, quien me instó a concluir este seminario para obtener el título.

A mis padres por su infinito amor, comprensión y apoyo.

Agradezco el apoyo de los Hnos. Rayo Torrente.

Al matrimonio Jaime Mejía por su asistencia técnica.

Especialmente gracias a nuestra tutora Msc. Eman Hussein por el tiempo que nos dedicó y su preocupación por que concluyeramos el presente trabajo.

Karla María Duarte Rivera

CONTENIDO

Pág.

Resumen 8
Introducción 9
Justificación 12
Objetivo General 13
Objetivos Específicos 14
Marco Teórico 15
Unidad I: Seguridad en Internet 16
1.1. Políticas y recomendaciones 22
1.2. Planeación de las necesidades de seguridad 23
1.3. Análisis de riesgos 25
1.3.1 Identificación de activos 26
1.3.2. Identificación de amenazas 27
1.3.3. Cuantificación de los riesgos 28
1.4. Análisis de costo-beneficio 28
1.4.1. Costo de las pérdidas 29
1.4.2. Costo de prevención 29
1.4.3. Como convencer a los directivos. 31
1.5. Políticas 32
1.5.1. El papel de las políticas 32
1.5.2. Estándares 34
1.5.3. Recomendaciones 35
1.5.4. Algunos consejos sobre como desarrollar políticas prácticas. 35

1.6. El problema de la seguridad por ocultación 39
1.6.1. Como declarar los problemas 42
1.6.2. Información confidencial 43
1.6.3. La administración de riesgos es cuestión de sentido común 44
Unidad II: Software dañinos 46
2.1. Definición de virus informático 46
2.2. Reseña histórica de los virus 47
2.3. Clasificación de los virus informáticos 51
2.3.1. Según su forma de actuar 52
2.3.2. Según su comportamiento 53
2.4. Daños que provocan 54
2.5. Síntomas típicos de una infección 57
2.6. Formas de contagio 58
2.7. Métodos de protección 59
Unidad III: Servicios de seguridad y Mecanismos de seguridad 60
3.1. Servicios de seguridad 61
3.2. Mecanismos de seguridad 62
Unidad IV: Aplicaciones de correos seguros 65
4.1. Arquitectura y servicios 65
4.2. Formatos de los mensajes 66
4.3. Protocolos 67
4.4. PEM (Privacy Enhanced Mail – Correo Privado Mejorado) 69
4.4.1. Origen de PEM 69
4.4.2. Servicios de seguridad en PEM 70
4.4.3. Formato e implementación PEM 71
4.5. *PGP (Pretty Good Privacy – Privacidad Muy Buena)* 73
4.5.1 Descripción operativa 74
4.5.2 Algoritmos que utiliza el standard PGP 92
4.5.3 Consideraciones de seguridad de los algoritmos y PGP en general. 97
Unidad V: Aspectos sociales 99

Diseño Metodológico 107
Conclusiones 122
Anexos 123
Lista de abreviaturas 124
Glosario 126
Bibliografia 129

RESUMEN

El presente documento describe los problemas que enfrenta todo usuario en la actualidad con el manejo de la información libre a través del Internet. Específicamente el robo de información. Los datos, información o archivos que son enviados de una PC a otra pueden ser interceptados y leídos por personas no autorizadas. Aquí se menciona la necesidad de diseñar mejores políticas, controles, procedimientos y recomendaciones a los administradores de redes y empresas en general.

También se expone el caso de los software dañinos o virus desde sus orígenes hasta las medidas que se pueden tomar para evitarlos.

Describe los servicios y mecanismos de seguridad que se deben tomar en cuenta para mejorar la seguridad en la comunicación entre usuarios.

Detalla el uso de aplicaciones de correos seguros. Menciona las razones que hace a la aplicación PGP ser la más generalizada y el uso que hace de los diferentes algoritmos para ofrecer mayor seguridad.

Resalta la importancia del uso de firmas digitales en los mensajes para protegerlos.

Se diseñó una aplicación la cual hace uso del método o cifrado de Vigenere que encripta / desencripta archivos y cadenas de textos.

INTRODUCCIÓN

A medida que ha aumentado la preparación de los usuarios en la utilización de los ordenadores y redes, la seguridad se ha convertido en un problema cada vez más grave para la industria informática y de comunicaciones. Cada vez es mayor el número de personas dotadas de los suficientes conocimientos como para causar daño al sistema informático de una organización. Debido a esto, cada vez se establecen mayores medidas preventivas y se dedica más atención a la seguridad de las redes.

Los principales tipos de violación de los sistemas de seguridad son:

- Falseamiento: modificación previa a la introducción de los datos en el sistema informático o en la red.
- Ataque ínfimo: consiste en la realización de acciones repetitivas muy pequeñas.
- Suplantación de personalidad: cuando un individuo accede a una red mediante el empleo de contraseñas o códigos no autorizados.
- "Puertas traseras": se da cuando los programas de seguridad son inadecuados o incluyen errores de programación.
- Intercepción y monitorización de los canales: las señales pueden ser interceptadas cuando el intruso encuentra la frecuencia adecuada.

A raíz de la interconexión del mundo empresarial a la Internet y utilización de correos electrónicos para enviar y almacenar información de todo tipo (noticias, documentos, normas y aplicaciones informáticas de libre distribución hasta complejas transacciones) se requieren medidas de seguridad que garanticen la confidencialidad, la integridad y el origen de dicha información.

Las soluciones que proponen los organismos de normalización consisten en dotar a las redes de una serie de servicios de seguridad que utilizan en su mayoría técnicas criptográficas como principal herramienta básica.

El **correo electrónico** (***correo-e***) es una herramienta de uso generalizado en la actualidad. Su funcionamiento ha quedado normado por estándares como X.822, X.400, SMTP y MIME, los cuales facilitan, la interacción pero contemplan tan solo elementos básicos de privacidad y ninguno de protección contra intrusos. Es por esto último que se han considerado diversas medidas de seguridad para mantener privacidad e integridad y garantizar autenticidad en el correo-e.

Cualquier herramienta para correo-e seguro debe tener tres características:

1. Ser surtido por varios vendedores o productores.
2. Interoperable.
3. Aprobado o avalado por las entidades estandarizadoras de Internet.

Entre los rasgos que ha de mantener está la *privacidad*, es decir, el encriptamiento de datos, la *autentificación*, que conlleva la *integridad* de los mensajes, y el manejo de llaves.

En el correo-e, el encriptamiento se hace por lo general con métodos de llave pública y la revisión de integridad mediante firmas electrónicas y funciones de dispersión para construir compendios a la manera de sumas de prueba.

El manejo de llaves se trata, por lo general, mediante autoridades certificadoras de llaves públicas, las cuales son expendedoras de certificados. En el intercambio de mensajes, los certificados quedan en función de las llaves públicas de los usuarios y de otros factores tales como “estampas de tiempo”, o “huellas digitales‟” (es decir, de valores de funciones de dispersión dependientes de llaves, señas de identidad de los usuarios, servidores de correo-e, etc.).

Conforme la presencia de Internet y sus servicios se vuelve más preponderante en nuestras vidas, se ha visto como se incrementa su mal uso, sobre todo en el correo-e.

Por lo que resulta importante contar con mecanismos para asegurar que la información que se transmita sobre Internet y otras redes sea altamente confiable.

El uso de correo-e seguro, ya tiene presencia en áreas como: la financiera, la gubernamental, la corporativa, la educativa, por citar sólo algunas. Sin embargo, se está observando que debido a que cada proveedor de software entiende y desarrolla los algoritmos a su manera, además de las soluciones propietarias, para integrar mecanismos de seguridad en los servidores de correo, es necesaria una mayor difusión de los estándares en el uso e implementación de estas herramientas. Se ha propiciado la generación de entes aisladas entre sí, razón por la cual el uso de esquemas de seguridad en el correo-e no se ha extendido ampliamente. Es importante considerar la interoperabilidad de los diversos productos comerciales existentes que administran el correo, sin olvidar una seguridad robusta, y cuya consecuencia principal será obtener un servicio de comunicación electrónica altamente confiable.

JUSTIFICACIÓN

Debido a que la Internet es el medio de comunicación más utilizado, en nuestros tiempos, es de vital importancia tratar el tema de la seguridad de la información. Para las organizaciones gubernamentales, no gubernamentales, empresas de servicios y cualquier usuario, la información puede representar: inversiones, trabajo, bienes o servicios que pueden ser violadas al viajar por el Internet.

La Seguridad en Internet no es sólo una preocupación empresarial, toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimicidad. Los datos pueden ser: leídos, alterados o bien borrados totalmente por personas que no tienen autorización.

Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

OBJETIVO GENERAL

Proteger el contenido de los archivos de textos, diseñando un sistema que aplique el Cifrado de Vigenere para encriptarlos y desencriptarlos.

OBJETIVOS ESPECÍFICOS

- Describir los problemas que se enfrentan con respecto a la seguridad en el Internet.
- Exponer las etapas del proceso de planeación para mejorar la seguridad.
- Analizar los virus informáticos, desde su origen hasta las medidas de prevención existentes.
- Mencionar y analizar los diferentes servicios y mecanismos de seguridad.
- Resaltar los servicios que brinda PGP a través de las diferentes funciones criptográficas que utiliza.
- Enfatizar la importancia que tienen las firmas digitales en los mensajes.
- Diseñar una aplicación que encripta / desencripta archivos de textos antes de ser enviados por correo electrónico.

MARCO TEÓRICO

UNIDAD I: SEGURIDAD EN INTERNET

Desde el comienzo de la utilización de sistemas informáticos ha existido una gran preocupación por la seguridad de la información que almacenan las diferentes organizaciones. Antes de la expansión del uso de equipamiento de procesamiento de datos, la seguridad de la información que una organización consideraba valiosa se proporcionaba por *medios físicos*, como el uso de armarios con cierre de seguridad para almacenar documentos confidenciales y *medios administrativos*, como los procedimientos de protección de datos plasmados en la contratación del personal. Con la introducción del computador, se hizo evidente la necesidad de disponer de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en el computador. Esto ocurre especialmente en el caso de sistemas compartidos como aquellos sistemas a los que se puede acceder por medio de una red telefónica pública, una red de datos o Internet.

Los responsables de los Centros de Cómputo se han encargado desde hace años de implantar controles de seguridad física frente a intrusos interesados en acceder a los sistemas, y han realizado periódicamente copias de seguridad para prevenir posibles pérdidas involuntarias de los datos. Las medidas de seguridad de la red son necesarias para proteger los datos durante la transmisión.

En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios en su labor de piratería. La definición de un entorno seguro implica la necesidad de estudiar varios aspectos y de establecer una infraestructura que dé soporte a los servicios de seguridad que se quieren proporcionar. Lo primero que hay que establecer es: ¿Qué aplicaciones necesitan seguridad? y ¿Cuántos servicios se necesitan?. En segundo lugar hay que determinar, ¿Cómo se

van a proporcionar esos servicios?, si van a ser transparentes al usuario, si se le va a dejar elegir el tipo de servicio, etc. También es necesario determinar, ¿En qué nivel se van a proporcionar?, si en el nivel de aplicación o en niveles inferiores.

Los protocolos de Internet fueron diseñados de una forma deliberada para que fueran simples y sencillos, tanto las aplicaciones como los niveles de transporte carecían de mecanismos de seguridad. Se ha incrementado la variedad y cantidad de usuarios que usan la red para fines tan diversos como el aprendizaje, la docencia, la investigación, la búsqueda de socios o mercados, o simplemente el juego. En medio de esta variedad han ido aumentando las acciones poco respetuosas con la privacidad y con la propiedad de recursos y sistemas a través de los ***Hackers, frackers, crakers ...***

Algunos ejemplos de violaciones a la seguridad son:

1. El usuario A envía un archivo al usuario B. El archivo contiene información confidencial que debe protegerse (por ejemplo: nómina). El usuario C, que no está autorizado a leer el archivo, observa la transmisión y captura una copia del archivo durante dicha transmisión.
2. Un administrador de red, D, transmite un mensaje a un computador, E, que se encuentra bajo su gestión. El mensaje ordena al computador E que actualice un fichero de autorización para incluir las identidades de nuevos usuarios a los que se va a proporcionar el acceso a ese computador. El usuario F intercepta el mensaje, altera su contenido añadiendo o borrando entradas y luego lo envía a E, quien lo acepta como si procediera del administrador D.
3. El usuario F podría construir su propio mensaje con las entradas deseadas y transmitirlo a E como si procediera del administrador D.
4. Un empleado es despedido sin previo aviso. El jefe de personal envía un mensaje a un sistema servidor para invalidar la cuenta del empleado. El empleado intercepta el mensaje y lo retrasa el tiempo suficiente para realizar un último acceso al servidor y recuperar información confidencial. Luego, el mensaje es enviado y el servidor notifica la confirmación para invalidar la cuenta de dicho

empleado. Esta acción puede pasar inadvertida durante un considerable período de tiempo.

5. Un cliente envía un mensaje a un corredor de bolsa con instrucciones para realizar diferentes transacciones. Más tarde, las inversiones pierden valor y el cliente niega haber enviado dicho mensaje.

La seguridad es un tema complejo, algunas razones son:

1. Los requisitos fundamentales de servicios de seguridad que deben cumplirse son muy claros: confidencialidad, autentificación, no repudio e integridad. Pero los mecanismos empleados para satisfacer estos requisitos pueden ser complejos.
2. En el desarrollo de un mecanismo particular de seguridad o algoritmo, siempre se deben tener en cuenta los posibles ataques a esas debilidades inadvertidas del mecanismo.
3. Las medidas empleadas tienen sentido cuando se consideran las contramedidas.
4. Después de diseñar distintos mecanismos de seguridad, es necesario decidir dónde usarlos, tanto la *ubicación física* (¿en qué puntos de la red se necesitan determinados mecanismos de seguridad?), como la *ubicación lógica* (¿en qué capa o capas deben estar localizados los mecanismos de seguridad?)
5. Los mecanismos de seguridad suelen implicar más de un algoritmo. Requieren que los participantes posean una información secreta. También existe una dependencia de los protocolos de comunicación, cuyo comportamiento puede complicar la tarea de desarrollar mecanismos de seguridad.

La figura 1.1 constituye un modelo de seguridad en redes. Un mensaje que ha de ser transmitido de una parte a otra. Las dos partes, llamadas interlocutores, en esta transacción deben cooperar para que el intercambio tenga lugar. Se establece un canal de información para ambos interlocutores. Los aspectos de seguridad entran en juego cuando se necesita o se quiere proteger la transmisión.

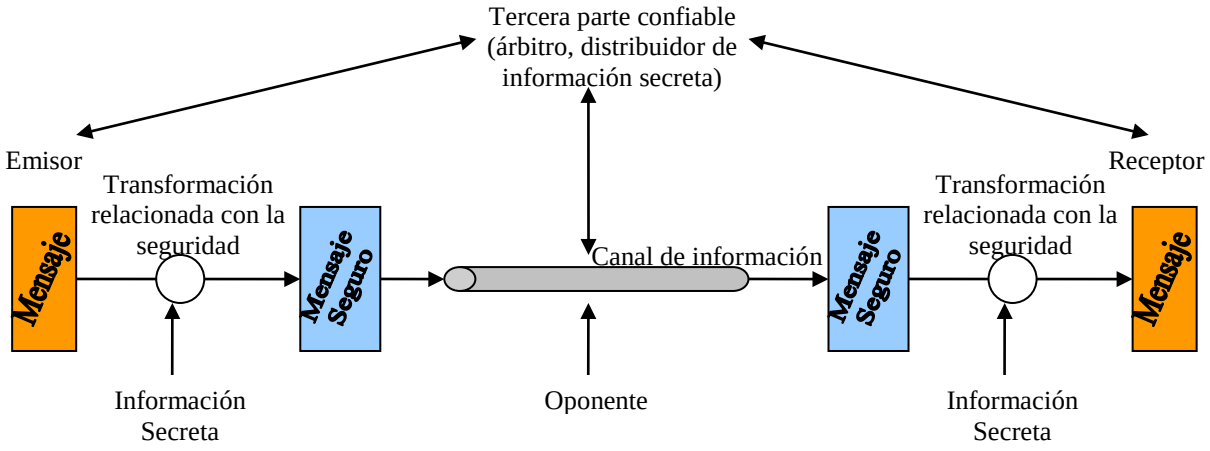


Figura 1.1 Modelo para la seguridad de redes

Todas las técnicas para proporcionar seguridad tienen dos aspectos:

- Una transformación relacionada con la seguridad de la información que se va a enviar. Ejemplo de ello tenemos el cifrado que desordena el texto original volviéndolo ilegible y la aplicación de un código que servirá para verificar la identidad del emisor.
- Alguna información secreta compartida por los interlocutores y desconocida para cualquier oponente. Como ejemplo tenemos una clave de cifrado utilizada tanto en el cifrado como en el descifrado.

Para lograr una transmisión segura, puede ser necesaria una tercera parte confiable, que sea la responsable de distribuir la información secreta a los dos interlocutores y la guarde de cualquier oponente.

Este modelo general muestra las siguientes tareas básicas en el diseño de un servicio de seguridad particular:

1. Diseñar un algoritmo para llevar a cabo la transformación relacionada con la seguridad. El algoritmo debe estar diseñado de forma que un oponente no pueda frustrar su finalidad.
2. Generar la información secreta que deba ser usada con el algoritmo.

3. Desarrollar métodos para distribuir y compartir la información secreta.
4. Especificar un protocolo para los dos interlocutores que hagan uso del algoritmo de seguridad y la información secreta, para obtener un servicio concreto de seguridad.

La figura 1.2 ofrece un modelo que refleja la preocupación por proteger un sistema de información del acceso no deseado. Los problemas ocasionados por la existencia de *hackers*, que tratan de penetrar sistemas a los que se puede acceder por una red. El intruso puede ser un empleado contrariado que quiere hacer daño, o un criminal que intenta explotar los sistemas computacionales para obtener beneficios financieros (obtención de números de tarjetas de crédito o realización de transferencias ilegales de dinero).

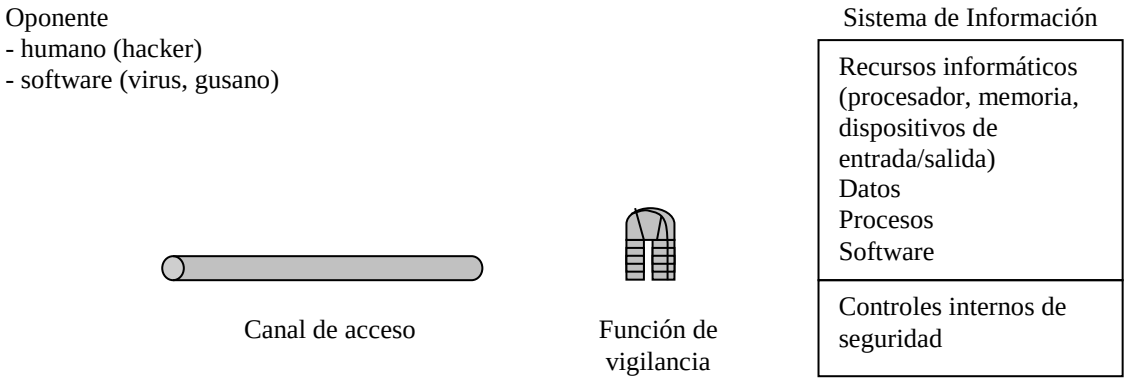


Figura 1.2 Modelo para la seguridad en el acceso a redes

Otro tipo de acceso no deseado consiste en introducir en un sistema computacional software que explote debilidades en el sistema y que pueda afectar a programas de aplicaciones, como editores y compiladores. Los programas pueden presentar dos tipos de amenazas:

- Amenazas al acceso a la información: captura o alteración de datos por parte de usuarios que no deberían tener acceso a dichos datos.
- Amenazas al servicio: explotación de fallos del servicio en los computadores para impedir el uso por parte de los usuarios legítimos.

Los virus y gusanos son dos ejemplos de ataque mediante software. Tales ataques pueden introducirse en un sistema por medio de un disco que contenga el programa no deseado oculto en software útil. También pueden ser introducidos en un sistema a través de una red.

Los mecanismos de seguridad necesarios para enfrentarse a accesos no deseados se dividen en dos grandes categorías. La primera categoría puede denominarse función de vigilancia. Incluye los procedimientos de conexión mediante cables, diseñados para negar acceso a usuarios no autorizados, y los software de ocultación, diseñados para detectar y rechazar gusanos, virus y ataques similares. Una vez que un usuario o software no accede, la segunda línea de la defensa consiste en una serie de controles internos que monitorizan la actividad y analizan la información almacenada con el fin de detectar la presencia de intrusos.

1.1. POLÍTICAS Y RECOMENDACIONES

La seguridad es una colección de soluciones técnicas a problemas que no son técnicos. Se puede invertir mucho tiempo, dinero y esfuerzo en seguridad informática, pero nunca se resolverá realmente el problema de la perdida accidental de datos o de la interrupción intencional de las actividades.

Por ejemplo un error en algún programa, una equivocación, mala suerte, mal tiempo o un agresor motivado y bien equipado, cualquier computadora puede ser comprometida, paralizada o algo peor.

El trabajo de los profesionales de la seguridad informática es ayudar a las organizaciones a decidir, cuanto tiempo y dinero quieren gastar en la seguridad. Otra parte del trabajo es cerciorarse de que las empresas tengan políticas, recomendaciones y procedimientos vigentes para que el dinero que se gaste se gaste bien. Finalmente el profesional debe auditar el sistema para verificar que se implanten los controles necesarios para lograr los objetivos de las políticas. Esto indica que la seguridad práctica es realmente una cuestión de administración y manejo más que una cuestión de destreza técnica. Por lo tanto, la seguridad tiene que ser una de las prioridades de la administración de la empresa.

El proceso de planeación de la seguridad se divide en seis etapas:

1. Planeación de las necesidades de seguridad.
2. Análisis de riesgos.
3. Análisis de costo-beneficio.
4. Creación de políticas que reflejen necesidades.
5. Implementación.
6. Auditoria y respuesta ante incidentes.

Hay dos principios de importancia fundamental, implícitos en política efectiva y planeación de seguridad:

- La conciencia sobre seguridad y políticas debe ir de arriba hacia abajo en una organización. La preocupación y conciencia de los usuarios son importantes, pero no bastan para construir y mantener una cultura efectiva de seguridad. Los directivos de la organización deben considerar que la seguridad es importante y aceptar las mismas reglas y reglamentos que todos los demás.
- La seguridad efectiva quiere decir proteger la *información.* Todos los planes, políticas y procedimientos deben reflejar la necesidad de proteger la información en cualquier de sus manifestaciones. Los datos privados no pierden su valor si se imprimen o envían por fax en lugar de estar archivados en un disco. La información confidencial de un cliente no pierde su valor si la mencionan por teléfono dos usuarios en lugar de estar contenida en mensajes de correo electrónico. La información debe protegerse en todas sus formas.

1.2. PLANEACIÓN DE LAS NECESIDADES DE SEGURIDAD

Hay muchas clases de seguridad que deben preocupar a los usuarios y a los administradores de sistemas de cómputo.

Algunos de los aspectos que se deben tomar en cuenta en la seguridad son:

Confidencialidad

Proteger la información para que nadie pueda leerla o copiarla, sin autorización del dueño. Este tipo de seguridad no solo protege toda la información *en su conjunto* sino también protege cada pedazo de información.

Integridad de datos

Proteger la información (incluyendo los programas) para evitar que se borre o altere en cualquier manera, sin el permiso del dueño de la información. Los ítems de información que deben protegerse incluyen registros contables, cintas de respaldos, hora de creación de los archivos y la documentación

Disponibilidad

Proteger los servicios para que no se degraden o dejen de estar disponibles sin autorización. Si el sistema no esta disponible cuando un usuario con autorización lo necesita, la consecuencia puede ser tan dañina como perder información que esta guardada en el sistema.

Consistencia

Asegurar que el sistema se comporta como lo esperan los usuarios autorizados. Si los programas o el equipo de repente se comportan en forma radicalmente distinta a como lo hacían antes, en especial después de una actualización o de la eliminación de un error, puede suceder un desastre. Basta imaginar lo que pasaría si el comando ***ls*** borrara archivos de vez en cuando en lugar de listar sus nombres. Este tipo de seguridad también puede considerarse como asegurar que los datos y programas que se usan sean *correctos*

Control

Reglamentar el acceso al sistema. Si individuos (o programas) desconocidos y no autorizados están en un sistema puede presentarse un enorme problema. Hay que preocuparse de cómo entraron, que habrán podido hacer y quien más habrá entrado al sistema.

Auditoria

Además de preocuparse acerca de usuarios no autorizados, los usuarios autorizados a veces se equivocan, o comenten actos maliciosos. Si esto sucede es necesario

determinar que se hizo, quien lo hizo y que fue afectado. La única forma de lograr esto es tener un registro inexpugnable de la actividad que sucede en el sistema e identifica en forma no ambigua a todos los actores y acciones.

Confianza

Los profesionales de la seguridad no hablan de sistemas de cómputo “seguros” o “inseguros”. Más bien se usa el término “confiable” para describir el nivel de confianza que se tiene en que un sistema se comporte como se espera. Esto reconoce que no se puede lograr la seguridad absoluta. Solo se puede tratar de acercarse a ella desarrollando una confianza suficiente en la configuración total para garantizar su uso en aplicaciones críticas.

Desarrollar una confianza adecuada en un sistema de cómputo requiere reflexión y planeación cuidadosas. Las decisiones deben basarse en decisiones sobre políticas sanas, y en un análisis de riesgos.

1.3. ANÁLISIS DE RIESGOS

El primer paso para mejorar la seguridad de un sistema es contestar estas preguntas básicas:

- ¿Que se debe proteger?
- ¿Contra que debe protegerse?
- ¿Cuanto tiempo, dinero y esfuerzo se esta dispuesto a invertir para obtener una protección adecuada?

El análisis de riesgos es una parte muy importante del proceso de seguridad informática. No se puede proteger algo si no se sabe contra que hay que protegerlo.

Después de conocer los riesgos se puede planear las políticas y técnicas que se necesitan para reducir esos riesgos.

Las etapas del análisis de riesgos son:

1. Identificación de los activos
2. Identificación de las amenazas
3. Cálculo de los riesgos

1.3.1 Identificación de activos

Se debe hacer una lista de todo lo que se quiere proteger. Los ítems que se tienen que proteger incluyen objetos tangibles (unidades de disco, monitores, cables de red, medios de respaldos, manuales) o intangibles (capacidad de seguir operando, imagen publica, reputación en el medio, acceso a la computadora). Esta lista debe contener todo lo que se considera valioso. Para determinar si algo es valioso hay que pensar en lo que costaría en perdida de ingresos, tiempo perdido o costo de reparación o reemplazo.
Algunos ítems que probablemente tienen que aparecer en la lista son:

Tangibles:

- Computadoras
- Datos privados
- Respaldos
- Manuales, guías y libros.
- Listados
- Equipo y cableado de comunicaciones
- Registros de personal
- Registros de auditoria

Intangibles:

- Salud y seguridad del personal
- Privacidad de los usuarios
- Contraseñas personales
- Imagen publica y reputación
- Disponibilidad de proceso
- Información sobre la configuración

Hay que tomar una perspectiva amplia sobre estos y otros ítems en lugar de considerar solo los aspectos asociados al cómputo.

1.3.2. Identificación de amenazas

El siguiente paso es hacer una lista de las amenazas a los activos. Algunas amenazas serán ambientales, como incendios, terremotos, explosiones o inundaciones. Pueden incluir eventos poco probables pero posibles como fallas estructurales o el descubrimiento de asbesto en la sala de computo que requeriría mantenerla vacía durante un largo tiempo. Otras amenazas provienen del personal y otras más de los extraños. He aquí algunos ejemplos:

- Enfermedades de personas clave
- Enfermedades simultáneamente del personal (epidemias)
- Perdida (por renuncia, despido o muerte) de personal clave
- Interrupción de servicios de teléfono o red
- Interrupción breve de otros servicios (teléfono, agua, electricidad)
- Rayos
- Inundaciones
- Robo de discos o cintas

- Robo de la computadora portátil de una persona clave
- Robo de la computadora casera de una persona clave
- Aparición de un virus
- Errores en programas
- Subversión de terceras partes (personal de mantenimiento de un proveedor)
- Problemas laborales)
- Terrorismo político
- Intrusos maliciosos
- Colocación de información privada o inapropiada en Usenet.

1.3.3. Cuantificación de los riesgos

Cuando se han identificado los riesgos debe estimarse la probabilidad de que ocurra cada uno de ellos. Esto puedo ser más sencillo si se consideran ocurrencias anuales.

La cuantificación de riesgos es un trabajo pesado. Algunas estimaciones se pueden obtener de terceros, por ejemplo las compañías de seguros. Si algo sucede en forma regular, la estimación puede basarse en los registros históricos.

1.4. ANÁLISIS DE COSTO-BENEFICIO

Al terminar el análisis de riesgos es necesario asignar un costo a cada riesgo, y determinar el costo de defenderse. A esto se le llama análisis de costo-beneficio.

1.4.1. Costo de las pérdidas

Calcular las pedidas puede ser muy difícil. En forma simple se toma en cuenta el costo de reparar o sustituir un ítem. Una evaluación mas sofisticada puede tomar en cuenta el costo de no disponer del equipo, de la capacitación adicional requerida, de los procedimientos adicionales que resulten de la perdida, el costo de la reputación de la empresa e incluso el costo a los clientes. En general, la inclusión de mas factores en el análisis de costos implicara mas trabajo, pero mejorará su precisión.

Para la mayor parte de los propósitos no se requiere asignar un valor exacto a cada riesgo posible. Normalmente es suficiente un rango de costos para cada ítem. Puede ser conveniente asignar estos costos con una escala de perdida mas fina que simplemente “pedida/no perdida”.

1.4.2. Costo de prevención

Hay que calcular el costo de prevenir cada tipo de perdida. Por ejemplo, el costo de recuperarse de una falla momentánea de potencia puede ser solo el tiempo de inactividad del personal además del tiempo necesario para reiniciar el equipo. Pero el costo de la prevención puede ser la adquisición de un sistema de potencia ininterrumpida. El costo debe amortizarse a lo largo de la vida esperada de las opciones, según sea apropiado. La obtención de estos costos puede revelar costos secundarios o ingresos que también deben tomarse en cuenta.

Por ejemplo, la instalación de un sistema contra incendios mejor puede hacer que disminuyan las primas del seguro contra incendios y además representar un beneficio fiscal adicional por depreciación de capital. Pero gastar dinero en un nuevo sistema contra incendios significa que el dinero no estará disponible para otras cosas, tales como capacitación de personal, o incluso para invertirlo.

No es posible eliminar los riesgos

Se pueden identificar y reducir los riesgos, pero no se pueden eliminar por completo. Por ejemplo, se puede adquirir un sistema de potencia ininterrumpida para reducir el riesgo de que una interrupción de potencia dañe los datos. Pero esta unidad puede fallar cuando se necesite. La interrupción puede durar más que la duración de las baterías. El personal de limpieza puede haber desconectado la unidad para conectar su pulidora.

Un análisis cuidadoso de riesgos permitirá identificar estos *riesgos secundarios* e incorporarlos a los planes. Por ejemplo, se puede comprar otra unidad de potencia ininterrumpida. Pero claro, ambas podrían fallar al mismo tiempo. Puede suceder una interacción entre ellas que no se tomo en cuenta cuando se instalaron. La probabilidad de que se interrumpa la potencia disminuye a medida que se adquieren más unidades de respaldo. Pero nunca llega a cero.

El análisis de riesgos ayuda a protegerse de riesgos humanos y naturales. Por ejemplo, puede ayudar a protegerse de intrusos identificando los riesgos y las medidas de protección. Pero tal como sucede con las fallas de potencia. No se puede eliminar la posibilidad de que alguien penetre en una computadora.
Esto es fundamental para la seguridad informática: no importa que tanto se asegure una computadora si el enemigo tiene suficiente tiempo, recursos, motivación y dinero para lograr penetrarla.

Hasta los sistemas que están certificados según el “Libro Naranja” del Departamento de Defensa de Estados Unidos son susceptibles de penetración. Una razón es que a veces los sistemas no están bien administrados. Otra es que algunos usuarios pueden aceptar sobornos para violar la seguridad. Los controles de acceso no sirven si no se administran bien. Tal como una cerradura no sirve para nada si el vigilante es quien esta robando un equipo a las 2 a.m.

Con frecuencia la gente es el eslabón más débil de un sistema de seguridad. El sistema mas seguro del mundo está totalmente abierto si el administrador coopera con quienes quieren penetrar. Las personas se pueden comprometer con dinero, amenazas o argumentos ideológicos. También pueden equivocarse, por ejemplo, enviando correo electrónico que contenga contraseñas a una persona equivocada.

En realidad es mas barato y fácil comprometer a una persona que a las salvaguardas tecnológicas.

1.4.3. Como convencer a los directivos.

La seguridad no es gratuita. Las medidas más complicadas de seguridad son más caras. Los sistemas más seguros son más difíciles de usar, aunque esto no tiene por que se así. La seguridad puede estorbar a los usuarios "avanzados" que muchas veces quieren llevar a cabo operaciones difíciles y a veces peligrosas sin autenticación o responsabilidad. Estos usuarios avanzados pueden ser muy poderosos dentro de una organización.

Al terminar el análisis de riesgos y el de costo-beneficio se debe convencer a los directivos de la organización que es necesario actuar. Normalmente se formularia una política que se adoptaría oficialmente. Con frecuencia, esta es una marcha cuesta arriba. Afortunadamente no hay razón para que esto suceda.

El objetivo del análisis de riesgos y de costo-beneficio es asignar prioridades a las acciones y al gasto en seguridad. Si el plan de negocios sugiere que no se acepte ningún riesgo mayor a 10,000 al año, sin seguro, se puede emplear el análisis realizando para determinar cuanto hay que gastar para lograr este objetivo.

El análisis es también una guía sobre que debe hacerse primero, que debe hacerse después y para identificar lo que puede dejarse para muchos años después. Otro

beneficio del análisis de riesgos es que ayuda a justificar ante los directivos las necesidades de recursos adicionales para la seguridad. Una gran cantidad de administradores y directores no sabe mucho sobre computadoras, pero entiende lo que es un riesgo y los análisis de costo-beneficios.

1.5. POLÍTICAS

Las políticas sirven para definir que se considera valioso y especifican que medidas hay que tomar para proteger esos activos.

Las políticas se pueden formular de varias maneras. Pueden escribirse políticas sencillas y generales que en unas cuantas paginas cubran muchas posibilidades. O se pueden establecer políticas para diversos activos: políticas para correo electrónico, para datos sobre el personal para información contable. Un tercer enfoque, el cual usan muchas empresas grandes, es tener políticas pequeñas y sencillas complementadas por estándares y recomendaciones sobre el comportamiento.

1.5.1. El papel de las políticas

Las políticas juegan tres papeles principales. Primero, aclaran que se esta protegiendo y por qué. Segundo, establecen la responsabilidad de la protección. Tercero, ponen las bases para resolver e interpretar conflictos posteriores. Lo que las políticas *no* deben ser generales y no variar mucho a lo largo del tiempo.

Por ejemplo:

> La información y el procesamiento de la información son un recurso crítico para la empresa XX. Se debe proteger la información según su valor para XX, y de acuerdo con la legislación aplicable. Todos los empleados comparten la responsabilidad de proteger y supervisar la información que se produzca, manipule, reciba o transmita en sus departamentos. Todos los empleados

también comparten la responsabilidad del mantenimiento, operación adecuada y protección de los recursos de proceso de la información XX.

La información que debe protegerse es aquella que se descubra, conozca, obtenga o maneje durante las actividades de negocios que no sea conocida en general fuera de XX. Esto incluye información privada de negocios (los nuestros y los de otras organizaciones y empresas), información sobre patentes, datos sobre el personal, información financiera, información sobre oportunidades de negocios y cualquier otra que le confiera una ventaja a XX si no se divulga. La información personal acerca de los empleados, clientes y proveedores también debe considerarse confidencial y debe protegerse.

Toda la información de XX que esté almacenada en cualquier forma –en medios de cómputo, listados en microfilm, medios fotográficos o cualquier otro medio tangible- es responsabilidad del director de información. Esto implica que las facilidades de XX solo se pueden usar para las funciones relacionadas con los negocios que indique el presidente. El director de Información es el responsable de proteger toda la información y los medios de procesar la información que pertenezcan a XX, estén o no ubicadas en instalaciones propiedad de la empresa. El director tendrá autoridad para actuar según esta responsabilidad con la aprobación del presidente XX. El director de información formulara los estándares y recomendaciones que sean necesarios, de acuerdo con la práctica usual de los negocios, para asegurar la protección y la continuidad del proceso de la información.

Es importante notar en este ejemplo de políticas que aparece la definición de que se esta protegiendo, quien es responsable de protegerlo y a quien le corresponde crear recomendaciones adicionales. Estas políticas se pueden mostrar a todos los empleados y a los extraños para explicárselas. Tienen vigencia sin hacer referencia a que sistema operativo se emplee o a quien sea el director de información.

1.5.2. Estándares

Los estándares sirven para codificar las prácticas exitosas de seguridad en una organización. Se redactan generalmente en términos de “es obligatorio”. Los estándares en general no dependen de las plataformas y por lo menos implican una métrica que permita determinar si se han cumplido. Los estándares se elaboran para apoyar las políticas y cambian lentamente en el tiempo. Pueden enfocarse a asuntos como la manera de investigar a los empleados nuevos, cuanto tiempo deben conversarse los respaldos y como deben probarse los sistemas de potencia ininterrumpida.

Por ejemplo, considérese un estándar para respaldos. Podría ser:

> Se efectuaran respaldos de todos los datos en línea y de todos los programas regularmente. Nunca se dejaran de hacer respaldos por más de 72 horas de funcionamiento normal del negocio. Todos los respaldos se guardaran por lo menos durante seis meses. El primer respaldo en enero y julio de cada año se guardara indefinidamente fuera de las premisas en una ubicación segura. Todos los medios de respaldo deben cumplir con los estándares de la industria para estos propósitos y ser legibles por lo menos después de cinco años de almacenamiento sin atención.

Este estándar no menciona mecanismos específicos de respaldo o ningún paquete. Establece claramente, sin embargo, que se tiene que guardar, por cuanto tiempo y cada cuando se tienen que hacer respaldos.

Este es un estándar posible para la autenticación:

> Cada cuenta en una computadora multiusuario tendrá un solo usuario autorizado para usarla. Ese usuario deberá autenticar su identidad al sistema usando alguna prueba positiva de identidad. Esta prueba de identidad puede hacerse mediante un objeto aprobado o una tarjeta inteligente, un mecanismo de contraseñas descartables autorizado o una unidad biométrica aprobada. No se permitirá el uso de contraseñas reutilizables para la autenticación primaria en ninguna

> computadora que esté conectada a una red o a un módem, que sea portátil, que se lleve fuera de la empresa o que se use fuera de una oficina privada.

1.5.3. Recomendaciones

Las recomendaciones se redacten en términos de “debería”. La intención de las recomendaciones es interpretar los estándares en el contexto de un cierto entorno, ya será un entorno de programas o un entorno físico. A diferencia de los estándares, se pueden violar las recomendaciones si resulta necesario. Como lo indica su nombre, las recomendaciones no son estándares de comportamiento sino guías para el comportamiento.

1.5.4. Algunos consejos sobre como desarrollar políticas prácticas.

El papel de las políticas (y de sus estándares y recomendaciones) es ayudar a proteger los ítems que (colectivamente) se consideran importantes. No necesitan ser demasiado específicas y complicadas en la mayoría de los casos. A veces es suficiente una afirmación de la política como se muestra en el ejemplo:

> El uso y la protección de este sistema son responsabilidad de todos. Haga solo lo que quisiera que hicieran todos. Respete la privacidad de los demás usuarios. Si aparece un problema arréglelo usted mismo o repórtelo en seguida. Cumpla todas las leyes que se refieren al uso del sistema. Acepte responsabilidad por lo que haga e identifique siempre.

A veces hay que emitir políticas más formales, que hayan sido revisadas por el departamento legal de la empresa y por varios consultores sobre seguridad, para proteger los activos. Cada organización es distinta.

Asignar un responsable

Cada elemento de información y de equipo que deba protegerse debe tener asignado un “responsable”. Esta es la persona responsable de la información, incluyendo sus copias, destrucción, respaldos y otros aspectos de la protección. Es también la persona que tiene cierta autoridad sobre otorgar acceso a la información.

El problema con al seguridad en muchos entornos es que existe información importante sin un responsable claramente establecido. El resultado es que los usuarios nunca saben quien toma las decisiones sobre el almacenamiento de la información, o quien regula el acceso a la información.

A veces la información desaparece sin que nadie se de cuenta durante un periodo largo por que no hay un “responsable” a quien avisar o que vigile la situación.

Ser positivo

La gente responde más favorablemente a las afirmaciones positivas que a las negativas. En lugar de escribir una lista larga de frases que contengan “no se debe”, piensen en como decir lo mismo de una manera positiva. La breve política que se acaba de mencionar podría haber sido redactada en forma negativa como se muestra a continuación, pero observe cuanto mejor se lee en su forma original.

> Es su responsabilidad no permitir que el sistema se use mal. No haga cosas que no quiere que los demás hagan. No viole la privacidad de los demás. Si encuentra un problema no lo mantenga en secreto si no puede arreglarlo usted mismo. No viole las leyes que rigen el uso del sistema. No trate de culpar a otros de lo que haga y no oculte su identidad. No lo pase mal.

Los empleados también son humanos

Al escribir las políticas hay que pensar en los usuarios. Cometerán errores y habrá malos entendidos. Las políticas no deben sugerir que los usuarios serán hostigados si ocurre un error.

Aun mas, debe tomarse en cuenta que los sistemas de información pueden contener datos de los usuarios que les gustaría mantener privados. Esto puede ser parte del correo electrónico, registros de personal y evaluaciones de su trabajo. Este material debe protegerse, aunque no se pueda garantizar una privacidad absoluta.

Concentrarse en la capacitación

Es prudente incluir estándares para la capacitación inicial y continua de todos los usuarios. Cada usuario debe tener una capacitación básica sobre la concientización de la seguridad, y tener alguna forma periódica de refrescar esa concientización. Los usuarios capacitados y educados son presas menos fáciles de timos y ataques de ingeniería social. También estarán más contentos sobre las medidas de seguridad si entienden por que se toman.

Una parte importante de cualquier sistema de seguridad es darle al personal tiempo y apoyo para que se continúen capacitando y educando. Siempre hay nuevas herramientas y nuevas amenazas, nuevas técnicas y nueva información por aprender. Si los empleados pasan 60 horas cada semana rastreando un virus fantasma en computadoras personales y haciendo respaldos, no serán tan efectivos como quienes reciben unas cuantas semanas de capacitación cada año. Mas aun, serán mas felices en su trabajo si se les da la oportunidad de crecer y aprender durante el mismo, y se les permite pasar las tardes y fines de semana con sus familias en lugar de tener que usarlos poniéndose al corriente con los respaldos e instalarlos programas.

La autoridad debe estar conmensurada con la responsabilidad

El primer principio de la administración de la seguridad de Spaf dice así:

> *Si tiene responsabilidad sobre la seguridad, pero no tiene autoridad para fijar las reglas y castigar a quienes las violen, su papel en la organización es asumir la culpa si sucede algo grave.*

Considérese el caso conocido de un administrador de un sistema que sorprendió a uno de los programadores tratando de irrumpir en la cuenta de *root* del sistema de nomina. Al investigar el incidente se descubrió que la cuenta de ese programador estaba llena de archivos de contraseñas de muchas maquinas de la red, muchas de las cuales estaban descifradas. El administrador inmediatamente cancelo la cuenta e hizo una cita con el supervisor del programador.

El supervisor no lo apoyó. Llamo al vicepresidente de la empresa y exigió que se le devolviera la cuenta al programador. Lo necesitaba para cumplir con un trabajo a tiempo. El administrador fue amonestado por cancelar la cuenta y se le dijo que no lo volviera hacer.

Tres meses después despidieron al administrador cuando alguien penetro al sistema de nomina que debía haber protegido. Se dice que el programador fue promovido y que le aumentaron el suelo, a pesar de que aparentaba tener mucho efectivo.

Quien se encuentre en una situación similar debe actualizar su currículo y empezar a buscar otro trabajo antes de que eso ocurra por circunstancia fuera de su control.

Elegir una filosofía básica

Debe decidirse si se adoptara el modelo: “todo lo que no este específicamente prohibido esta permitido”, o bien, el que dice “Todo esta prohibido excepto lo que este específicamente permitido”. Luego hay que ser consistente en lo que se defina como “todo lo demás”.

Adoptar defensas a fondo

Al planear las defensas y las políticas no hay que detenerse en un sola capa. Deben instaurarse varios niveles independientes y redundantes de protección. Esto incluye la vigilancia y auditoria para asegurar que las protecciones funcionen. La oportunidad de que un agresor penetre una sola capa defensiva es mucho mayor de que penetre tres capas más un sistema de alarmas.

1.6. EL PROBLEMA DE LA SEGURIDAD POR OCULTACIÓN

En la seguridad tradicional existe el concepto de “necesidad de saber”. La información se reparte, y a cada cual se le entrega solo lo que necesita para hacer su trabajo. En ambientes en los que ciertos ítems de información son sensibles o donde se deduce un problema de seguridad, esta política tiene sentido. Si tres ítems de información juntos pueden permitir una conclusión dañina y nadie conoce más de dos de ellos, se puede asegurar la confidencialidad.

En un ambiente de operación de computadoras el concepto de “necesidad de saber” por lo general no es apropiado. Esto es particularmente cierto si se basa la seguridad en el hecho de que el enemigo desconoce algo técnico. Este concepto incluso puede ser dañino para la seguridad.

Cuatro pasos para lograr una computadora más segura

Operar una computadora segura es un trabajo pesado. Si no hay tiempo para hacer un análisis de riesgos y de costo-beneficio completo, como se ha descrito antes, se recomienda que por lo menos se tomen los siguientes cuatro sencillos pasos:

1. **Decidir cuan importante es la seguridad del sitio**. Si es muy importante y se piensa que la organización sufriría un daño importante si se violara, debe darse suficiente prioridad a la respuesta. Asignar la responsabilidad de la seguridad a un medio tiempo de un programador con exceso de trabajo y sin capacitación formal en seguridad es una invitación a que ocurran problemas.
2. **Involucrar y educar a la comunidad de usuarios**. ¿Entienden los usuarios del sitio los peligros y riesgos que implican las malas prácticas de seguridad (y saben cuales son esas prácticas?) Los usuarios deben saber que hacer y a quien llamar si ven algo sospechoso o inapropiado. Educar a los usuarios ayuda a convertirlos en parte del sistema de seguridad. Ocultarles las limitaciones del sistema y de la operación no mejora la seguridad del sistema. Los agresores siempre tienen otras fuentes de información.
3. **Idear un plan para realizar y guardar respaldos de los datos del sistema**. Debe haber un lugar fuera del sitio para guardarlos por si sucede un desastre. Así se podrá reconstruir el sistema.
4. **Permanecer curioso y sospechar**. Si algo inusual sucede, hay que sospechar que existe un intruso, y debe investigarse. Normalmente se encontrara que es un error de programación o un error de uso de algún recurso del sistema. Pero de vez en cuando se encontrara algo mas serio. Por ello, cada vez que algo suceda que no se pueda explicar completamente se debe sospechar que existe un problema de seguridad e investigarlo.

Considere un ambiente en el cual la administración decide esconder los manuales para que los usuarios no puedan conocer los comandos y opciones que pueden usarse para penetrar el sistema. Los administradores pueden pensar que han mejorado la seguridad, pero probablemente no lo han logrado. Un enemigo persistente encontrara la misma documentación en otro lugar, la obtendrá de otros usuarios o de otros sitios. Muchos proveedores venden copias de sus manuales sin pedir una licencia de uso. Con frecuencia lo único que hay por hacer es ir al colegio ó universidad más cercana para encontrar copias de los manuales. Muchísima información sobre la documentación de UNIX esta disponible en la librería más cercana. Los administradores no pueden cerrar todos los caminos que permiten aprender cosas sobre el sistema.

Pero los usos locales pierden eficiencia puesto que no pueden consultar la documentación y aprender mejores opciones. También tendrán una actitud negativa por el mensaje implícito de la administración: “No confiamos completamente en que sean usuarios responsables”. Además, si alguien empieza a abusar de los comandos y características del sistema, la administración no tiene acceso al talento que se necesita para reconocer o resolver el mismo. Y si algo llega a suceder a los pocos usuarios que tienen permiso de ver la documentación, entonces no habrá nadie con la experiencia o conocimientos necesarios para tomar su lugar o ayudar a resolver un problema.

Ocultar los errores de programación o las características excepcionales en secreto es también una mala práctica de seguridad. Los desarrolladores de sistema con frecuencia colocan puertas traseras en sus programas para obtener privilegios sin tener que dar una contraseña. Otras veces se permite que errores de programación que tiene implicaciones profundas de seguridad persistan ya que la administración supone que nadie los conoce. El problema con estos enfoques es que las características y los errores de los programas tienden a ser descubiertos por accidentes o por intrusos maliciosos persistentes. Si se mantienen en secreto no se pueden vigilar y no se pueden corregir. Cuando sean descubiertos, el problema volverá a todos los sistemas similares vulnerables a ataques por parte de quienes los hayan encontrado.

Mantener algoritmos secretos, tales como algoritmos de cifrado desarrollados localmente, también es una practica dudosa. A menos que sea experto en criptografía, es difícil juzgar la fuerza de un algoritmo. El resultado de esa política puede ser un mecanismo que tiene un enorme agujero. Un algoritmo secreto no puede ser estudiado por nadie y por lo tanto, si alguien descubre una falla, podrá tener acceso a los datos sin que nadie lo sepa.

Asimismo mantener en secreto el código fuente del sistema operativo o de una aplicación no garantiza la seguridad. Quienes verdaderamente quieran penetrar el sistema de ve en cuando encontraran un agujero con o sin el código fuente. Pero sin el código fuente, los usuarios no pueden examinar un programa de manera sistemática para encontrar problemas.

La clave es la actitud. Cuando se toman medidas defensivas basadas principalmente en secretos se pierde toda la seguridad sin la discreción se pierde. Se puede caer en la situación de no saber y no poder determinar si se ha pedido la discreción, por que para mantenerla se han tenido que restringir las auditorias y la vigilancia. Es mejor usar algoritmos y mecanismos robustos y conocidos pueden desalentar a algunos agresores y pueden lograr que los curiosos busquen su diversión en otros sitios. Poner dinero en una caja fuerte es mejor que esconderlos en un frasco de mayonesa en la cocina por que nadie sabe que esta allí.

1.6.1. Como declarar los problemas

Si se descubre una falla de seguridad en programas distribuidos o ampliamente disponibles, es necesario avisárselo al proveedor *discretamente* en cuanto sea posible.

Si se “anuncia” una falla de seguridad se pone en riesgo a todos los que usan ese programa pero no tienen la capacidad o el tiempo de corregirlo. En el ambiente de usuarios de UNIX muchos están acostumbrados a tener a mano el código fuente para

hacer localmente las modificaciones que se requiera. Lamentablemente no todos tienen esa suerte, y muchos esperan semanas o meses para que el proveedor les entregue versiones corregidas de los programas. Algunos sitios ni siquiera son capaces de actualizar sus programas por que usan aplicaciones de llave en mano o aplicaciones que han sido certificadas en la configuración actual. Otros sistemas los usan individuos que no tienen los conocimientos necesarios para arreglar los problemas. Aun otros ni siquiera están en producción, o cuando menos están fuera de mantenimiento. Es necesario actuar en forma responsable. Puede ser preferible distribuir los arreglos sin dar muchas explicaciones sobre la vulnerabilidad subyacente que dar a los agresores detalles de cómo penetrar los sistemas que no se hayan arreglado.

Se conocen instancias de que persona bien intencionadas han reportado problemas de seguridad en foros públicos. Aunque la intención era obtener arreglos rápidos de los proveedores afectados, el resultado ha sido una oleada de instrucciones en sistemas cuyos administradores no tenían acceso al foro, o que no pudieron hacer los arreglos apropiados a su ambiente.

1.6.2. Información confidencial

Alguna información relacionada con la seguridad es apropiadamente confidencial. Por ejemplo, evitar que las contraseñas sean públicas es sensato. Esto no es un ejemplo de seguridad por ignorancia. Las contraseñas se han diseñado para utilizarlas confidencialmente, que no es lo mismo que una falla o una puerta trasera que le otorga al intruso el poder del súper usuario. Además, las contraseñas deben cambiarse periódicamente para que sigan siendo confidenciales.

1.6.3. La administración de riesgos es cuestión de sentido común

La clave para tener éxito en el análisis de riesgos es identificar todas las amenazas posibles al sistema, pero solo defenderse de aquellas que parecen ser amenazas reales.

Sólo porque la gente constituye el eslabón más débil no hay que olvidar otras salvaguardas. Las personas no son predecibles, pero penetrar a través de un MODEM que no tiene contraseña es más barato que un soborno. Así que deben emplearse defensas tecnológicas cuando se pueda y mejorar la seguridad a través del personal educando a los colaboradores y usuarios.

Las defensas deben emplearse a fondo, con varios niveles para respaldarse cuando uno falle. Por ejemplo, se puede adquirir una segunda unidad de potencia ininterrumpida, o poner una cerradura en la puerta de la sala de cómputo aunque exista una cerradura en la entrada del edificio. Se pueden derrotar estas combinaciones pero el esfuerzo y el costo para el enemigo aumenta, y a lo mejor se convence de que no vale la pena hacer el esfuerzo. Por lo menos se tiene la esperanza de que actúen mas lentamente y que la vigilancia y las alarmas convoquen ayuda de que algo importante se pierda o se dañe.

Pensando en estos límites es importante acercarse a la seguridad informática con un conjunto de prioridades bien pensado. No es posible protegerse de todas las amenazas. A veces conviene dejar que algo suceda en lugar de prevenirlo y después limpiar lo que haya pasado. Por ejemplo, puede ser más barato y menos complicado dejar que se interrumpa el servicio por fallas de potencia y luego reiniciar los sistemas que comprar una unidad de potencia ininterrumpida. Y no vale la pena defenderse de algunas amenazas por que son demasiado poco probables (una invasión de extraterrestres) o las defensas son demasiado difíciles (una explosión nuclear a 500 metros del centro de datos) o sencillamente son demasiado catastróficas y horribles (la administración decide cambiar todas las computadoras que usan UNIX por

computadoras son un conocido sistemas operativo para computadoras personales). La clave de una buena administración es saber de que preocuparse y hasta donde preocuparse.

Hay que decidir que se quiere proteger y cuanto va a costar la prevención de esas perdidas en comparación con el costo de recuperarse de las mismas. Luego, se tiene que decidir que acciones y que medidas de seguridad deben tomarse con base en una lista ordenada por prioridades de las necesidades mas criticas. Es importante asegurarse de incluir no solo las computadoras en la lista: no hay que olvidar que las cintas de respaldo, las conexiones de red, las terminales y la documentación también forman parte del sistema, y representan una perdida en potencia. La seguridad del personal, del sitio corporativo y de la reputación son también importantes y deben incluirse en sus planes.

UNIDAD II: SOFTWARE DAÑINOS

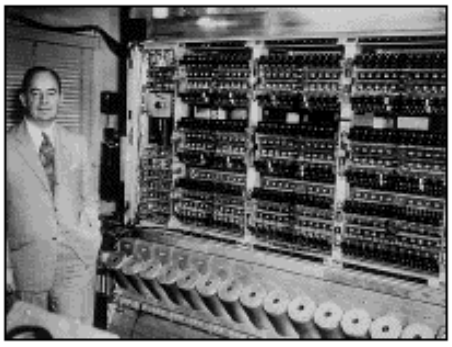
2.1. DEFINICIÓN DE VIRUS INFORMÁTICO

Un **virus informático** es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria **RAM (Random Access Memory – Memoria de Acceso Aleatorio**) de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al del programa infectado y se graba en disco, con lo cual el proceso de replicado se completa.

2.2. RESEÑA HISTÓRICA DE LOS VIRUS



En 1939, el famoso científico matemático **John Louis Von Neumann**, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "**Teoría y organización de autómatas complejos**", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la **AT&T (American Telephone and Telegraph)**, 3 jóvenes programadores: **Robert Thomas Morris**, **Douglas McIlory** y **Victor Vysottsky**, a manera de entretenimiento crearon un juego al que denominaron **CoreWar.** El juego consistía en que dos jugadores escribieran cada uno un programa llamado *organismo*, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera. Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un *organismo* suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas **destinados a dañar** en la escena de la computación.

A pesar de muchos años de clandestinidad, existen reportes acerca del virus **Creeper**, creado en 1972 por **Robert Thomas Morris**, que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto del software antivirus.

En Agosto de 1981 la **International Business Machine** lanza al mercado su primera computadora personal, simplemente llamada **IBM PC**. Un año antes, la IBM habían buscado infructuosamente a **Gary Kildall**, de la **Digital Research**, para adquirirle los derechos de su sistema operativo CP/M, pero éste se hizo de rogar, viajando a Miami donde ignoraba las continuas llamadas de los ejecutivos del "gigante azul".

Es cuando oportunamente aparece **Bill Gates**, de la Microsoft Corporation y adquiere a la **Seattle Computer Products**, un sistema operativo desarrollado por **Tim Paterson**, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de **PC-DOS** se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de **MS-DOS**.

El nombre del sistema operativo de Paterson era "**Quick and Dirty DOS**" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

La enorme prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado **PC-DOS (Personal Computer – Disk Operating System)** y posteriormente del MS-DOS **fueron totalmente vulnerables a los virus**, ya que fundamentalmente heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

Keneth Thompson, quien en 1969 creó el Sistema Operativo **UNIX**, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.

En 1984 el Dr. Fred Cohen ese mismo año escribió su libro "**Virus informáticos: teoría y experimentos**", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del **BIX BBS**, un foro de debates de la ahora revista **BYTE** reportaron la presencia y propagación de algunos programas que habían ingresado a sus computadoras en forma subrepticia, actuando como "caballos de troya", logrando infectar a otros programas y hasta el propio sistema operativo, principalmente al Sector de Arranque.

Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

En 1986 se difundieron los virus **(c) Brain, Bouncing Ball** y Marihuana y que fueron las primeras especies representativas de difusión masiva. Estas tres especies virales tan sólo infectaban el sector de arranque de los diskettes. Posteriormente aparecieron los virus que infectaban los archivos con extensión **EXE** y **COM**.

El 2 de Noviembre de 1988 **Robert Tappan Morris**, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, logrando infectar 6,000 servidores conectados a la red. Cabe mencionar que el **ArpaNet** empleaba el **UNIX**, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US $ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario. Actualmente es un experto en Seguridad y ha escrito innumerables obras sobre el tema.

En 1989 su connacional, el virus **Dark Avenger** o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida **técnica de infección**, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos.

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-copiarse infectando a otros documentos. Los llamados **macro virus** tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access.
A principios de 1999 se empezaron a propagar **masivamente** en Internet los **virus anexados** (adjuntos) a mensajes de correo, como el **Melisa** o el macro virus **Melissa**. Ese mismo año fue difundido a través de Internet el peligroso **CIH** y el **ExploreZip**, entre otros muchos más.

A fines de Noviembre de este mismo año apareció el **BubbleBoy**, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato **HTML**. En Junio del 2000 se reportó el **VBS/Stages.SHS**, primer virus oculto dentro del Shell de la extensión **.SHS**.

El 18 de Septiembre del 2001 el virus **Nimda** amenazó a millones de computadoras y servidores, a pocos días del fatídico ataque a las **Torres Gemelas de la isla de Manhattan**, demostrando no solo la vulnerabilidad de los sistemas, sino la falta de previsión de muchos de los administradores de redes y de los usuarios.

2.3. CLASIFICACIÓN DE LOS VIRUS INFORMÁTICOS

Según algunos autores existen, fundamentalmente dos tipos de virus:

1) *Aquellos que infectan archivos*. A su vez, éstos se clasifican en:
    - *Virus de acción directa*. En el momento en el que se ejecutan, infectan a otros programas.
    - *Virus residentes*. Al ser ejecutados, se instalan en la memoria de la computadora. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.
2) *Los que infectan el sector de arranque, (virus de boot)*. El sector de arranque es lo primero que lee el ordenador cuando es encendido. Estos virus residen en la memoria.
3) Existe una tercera categoría llamada *multipartite*, pero corresponde a los virus que infectan archivos y al sector de arranque, por lo que se puede decir que es la suma de las dos categorías anteriores.

Para otros autores, la clasificación de los virus también se divide en dos categorías, pero el criterio de clasificación utilizado es distinto:

1) *Virus de archivos*, que modifican archivos o entradas de las tablas que indican el lugar donde se guardan los directorios o los archivos.
2) *Virus de sistema operativo*, cuyo objetivo consiste en infectar aquellos archivos que gobiernan la computadora.

Existe una tercera clasificación, la cual atiende a la plataforma en la que actúa el virus y a algunas de sus características más importantes.

2.3.1. Según su forma de actuar

1. **Acompañante:** estos virus basan su principio en que MS-DOS ejecuta en primer lugar el archivo con extensión COM frente al de extensión EXE, en el caso de existir dos archivos con el mismo nombre pero diferente extensión dentro del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar. Después ejecuta el nuevo archivo COM, creado por el virus, y cede el control al archivo EXE.
2. **Archivo:** los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.
3. **Worms o gusanos:** se registran para correr cuando inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.
4. **Troyanos:** suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos. Funcionan de modo similar al caballo de Troya; ayudan al atacante a entrar al sistema infectado, haciéndose pasar como contenido genuino (salvapantallas, juegos, música). En ocasiones descargan otros virus para agravar la condición del equipo.
5. **Jokes o virus de broma:** no son realmente virus, sino programas con distintas funciones, pero todas con un fin de diversión, nunca de destrucción, aunque pueden llegar a ser muy molestos.
6. **Hoaxes o falsos virus:** son mensajes con una información falsa; normalmente son difundidos mediante el correo electrónico, a veces con fin de crear confusión

entre la gente que recibe este tipo de mensajes o con un fin aún peor en el que quieren perjudicar a alguien o atacar al ordenador mediante ingeniería social.

7. **Virus de macros:** un macro es una secuencia de órdenes de teclado y mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuarán hasta que el archivo se abra o utilice.

2.3.2. Según su comportamiento

1. *Virus uniformes*, que producen una replicación idéntica a sí mismos.
2. *Virus cifrados*, que cifran parte de su código para que sea más complicado su análisis. A su vez pueden emplear:
    - *Cifrado fijo*, empleando la misma clave.
    - *Cifrado variable*, haciendo que cada copia de sí mismo esté cifrada con una clave distinta. De esta forma reducen el tamaño del código fijo empleable para su detección.
3. *Virus oligomórficos*, que poseen un conjunto reducido de funciones de cifrado y eligen una de ellas aleatoriamente. Requieren distintos patrones para su detección.
4. *Virus polimórficos*, que en su replicación producen una rutina de cifrado completamente variable, tanto en la fórmula como en la forma del algoritmo. Con polimorfismos fuertes se requiere de emulación, patrones múltiples y otras técnicas antivirus avanzadas.
5. *Virus metamórficos*, que reconstruyen todo su cuerpo en cada generación, haciendo que varíe por completo. De esta forma se llevan las técnicas avanzadas

de detección al límite. Por fortuna, esta categoría es muy rara y sólo se encuentran en laboratorio.

6. *Sobrescritura*, cuando el virus sobrescribe a los programas infectados con su propio cuerpo.
7. *Stealth* o silencioso, cuando el virus oculta síntomas de la infección.

Existen más clasificaciones según su comportamiento, siendo las citadas, parte de las más significativas y reconocidas por la mayoría de los fabricantes de antivirus.

Los virus más enviados según la **ICVS (Informatic control virus scanner)** son:

Tipo	**1998**	**2000**	**2003**	**2005**
Troyanos	20%	15%	22%	25%
Gusanos	22%	20%	25%	27%
Boot	5%	1%	4%	2%
Otros	52%	64%	49%	46%

Tabla 2.1 Virus más enviados

2.4. DAÑOS QUE PROVOCAN

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Otra de las características es la posibilidad que tienen de ir *replicándose*. Las redes en la actualidad ayudan a dicha propagación cuando éstas no tienen la seguridad adecuada. Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Hay que tener en cuenta que cada virus plantea una situación diferente.

Definiremos **daño** como una acción indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños.

Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad:

a. DAÑOS TRIVIALES.

Sirva como ejemplo la forma de trabajo del virus **FORM** (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.

b. DAÑOS MENORES.

Un buen ejemplo de este tipo de daño es el **JERUSALEM**. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.

c. DAÑOS MODERADOS.

Cuando un virus formatea el disco rígido, mezcla los componentes de la **FAT** (File Allocation Table, Tabla de Ubicación de Archivos), o sobreescribe el disco rígido. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup. Esto quizás nos lleve una hora.

d. DAÑOS MAYORES.

Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus **DARK AVENGER**, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: "**Eddie lives … somewhere in time**" (Eddie vive … en algún lugar del tiempo). Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese.

Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese backup.

e. DAÑOS SEVEROS.

Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del **DARK AVENGER** (es decir, no podemos buscar la frase **Eddie lives ...**).

f. DAÑOS ILIMITADOS.

Algunos programas como **CHEEBA**, **VACSINA.44.LOGIN** y **GP1** entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de **CHEEBA**, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

2.5. SÍNTOMAS TÍPICOS DE UNA INFECCIÓN

- ✓ El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- ✓ El tamaño del programa cambia sin razón aparente.
- ✓ El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- ✓ Si se corre el CHKDSK no muestra "655360 bytes available".
- ✓ En Windows aparece "32 bit error".
- ✓ La luz del disco duro en la **CPU (Central Process Unit – Unidad Central de Procesos)** continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- ✓ No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate.
- ✓ Aparecen archivos de la nada o con nombres y extensiones extrañas.
- ✓ Suena "clicks" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- ✓ Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- ✓ En la pantalla del monitor pueden aparecen mensajes absurdos tales como "Tengo hambre. Introduce un Big Mac en el Drive A".
- ✓ En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows ’98 (No puedo evitarlo, es mas fuerte que yo...!!).

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado.

2.6. FORMAS DE CONTAGIO

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como *ejecute este programa y gane un premio*.
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software pirata o de baja calidad.

En el sistema Windows puede darse el caso de que el ordenador pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes, por el simple hecho de estar, la máquina

conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de búfer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error y hasta reinicios involuntarios, reenviarse a otras máquinas mediante la red local o Internet, entre otros daños. En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría. De manera frecuente, el usuario deberá descargar actualizaciones y parches de seguridad.

2.7. MÉTODOS DE PROTECCIÓN

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser:

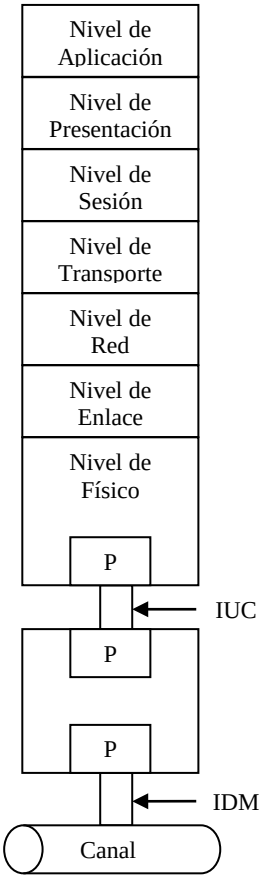
- **Antivirus**: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

- **Filtros de ficheros**: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

UNIDAD III: SERVICIOS DE SEGURIDAD Y MECANISMOS DE SEGURIDAD

La **Organización Internacional de Normalización (ISO)**, que describe el Modelo de Referencia **OSI (Open Systems Interconnection)**, recomienda establecer cifrado en el nivel de presentación por las siguientes razones:

Figura 3.1 Modelo de Referencia OSI



P: Puerto
IUC: Interfaz de la Unidad de Conexión
IDM: Interfaz Dependiente del Medio

1) Los servicios de cifrado han de colocarse en un nivel superior al de red para simplificarlo de extremo a extremo. En el nivel de transporte existen estos servicios. Por esto, el cifrado ha de realizarse en el cuarto nivel o uno superior.

2) Para minimizar la cantidad de programas a los que ha de confiarse el texto legible, el servicio de cifrado debe encontrarse en un nivel superior al de transporte.

3) En el nivel de aplicación las transformaciones sintácticas sobre los datos cifrados serían difíciles, por tanto, el cifrado ha de establecerse debajo de este nivel.

4) Es posible que no todos los campos necesiten ser cifrados y para esto donde mejor puede hacerse es en el nivel de presentación o uno superior.

3.1. SERVICIOS DE SEGURIDAD

Para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes servicios de seguridad:

1) **Autenticación de entidad par**: este servicio corrobora la fuente de una entidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra. Antes de que el tráfico sea enviado/recibido, cada router/cortafuego/servidor debe ser capaz de identificar la identidad de su interlocutor.

2) **Control de acceso (Autorización): e**ste servicio se utiliza para evitar el uso no autorizado de recursos. Se trata de un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

3) **Confidencialidad de datos:** proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

4) **Integridad de datos:** con este garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

5) **No repudio**: ésta es una forma de garantizar que el emisor de un mensaje no podrá posteriormente negar haberlo enviado, mientras que el receptor no podrá negar haberlo recibido. Puede ser de dos tipos:
   - **Con prueba de origen**. Cuando el destinatario tiene prueba del origen de los datos.
   - **Con prueba de entrega**. Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

3.2. MECANISMOS DE SEGURIDAD

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del Modelo de Referencia OSI los siguientes mecanismos de seguridad:

- **Cifrado**. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.
  Este mecanismo soporta el servicio de confidencialidad de datos y a la vez actúa como complemento de otros mecanismos de seguridad.

- **Firma digital**: es el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

  La figura 3.2 describe la firma digital según **ITU (International Telecommunications Committee)** y OSI utiliza un esquema criptográfico asimétrico. La firma consiste en una cadena que contiene el resultado de cifrar con RSA aplicando la clave privada del firmante, una versión comprimida, mediante una función Hash unidireccional y libre de colisiones, del texto a firmar.

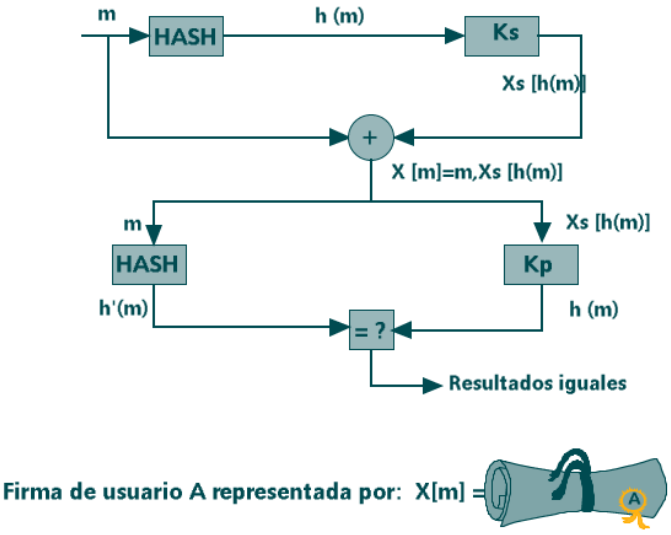


Figura 3.2 Firma Digital

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función Hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

El mecanismo de firma digital soporta los servicios de integridad de datos, autenticación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

- **Control de acceso:** este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el enviante está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

  El mecanismo de control de acceso soporta el servicio de control de acceso.

- **Integridad de datos:** es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

  Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede

ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.
El mecanismo de integridad de datos soporta el servicio de integridad de datos.

- **Intercambio de autenticación**. Existen dos grados en este mecanismo:
  - **Autenticación simple**. El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.

Figura 3.3 Autenticación

  - **Autenticación fuerte.** Utiliza las propiedades de los criptosistemas de clave pública.
    Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública. Para que un usuario confíe en el procedimiento de autenticación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación **(CA – Certification Authority)**. La Autoridad de Certificación utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado. Un certificado es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario. El mecanismo de intercambio de autenticación se utiliza para soportar el servicio de autenticación de entidad par.

UNIDAD IV: APLICACIONES DE CORREOS SEGUROS

La aplicación distribuida que más se usa es el correo electrónico y existe un aumento de interés en proporcionar servicios de autentificación y confidencialidad como parte de la herramienta de correo electrónico.

Se trataran dos enfoques que podrían dominar la seguridad de correo electrónico.

4.1. ARQUITECTURA Y SERVICIOS

Los sistemas de correo-e se integran de dos subsistemas: ***el agente usuario***, coloca los mensajes en la cola del correo-e; y ***el agente transferencia de mensajes***, es el responsable de inicializar el enlace de comunicación con las computadoras remotas y transmitir el correo-e.

La aplicación del agente usuario son los programas locales que ofrecen una interacción con el sistema de correo-e sobre la base de línea de comando, basados en menús o con una interfase gráfica.

Los agentes transferencia de mensajes son usualmente los procesos del sistema operativo, y mueven el correo-e a través del sistema o de la red. Un sistema de correo-e soporta cinco funciones básicas: composición, transferencia, reporte, despliegue y disposición.

Además, a estos servicios básicos, la mayoría de los sistemas de correo-e ofrecen una amplia variedad de características avanzadas para administrar los mensajes del usuario. Un servicio muy usado en el correo-e son las listas de interés, las cuales

permiten con sólo enviar un mensaje a la lista de correo-e en particular, repartir una copia idéntica del mensaje a todos los subscriptores de la lista, lo que evita la necesidad de enviar un correo-e a cada uno de ellos.

Una idea clave en todos los sistemas modernos de correo-e es la distinción entre el sobre y su contenido. El sobre envuelve el mensaje que contiene toda la información necesaria para transportar el mensaje, tales como la dirección destino, prioridad y nivel de seguridad. El agente transporte usa el sobre para el enrutamiento del mensaje.

4.2. FORMATOS DE LOS MENSAJES

El **RFC 822** define un mensaje que se integra de dos partes: **un encabezado y un cuerpo**.
El encabezado consiste de una serie de nombres de campo, después del cual hay una línea en blanco que marca el fin del encabezado y el principio del cuerpo, el cual consiste de sólo texto **ASCII (A**merican **S**tandard **C**ode for **I**nformation **I**nterchange**) (RFC 822)**. El encabezado contiene información de control para el agente usuario. El cuerpo del mensaje contiene el mensaje a recibir.

Para transmitir datos no ASCII a través del correo-e, el **IETF (*Internet Engineering Task Force*)** definió el formato **MIME (*Multipurpose Internet Mail Extensions*)**.

MIME permite que datos arbitrarios sean codificados en ASCII y poder ser transmitidos en un mensaje de correo-e normal. Para acomodar los tipos de datos arbitrarios, cada mensaje MIME incluye información que le dice al recipiente receptor el tipo de dato y la codificación usada. La información de MIME reside en el encabezado del mensaje según el RFC 822 – en el encabezado MIME se especifica la versión de MIME usada, el tipo de dato que esta siendo enviada y la codificación usada para convertir los datos en

ASCII. En el formato MIME, existen siete tipos de datos: texto, imagen, audio, vídeo, mensaje, multiparte y aplicación.

En adición a los formatos de los mensajes, el protocolo **TCP/IP** especifica un estándar para el intercambio de correo-e entre computadoras. Esto es, la norma define el formato exacto de los mensajes de correo-e a transferir de un servidor a otro. El protocolo para transferencia de mensajes es conocido con el nombre de **SMTP (*Simple Mail Transfer Protocol*)**.

SMTP define sus reglas para transmitir el correo-e entre computadoras. El protocolo tiene dos funciones: emisor y receptor. El emisor establece una conexión TCP con el receptor, usando el puerto 25. Durante una sesión SMTP el emisor y el receptor intercambian una secuencia de comandos y respuestas. Primero, identifican los nombres de dominio de las computadoras. Después, el emisor ejecuta una transacción de correo-e por la secuencia siguiente: identifica el origen del mensaje, identifica los recipientes de correo-e, transmite el mensaje y transmite un código que indica que el mensaje esta completo. Al final de la transacción, el emisor puede: iniciar otra transacción, invierte las funciones y se vuelve receptor, termina y cierra la conexión.

4.3. PROTOCOLOS

Los servicios de seguridad pueden ser agregados a cada enlace de comunicación a lo largo de una trayectoria dada, o pueden ser integrados alrededor de los datos que están siendo enviados, siendo esto independiente de los mecanismos de comunicación. Este enfoque avanzado es frecuentemente llamado seguridad “nodo-a-nodo” (end-to-end).

Las dos características de este tipo de seguridad son privacidad (donde el recipiente deseado sólo puede leer el mensaje) y la autentificación (en el otro caso, recipiente puede asegurar la identidad del emisor). La capacidad técnica de estas funciones es bien conocida desde hace tiempo, sin embargo, recientemente ha sido sólo aplicada al correo-e de Internet.

Es usual que se cuente con un mecanismo de autentificación de quién origina el mensaje y privacidad para los datos. Además, de proveer un esquema de recepción firmada desde el recipiente. En núcleo de estás capacidades en el uso de la tecnología de llave pública y el uso a gran escala de llaves públicas, lo que requiere un método de certificación que dada una llave pertenece a un usuario dado.

Aunque, se ofrecen servicios parecidos al usuario final, los dos protocolos tienen formatos distintos. Adicionalmente, y esto es importante a los usuarios corporativos, en este caso se cuenta con diversos formatos para los certificados. Lo que significa, que no sólo los usuarios no pueden comunicarse con los que usen otro, además, no pueden compartir los certificados de autenticación. La diferencia entre los dos protocolos es parecida a la diferencia entre los formatos GIF y JPEG, siendo que hacen las mismas cosas, más no su formato entre ellos.

Existen dos propuestas principales para ofrecer los servicios de seguridad que hemos mencionado: **S/MIME** y **PGP (Pretty Good Privacy)**. Otros protocolos han sido propuestos en el pasado como son: **PEM (Private Enhanced Mail)** y **MOSS (MIME Object Security Services)**, no han tenido mayor presencia. Sin embargo, ahora diversos proveedores de servidores de correo-e, incluyen en sus productos a **S/MIME, PGP/MIME y OpenPGP**.

4.4. PEM (PRIVACY ENHANCED MAIL – CORREO PRIVADO MEJORADO)

PEM (Privacy Enhanced Mail) es una de las primeras propuestas a nivel IETF para asegurar el correo electrónico a través de criptografía de llave pública. PEM es el formato de correo seguro normalizado por Internet.

4.4.1. Origen de PEM

Se crea en 1993 y sus especificaciones se encuentran en los RFCs 1421, 1422, 1423 y 1424. A pesar de que PEM se convirtió en un estándar IETF su uso nunca se generalizó ni se implementó. Una de las causas fue que este protocolo depende de la previa implantación de una infraestructura de llave pública, **PKI** (Public Key Infraestructura – Infraestructura de Clave Pública), con una sola raíz. El desarrollo de tal PKI demostró ser imposible hasta que el costo operacional y la responsabilidad legal de la raíz y política de la autoridad certificadora se entendieran.

Los intentos por implementar PEM se abandonaron cuando el sistema de correo electrónico requirió extender el protocolo para soportar MIME, éste lo creó IETF en junio de 1992. Su objetivo es permitir a los clientes de e-mail enviar y recibir mensajes de texto plano y con formatos y figuras, ficheros ejecutables, sonidos, imágenes, etc. Aunque un mensaje MIME puede transportar un objeto PEM o un mensaje PEM puede transportar un objeto MIME, es mejor combinar los dos y proporcionar una solución uniforme en la que los protocolos funcionen de forma complementaria. Dicha combinación dio como resultado el desarrollo de MOSS, que es considerado como la inserción de PEM dentro de MIME.

MOSS proporciona autenticidad, integridad, confidencialidad y no repudiación de correo electrónico ni de la información anexa al correo. Se encuentra especificado en el RFC

1848 y es independiente del algoritmo de cifrado utilizado, aunque se recomienda usar MD2 y MD5, RSA como algoritmo de cifrado público y DES como algoritmo simétrico. MOSS soporta dos tipos de manejo de llaves X.509 y un manejo manual de llaves, lo cual representa una gran diferencia con respecto a PEM, que solo permitía X.509. Un punto importante a tomar en cuenta es que MOSS toma como entrada un objeto MIME y produce como salida otro igual. Además, RSA creó, en 1995, S/MIME, que está basado en el estándar PKCS 7 y la especificación MIME, para los mensajes, y en el formato X.509V.3, para los certificados, con el objetivo de prevenir intercepción y modificación de correos electrónicos. La propuesta se divide en cinco partes, la sintaxis criptográfica del mensaje (RFC 3852); los algoritmos de cifrado (RFC 3370); la especificación del mensaje ((RFC 3851); el manejo de certificados (RFC 3851) y la especificación del método para un acuerdo de llaves, basado en Diffie-Hellman (RFC 2631). La parte del mensaje que se desea proteger (firmada, cifrada o ambas) se envuelve en un paquete de datos, al cual se le aplican las operaciones necesarias y se inserta en una entidad MIME. Para que S/MIME pueda utilizarse, es necesario proporcionarle un certificado al usuario, sin embargo S/MIME no específica la forma de generarlo. El usuario puede obtenerlo a través de una PKI de su compañía o recurrir a alguna de las organizaciones que generan certificados personales o asociados a una dirección de correo electrónico.

4.4.2. Servicios de Seguridad en PEM

Incluye los servicios de:

1. Autenticación fuerte de origen
2. Integridad del mensaje
3. No repudio en el origen cuando se utiliza gestión de clave con algoritmo de clave asimétrica
4. Confidencialidad o privacidad.

Los tres primeros servicios se consiguen por medio de la firma digital. Para implementar la confidencialidad se hace uso del algoritmo simétrico DES: para cada mensaje se utiliza una clave DES que llamaremos de sesión. Se cifra el mensaje con esta clave y a continuación se envía encriptada con la clave secreta del destinatario. De esta manera se garantiza que sólo el destinatario puede recuperar la clave de sesión y leer el mensaje. En cualquiera de los casos (con o sin privacidad) tanto el mensaje como la firma y la clave de sesión se encapsulan en un formato imprimible (7 bits) que luego puede ser incluido en un mensaje RFC 822 o bien transmitido por cualquier otro medio.

Servicios de seguridad no contemplados:

1. Control de acceso
2. Confidencialidad del tráfico de mensajes
3. No repudio del mensaje por parte del receptor

4.4.3. Formato e Implementación PEM

PEM es compatible con otros modelos de mensajería como, por ejemplo, X.400.

PEM se implementa en el nivel de aplicación: es independiente de los protocolos de los niveles OSI o TCP/IP inferiores y es independiente de los sistemas operativos o del ordenador.

PEM se puede implementar como un módulo independiente que trabaje con el cliente de correo habitual para el usuario.

TIS/PEM

Plataformas UNIX. Trusted Information System. Código fuente disponible para los ciudadanos o empresas de Estados Unidos y Canadá. Usa una jerarquía de certificación múltiple.

RIPEM

Implementa parte de los protocolos PEM sin certificados para autenticación de claves. Gratuito para aplicaciones no comerciales. Exportación prohibida fuera de Estados Unidos. Existen versiones utilizadas en todo el mundo.

4.5. *PGP (PRETTY GOOD PRIVACY – PRIVACIDAD MUY BUENA)*

PGP es un esquema de uso extendido que no depende de ninguna organización o autoridad, por lo que es tan adecuado para el uso individual y personal como para la incorporación en configuraciones de red gestionadas por organizaciones.
PGP es un criptosistema (sistema de cifrado) que fue diseñado por Phil Zimmermann en 1991. Esta aplicación tiene como finalidad proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales. PGP es una aplicación de alta seguridad criptográfica que puede ser utilizada bajo varias plataformas (MSDOS, UNIX, etc.), y nos permite intercambiar archivos o mensajes proporcionando los servicios de confidencialidad y autentificación.

Básicamente, Zimmermann ha hecho lo siguiente:

1. Seleccionar los mejores algoritmos existentes.
2. Integrar estos algoritmos en una aplicación de propósito general independiente del sistema operativo y del procesador, y que se basa en un grupo reducido de comandos.
3. Ofrecer gratuitamente el paquete y su documentación, incluido el código fuente.
4. Proporcionar una versión comercial de PGP totalmente compatible y de bajo coste.

PGP ha crecido rápidamente debido a las siguientes razones:

1. Está disponible de forma gratuita, que se ejecutan en una gran variedad de plataformas (Windows, Unix, Macintosh, etc.)
2. Se basa en algoritmos que han sobrevivido a revisiones exhaustivas y se consideran sumamente seguros.
3. Tiene un amplio ámbito de aplicabilidad, desde corporaciones hasta particulares que desean comunicarse de forma segura con usuarios de todo el mundo.

4. No fue desarrollado por ninguna organización gubernamental o de estándares, ni lo controlan en la actualidad. Esto hace que PGP sea atractivo.
5. Está propuesto como estándar de Internet.

4.5.1 Descripción operativa

La operación real de PGP consiste en cinco servicios: autentificación, confidencialidad, compresión, compatibilidad con correo electrónico y segmentación.

Tabla 4.1 Resumen de los servicios de PGP

Función	***Algoritmos usados***	***Descripción***
Firma Digital	DSS / SHA o RSA / SHA	Se crea un código hash de un mensaje usando SHA-1. El resumen del mensaje se cifra usando DSS o RSA con la clave privada del emisor, y se incluye en el mensaje.
Cifrado de mensaje	CAST o IDEA o 3DES Diffie-Hellman o RSA	Se cifra un mensaje usando CAST-128, IDEA o 3DES con una clave de sesión de un solo uso generada por el emisor. La clave de sesión se cifra usando Diffie-Hellman o RSA con la clave pública del receptor, y se incluye en el mensaje.
Compresión	ZIP	Un mensaje se puede comprimir usando ZIP para su almacenamiento o transmisión.
Compatibilidad con correo electrónico	Conversión radix 64	Para proporcionar transparencia para las aplicaciones de correo electrónico, un mensaje cifrado se puede convertir en una ristra ASCII usando conversión radix 64.
Segmentación	-	Para ajustarse a las limitaciones de tamaño de mensaje, PGP realiza la segmentación y el reensamblado.

Autentificación

La figura 4.1 ilustra el servicio de firma digital suministrado por PGP.

1. El emisor crea un mensaje.
2. Se usa SHA-1 para generar un código *hash* del mensaje de 160 bits.
3. El código *hash* se cifra con RSA usando la clave privada del emisor y el resultado se añade antepuesto al mensaje.
4. El receptor usa RSA con la clave pública del emisor para descifrar y recuperar el código *hash*.
5. El receptor genera un nuevo código *hash* para el mensaje y lo compara con el código *hash* descifrado. Si los dos coinciden, el mensaje se considera auténtico y se acepta.

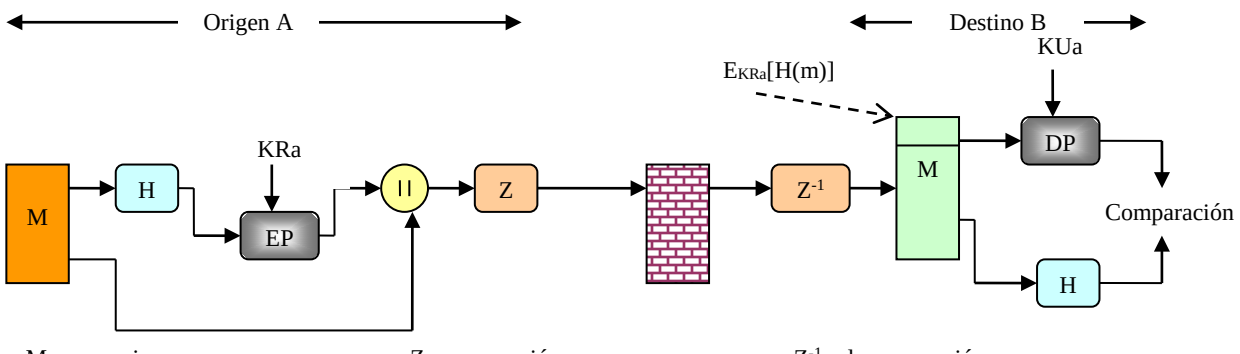


Figura 4.1 Función criptográfica PGP, solo autentificación

La combinación de SHA-1 y RSA ofrece un esquema eficaz de firma digital. Por una parte, debido al RSA, el receptor está seguro de que sólo el proveedor de la clave privada correspondiente puede generar la firma. Por otro lado, debido al SHA-1, el receptor está seguro de que nadie más puede generar un nuevo mensaje que coincida con el código *hash* y con la firma del mensaje original.

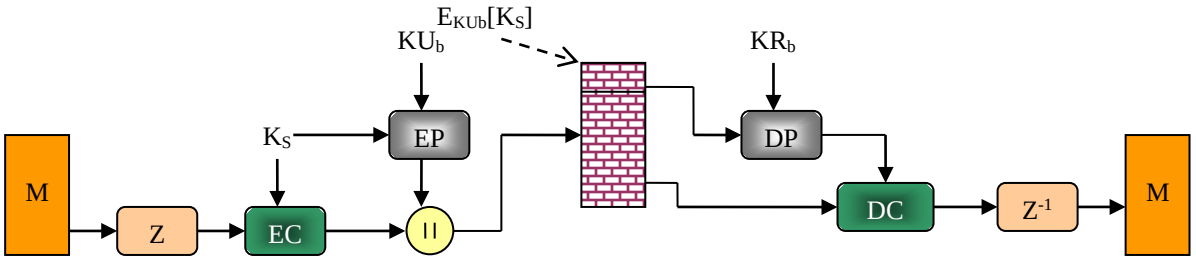
Aunque las firmas se encuentran normalmente adjuntas al mensaje o al fichero que firman, no siempre es así: también pueden encontrarse separadas. Una firma puede almacenarse y transmitirse separada del mensaje que firma. Un usuario podría desear mantener un fichero de seguimiento con las firmas separadas de todos los mensajes enviados y recibidos. Además, una firma separada de un programa ejecutable pede detectar un virus. Por último, las firmas separadas se pueden usar cuando más de una parte debe firmar el documento. La firma de cada persona es independiente y se aplica sólo al documento.

Confidencialidad

La confidencialidad se consigue cifrando los mensajes que van a transmitirse o a almacenarse localmente como ficheros. En ambos casos se puede usar el algoritmo de cifrado simétrico CAST-128, IDEA o 3DES utilizando siempre el modo CFB de 64 bits.

Como es habitual, se debe enfrentar el problema de la distribución de claves. En PGP cada clave simétrica se usa una sola vez. Es decir, una nueva clave se genera como un número aleatorio de 128 bits para cada mensaje. Así, aunque a esta se le conoce en la documentación como clave de sesión, en realidad se trata de una clave de un solo uso. Como ha de usarse una sola vez, la clave de sesión se añade al mensaje y se transmite con él. Para proteger la clave, se cifra con la clave pública del receptor. En la figura 4.2 muestra la secuencia que se puede describir de la siguiente manera:

1. El emisor genera un mensaje y un número aleatorio de 128 bits para usarlo como clave de sesión sólo para este mensaje.
2. El mensaje se cifra, usando CAST-128 o IDEA o 3DES, con la clave de sesión.
3. La clave de sesión se cifra con RSA, usando la clave pública del receptor, y se añade antepuesta al mensaje.
4. El receptor usa RSA con su clave privada para descifrar y recuperar la clave de sesión.
5. La clave de sesión se usa para descifrar el mensaje.



M – mensaje
EC – cifrado simétrico
DC – descifrado simétrico
Ks – clave de sesión

Z – compresión
| | - concatenación
EP – cifrado de clave pública
DP – descifrado de clave pública

Z^{-1} – descompresión

Figura 4.2 Función criptográfica PGP, solo confidencialidad

Como alternativa al uso del RSA para el cifrado de la clave, PGP proporciona la opción conocida como Diffie-Hellman (algoritmo de intercambio de claves). De hecho, PGP es una variante de Diffie-Hellman que proporciona cifrado/descifrado, conocido como El Gamal.

Se pueden hacer algunas observaciones al respecto. En primer lugar, para reducir el tiempo de cifrado es preferible usar la combinación de cifrado simétrico y de clave pública que usar simplemente RSA o El Gamal para cifrar el mensaje directamente: CAST-128 y los demás algoritmos simétricos son sensiblemente más rápidos que RSA o El Gamal. Por otra parte, el uso del algoritmo de clave pública resuelve el problema de la distribución de las claves de sesión, porque sólo el receptor puede recuperar la clave de sesión que va unida al mensaje. Cada mensaje consiste en un elemento único e independiente con su propia clave. Además, dado que el correo electrónico se almacena y se reenvía, no son prácticas las negociaciones para garantizar que las dos partes que se comunican tienen la misma clave de sesión. Por último, el empleo de claves simétricas de un solo uso refuerza lo que ya es un enfoque robustote cifrado simétrico. Sólo se cifra una pequeña cantidad de texto claro con cada clave y no existe relación entre las claves. Así, hasta donde el algoritmo de clave pública es seguro, el esquema total es seguro.

Confidencialidad y Autentificación

Ambos servicios se pueden usar para el mismo mensaje. Primero se genera una firma para el mensaje en texto claro y se adjunta antepuesta a dicho mensaje. Luego, se cifra el mensaje en texto claro y la firma usando CAST-128 (o IDEA o 3DES), y la clave de sesión se cifra usando RSA (o El Gamal). Esta secuencia es preferible a la secuencia inversa, que consistiría en cifrar el mensaje y luego generar una firma para el mensaje cifrado. Generalmente, es más conveniente almacenar una firma con una versión en texto claro del mensaje. Además, para la verificación de la tercera parte, si la firma se lleva a cabo en primer lugar, la tercera parte no necesita ocuparse de la clave simétrica al verificar la firma.

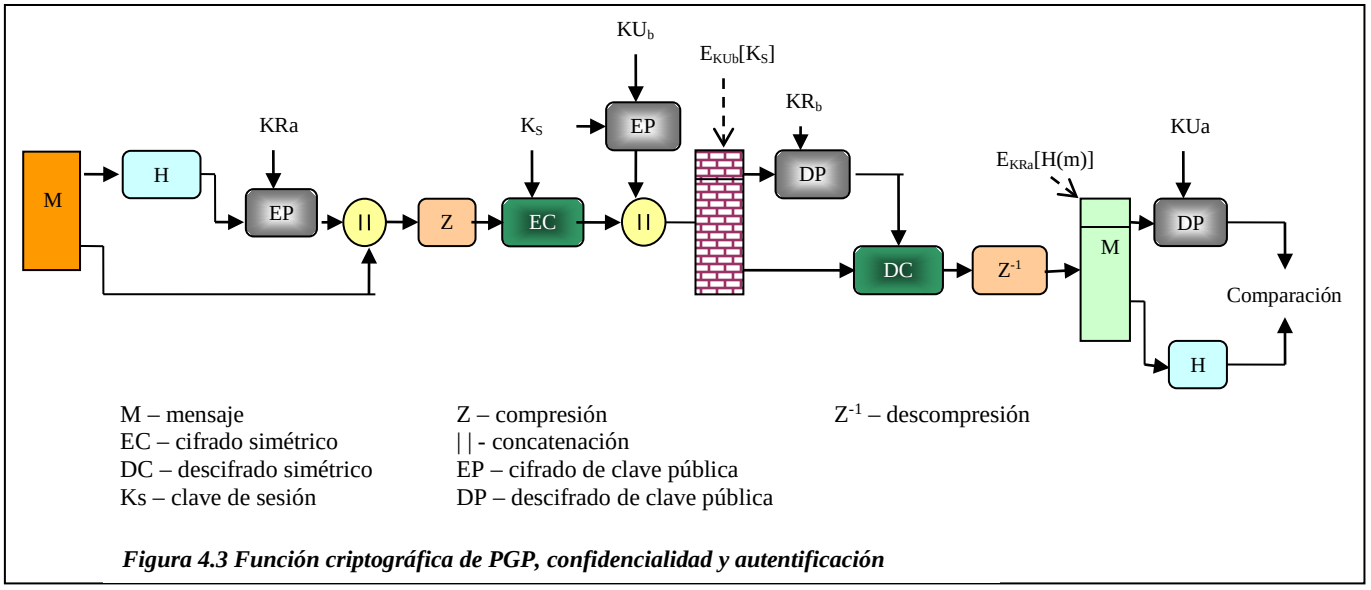


Figura 4.3 Función criptográfica de PGP, confidencialidad y autentificación

En resumen, cuando se usan los dos servicios, primero el emisor firma el mensaje con su propia clave privada, luego cifra el mensaje con una clave de sesión y a continuación cifra la clave de sesión con la clave pública del receptor.

Compresión

PGP comprime el mensaje después de aplicar la firma, pero antes del cifrado. Esto tiene la ventaja de ahorrar espacio tanto para la transmisión de correo electrónico como para el almacenamiento de ficheros.

La ubicación del algoritmo de compresión es crítica:

1. La firma se genera antes de la compresión debido a dos razones fundamentales:
    a. Es preferible firmar un mensaje descomprimido para poder almacenar solamente el mensaje descomprimido junto con la firma para su verificación posterior. Si se firma un documento comprimido, será necesario almacenar una versión comprimida del mensaje para su posterior verificación o volver a comprimir el mensaje cuando se requiera verificación.

    b. Incluso si se estuviese dispuesto a generar de forma dinámica un mensaje que se ha vuelto a comprimir para su verificación, el algoritmo de compresión de PGP presenta una dificultad. El algoritmo no es determinista; distintas implementaciones permiten diferentes compromisos entre la velocidad de ejecución y el ratio de compresión y, como resultado, producen distintas formas comprimidas. Sin embargo, los distintos algoritmos de compresión pueden operar entre sí, ya que cualquier versión del algoritmo puede descomprimir correctamente la salida de cualquier otra versión. Aplicar la función hash y la firma después de la compresión restringiría todas las implementaciones de PGP a la misma versión del algoritmo de compresión.

2. El cifrado del mensaje se aplica después de la compresión para reforzar la seguridad criptográfica. Como el mensaje comprimido tiene menos redundancia que el texto claro original. El criptoanálisis presenta más dificultades.

Compatibilidad con correo electrónico

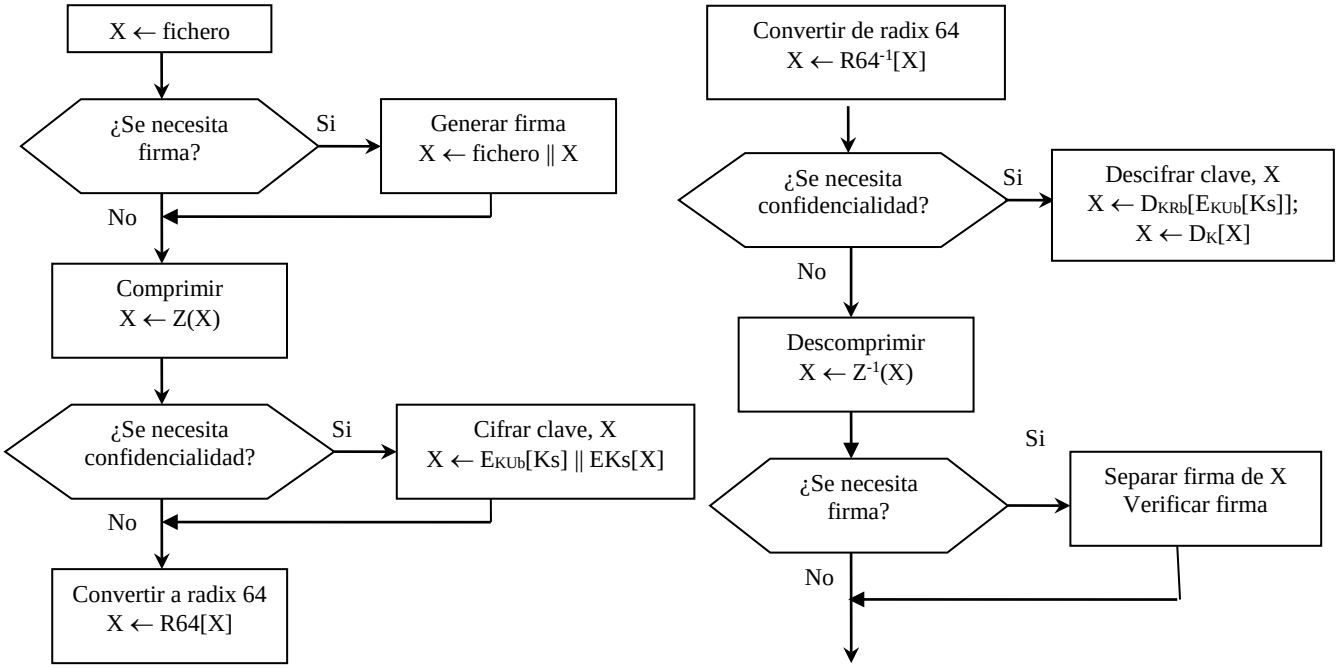
Cuando se usa PGP, se cifra al menos una parte del bloque que se va a transmitir. Si sólo se usa el servicio de firma, se cifra el resumen del mensaje (con la clave privada del emisor). Si se usa el servicio de confidencialidad, se cifran (con una clave simétrica de un solo uso) el mensaje y la firma (si estuviese presente). Por consiguiente, parte del bloque resultante consiste en una ristra de octetos arbitrarios de ocho bits. Sin embargo, muchos sistemas de correo electrónico sólo permiten el uso de bloques de texto ASCII. Para ajustarse a esta restricción, PGP proporciona el servicio de convertir la ristra binaria de ocho bits en una ristra de caracteres ASCII imprimibles.

El esquema que se usa para ello es la conversión radix 64. A partir de cada grupo de tres octetos de datos binarios se obtienen cuatro caracteres ASCII. El uso de radix 64 expande un mensaje un 33%. Afortunadamente, las partes del mensaje correspondientes a la clave de sesión y a la firma son relativamente compactas, y el mensaje en texto claro ha sido comprimido. De hecho, la compresión debería ser más que suficiente para compensar la expansión de radix 64.

Un aspecto destacable del algoritmo radix 64 es que convierte la ristra de entrada a formato radix 64 independientemente del contenido, incluso si la entrada es texto ASCII. Por consiguiente, Si un mensaje está firmado, pero no cifrado, y la conversión se aplica al bloque completo, la salida será ilegible al observador casual, lo cual proporciona un cierto grado de confidencialidad. De manera opcional, PGP puede configurarse para convertir a formato radix 64 sólo la parte de la firma de los mensajes firmados en texto claro. Esto permite que el receptor humano lea el mensaje sin usar PGP. Sin embargo, aún tendría que usarse PGP para verificar la firma.

La figura 4.4 muestra la relación entre los primeros cuatro servicios. En la transmisión, si es necesario, se genera una firma usando un código hash del texto claro descomprimido. Luego se comprime el texto claro y, si está presente, también la firma. A continuación, si se necesita confidencialidad, se cifra el bloque (texto claro

comprimido o firma comprimida más texto claro) y se añade antepuesto con la clave de cifrado simétrico cifrada con clave pública. Por último, l bloque completo se convierte a formato radix 64.



a) Diagrama genérico de transmisión ***b) Diagrama genérico de recepción***

Figura. 4.4 Transmisión y recepción de mensajes PGP

En la recepción, el bloque que se recibe se convierte de formato radix 64 nuevamente a binario Luego, si el mensaje está cifrado, el receptor recupera la clave de sesión y descifra el mensaje. El bloque resultante, luego, se descomprime. Si el mensaje está firmado, el receptor recupera el código hash transmitido y lo compararon su propio cálculo del código hash.

Segmentación y Reensamblado

Las herramientas de correo electrónico se limitan con frecuencia a una longitud máxima de mensaje. Por ejemplo, muchas de las herramientas accesibles a través de Internet imponen una longitud máxima de 50,000 octetos. Cualquier mensaje mayor debe subdividirse en segmentos más reducidos, cada uno de los cuales se envía por separado.

Para ajustarse a esta restricción, PGP subdivide automáticamente los mensajes demasiado largos en segmentos lo suficientemente cortos para ser enviados por correo electrónico. La segmentación se lleva a cabo después de todo el procesamiento, incluida la conversión de radix 64. Por lo tanto, el componente clave de sesión y el componente firma aparecen una sola vez, al principio del primer segmento. En el extremo receptor, PGP debe retirar todas las cabeceras del correo electrónico y reensamblar el bloque original completo antes de realizar los pasos de la figura 4.4 b).

Claves criptográficas y Ficheros de claves

PGP hace uso de cuatro claves: claves simétricas de sesión de un solo uso, claves públicas, claves privadas y claves simétricas basadas en frases clave (que se explicarán más adelante). Con respecto a estas claves, se pueden identificar tres requisitos:

1. Se necesita un medio para la generación imprevisible de claves de sesión.
2. Nos gustaría permitir que un usuario tenga múltiples parejas de clave pública/clave privada. El motivo de esto es que el usuario podría querer cambiar su pareja de claves de vez en cuando. Cuando esto ocurre, cualquier mensaje en proceso se creará con una clave obsoleta. Además, los receptores sólo conocerán la clave pública antigua hasta recibir una actualización. Aparte de la necesidad de cambiar las claves de vez en cuando, un usuario podría querer

tener múltiples parejas de claves en un momento dado para interactuar con diferentes grupos de interlocutores o simplemente para mejorar la seguridad limitando la cantidad de material cifrado con una de las claves. El resultado de todo esto esto es que no hay una correspondencia de uno a uno entre los usuarios y sus claves públicas. Por lo tanto, se necesita algún medio para identificar claves particulares.

3. Cada entidad PGP debe mantener un archivo con sus propias parejas de claves y otro con las claves públicas de los interlocutores.

Generación de claves de sesión

Cada clave de sesión está asociada a un solo mensaje y se usa sólo con el fin de cifrar y descifrar ese mensaje. Recordemos que el cifrado/descifrado de mensajes se realiza con un algoritmo de cifrado simétrico. CAST-128 e IDEA usan claves de 128 bits; 3DES usa una de 168 bits.

La entrada al generador de números aleatorios consiste en una clave de 128 bits y dos bloques de 64 bits que se tratan como texto claro que se va a cifrar. Usando el modo de realimentación de cifrado, el cifrador produce dos bloques de texto cifrado de 64 bits, que se concatenan para formar la clave de sesión de 128 bits.

La entrada “texto claro” al generador de números aleatorios, que consiste en dos bloques de 64 bits, procede de una ristra de números generados de forma aleatoria de 128 bits. Estos números se basan en entradas de pulsaciones de teclas por parte del usuario. El tiempo de pulsación y las teclas pulsadas se usan para generar la ristra aleatoria. Por lo tanto, si el usuario pulsa teclas arbitrarias a su ritmo normal, se generará una entrada razonablemente “aleatoria”. Esta entrada aleatoria también se combina con la salida de la clave de sesión anterior del algoritmo para formar la entrada de la clave al generador. El resultado de la alteración es producir una secuencia de claves de sesión efectivamente impredecible.

Identificadores de clave

Un mensaje cifrado está acompañado de una forma cifrada de la clave de sesión que se empleó. La clave de sesión se cifra con la clave pública del receptor. Así, sólo el receptor podrá recuperar la clave de sesión y, por consiguiente, el mensaje. Si cada usuario utilizó una única pareja de claves pública/privada, el receptor debería saber automáticamente qué clave usar para descifrar la clave de sesión: la clave privada única del receptor. Sin embargo, no olvidemos el requisito de que cualquier usuario dado podría tener múltiples parejas de claves.

Entonces, ¿cómo sabe el receptor cuál de sus claves públicas se usó para cifrar la clave de sesión? Una solución simple sería transmitir la clave pública con el mensaje. Entonces, el receptor podría verificar que efectivamente se trata de una de sus claves públicas y continuar. Este esquema funcionaría, pero constituye un gasto innecesario de espacio. Una clave pública RSA podría tener una longitud de cientos de dígitos decimales. Otra solución sería asociar un identificador a cada clave pública que sea única al menos en un usuario. Es decir, la combinación del identificador del usuario (user ID) y el identificador de clave (key ID) sería suficiente para identificar una clave en especial. Entonces, sólo sería necesario transmitir el identificador de clave más corto. Sin embargo, esta solución trae un problema de gestión y de costes adicionales: los identificadores de clave deben ser asignados y almacenados para que tanto el emisor como el receptor puedan establecer la relación entre identificador de clave y clave pública.

La solución adoptada por PGP es la de asignar un identificador de clave a cada clave pública que, con un gran índice de probabilidad, es única en el identificador de un usuario. El identificador de clave asociado con cada clave pública consiste en sus 64 bits menos significativos. Es decir, l identificador de clave pública KU_a es (KU_a mod 2^{64}). Esta es una longitud suficiente para que la probabilidad de duplicación de identificadores de clave sea muy pequeña.

También se necesita un identificador de clave para la firma digital PGP. Como un emisor puede usar una clave privada, de una serie de claves privadas, para cifrar el resumen del mensaje, el receptor debe saber que clave pública se debe usar. Por lo tanto, el componente firma digital de un mensaje incluye el identificador de clave de 64 bits de la clave pública que se requiere. Cuando se recibe el mensaje, el receptor verifica que el identificador de clave es el de una clave pública para ese emisor y entonces procede a verificar la firma.

Podemos observar el formato de un mensaje transmitido, que se muestra en la figura 4.5. Un mensaje está formado por tres componentes: el componente de mensaje, los componentes de firma (opcional) y el componente de clave de sesión.

El **componente mensaje** incluye los datos reales que se van a almacenar o transmitir, así como un nombre de archivo y un sello de tiempo que especifica el momento de creación.

El **componente firma** incluye lo siguiente:

- ✓ **Sello de tiempo:** el momento en que se creó la firma.
- ✓ **Resumen de mensaje:** el resumen SHA-1 de 160 bits, cifrado con la clave de firma privada del emisor. El resumen se calcula con el sello de tiempo de la firma concatenado con la parte de datos del componente de mensaje. La inclusión del sello de tiempo de la firma en el resumen evita los ataques de repetición. La exclusión de las partes del nombre del archivo y sello de tiempo del componente de mensaje garantiza que las firmas adjuntas son exactamente las mismas que las firmas adjuntas antepuestas al mensaje. Las firmas separadas se calculan en un fichero separado que no tiene ninguno de los campos de cabecera del componente de mensaje.
- ✓ **Dos octetos iniciales del resumen del mensaje:** para permitir que el receptor determine si se usó la clave pública correcta para descifrar el resumen del mensaje para la autentificación, se compara la copia en texto claro de los dos primeros octetos con los dos primeros octetos del resumen

descifrado. Estos octetos también sirven de comprobación del marco de 16 bits para el mensaje.

- ✓ **Identificador de clave de la clave pública del emisor:** identifica la clave pública que debería usarse para descifrar el resumen del mensaje y, por lo tanto, identifica la clave privada que se utilizó para cifrar el resumen del mensaje.

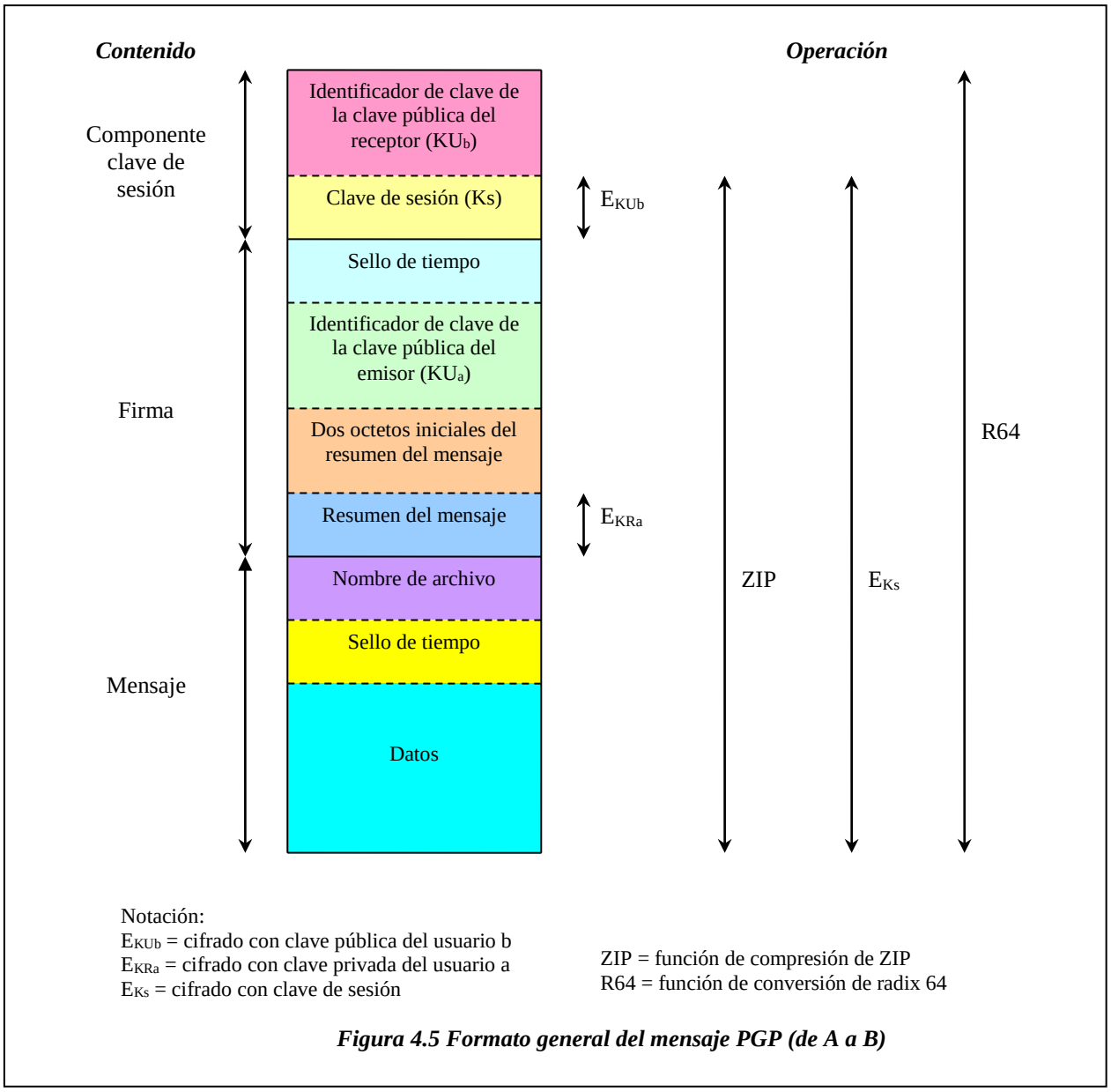


Figura 4.5 Formato general del mensaje PGP (de A a B)

El componente de mensaje y el componente opcional de firma pueden comprimirse usando ZIP y pueden cifrarse usando una clave de sesión.
El **componente clave de sesión** incluye la clave de sesión y el identificador de la clave pública del receptor que utilizó el emisor para cifrar la clave de sesión.

El bloque completo se codifica normalmente con radix 64.

Ficheros de claves

Se ha comprobado que los identificadores de clave son críticos para la operación de PGP y en cualquier mensaje PGP que proporcione confidencialidad y autentificación se incluyen dos identificadores de clave. Es necesario almacenar y organizar estas claves de forma sistemática para que todas las partes las usen de forma eficaz y efectiva.
El esquema usado en PGP es el de proporcionar un par de estructuras de datos en cada nodo, una para almacenar las parejas de claves pública/privada pertenecientes a ese nodo, y otra parte almacenar las claves públicas de otros usuarios conocidos en ese nodo. Estas estructuras de datos se conocen como fichero de claves privadas y fichero de claves públicas.

La estructura general de un ***fichero de claves privadas*** contiene las siguientes entradas:

- ✓ **Sello de tiempo:** fecha y hora en que se generó la pareja de claves.
- ✓ **Identificador de clave:** los 64 bits menos significativos de la clave pública para esa entrada.
- ✓ **Clave pública:** la parte de la clave pública de la pareja en cuestión.
- ✓ **Clave privada:** la parte de clave privada de la pareja en cuestión; este campo está cifrado.
- ✓ **Identificador de usuario:** es la dirección de correo electrónico del usuario, el usuario puede elegir un nombre diferente o reutilizar el mismo identificador de usuario más de una vez.

El fichero de claves privadas se puede indexar por el identificador de usuario o el identificador de clave. Aunque se intenta que el fichero de claves privadas se almacene sólo en la máquina de usuario que creó y posee la pareja de claves, y que sólo ese usuario pueda acceder a él, tiene sentido hacer que el valor de la clave privada sea lo más seguro posible. Por los tanto, la clave privada no se almacena en el fichero de claves. En vez de eso, la clave se cifra tomando en cuenta el procedimiento siguiente:

1. El usuario elige una frase clave para el cifrado de claves privadas.
2. Cuando el sistema genera una nueva pareja de claves pública/privada usando RSA, pide la frase clave al usuario. Usando SHA-1, se genera un código hash de 160 bits a partir de la frase clave, y la frase clave se descarta.
3. El sistema cifra la clave privada usando CAST-128 o IDEA o 3DES con los 160 bits como clave. Luego el código hash se descarta, y la clave privada cifrada se almacena en el fichero de claves privadas.

Posteriormente, cuando un usuario accede al fichero de claves privadas para recuperar una clave privada, debe suministrar la frase clave. PGP recuperará la clave privada cifrada, generará el código hash de la frase clave y descifrará la clave privada cifrada usando CAST-128 o IDEA o 3DES (según el utilizado) con el código hash. Como cualquier sistema que se basa en contraseñas, la seguridad de este sistema depende de la seguridad de la contraseña. El usuario deberá utilizar una frase clave que no sea fácil de adivinar, pero sí fácil de recordar.

La estructura general de un ***fichero de claves públicas*** contiene las siguientes entradas:

- ✓ **Sello de tiempo:** fecha y hora en que se generó la entrada.
- ✓ **Identificador de clave:** los 64 bits menos significativos de la clave pública para esta entrada.
- ✓ **Clave pública:** clave pública para esta entrada.
- ✓ **Identificador de usuario:** identifica al propietario de la clave. Varios identificadores de usuario pueden estar asociados a una sola clave pública.

El fichero de claves públicas se puede indexar por el identificador de usuario o de clave.

¿Cómo se usan los ficheros de claves en la transmisión y recepción de mensajes?

En la figura 4.6, la entidad PGP emisora realiza los siguientes pasos:

1. Firmar el mensaje.
    a. PGP recupera la clave privada del emisor del fichero de claves privadas usando un *identificador de usuario* como índice. Si su identificador de usuario no se proporcionó, se recupera la primera clave del fichero.
    b. PGP solicita al usuario la frase clave para recuperar la clave privada que no está cifrada.
    c. Se construye el componente de firma del mensaje.
2. Cifrar el mensaje.
    a. PGP genera una clave de sesión y cifra el mensaje.
    b. PGP recupera la clave pública del receptor del fichero de claves públicas usando su identificador de usuario como índice.
    c. Se construye el componente de clave de sesión del mensaje.

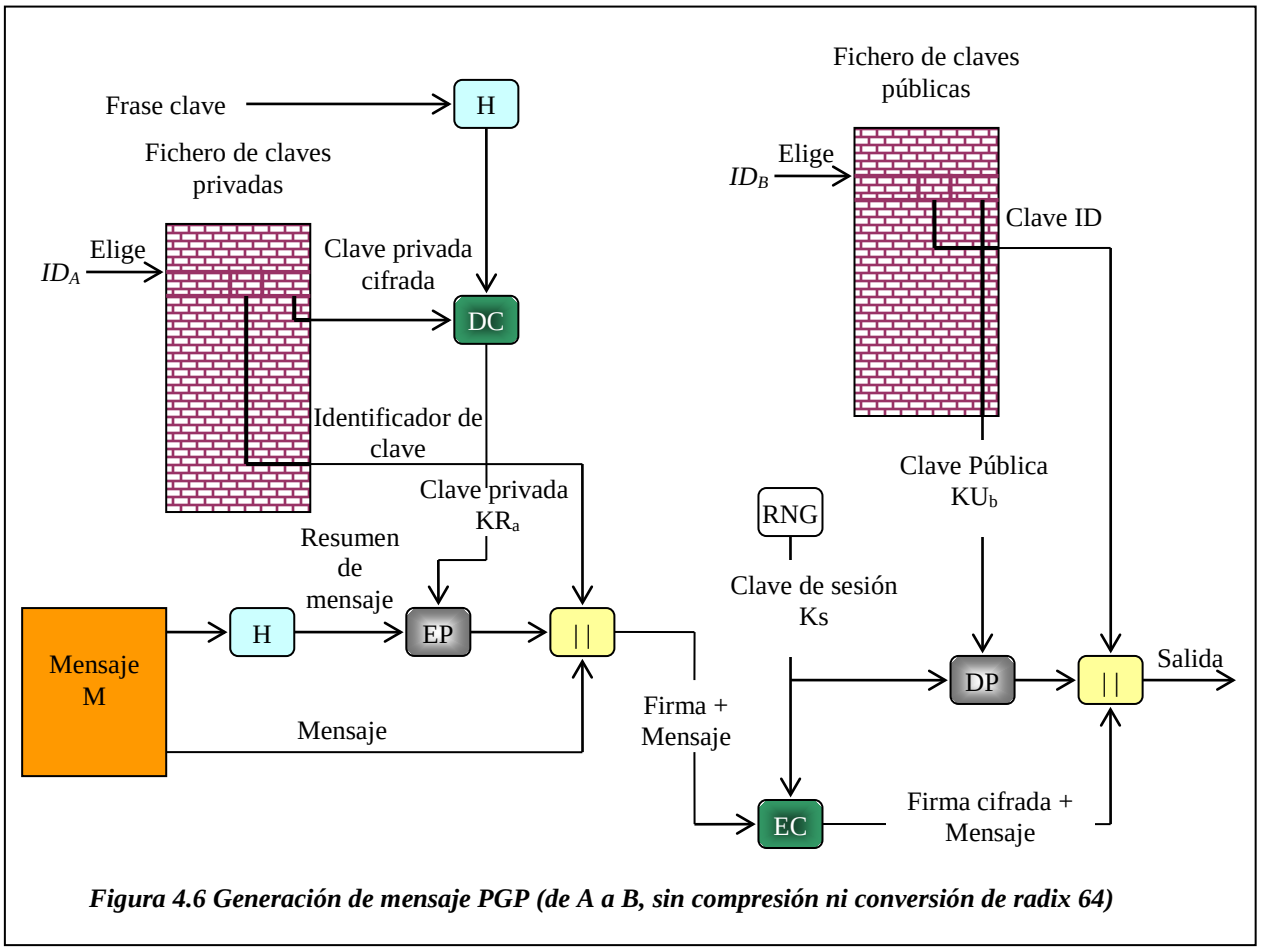


Figura 4.6 Generación de mensaje PGP (de A a B, sin compresión ni conversión de radix 64)

En la figura 4.7, la entidad PGP receptora realiza los siguientes pasos:

1. Descifrar el mensaje.
    a. PGP recupera la clave privada del receptor seleccionada del fichero de claves privadas, usando como índice el campo identificador de clave del componente clave de sesión del mensaje.
    b. PGP pide al usuario la frase clave para recuperar la clave privada sin cifrar.
    c. Luego, PGP recupera la clave de sesión y descifra el mensaje.
2. Autentificar el mensaje.

a. PGP recupera la clave pública del emisor del ficherote claves públicas, usando como índice el campo identificador de clave en el componente de clave de firma del mensaje.
b. PGP recupera el resumen del mensaje transmitido.
c. PGP calcula el resumen de mensaje para el mensaje recibido y lo compara con el resumen de mensaje transmitido para autentificar.

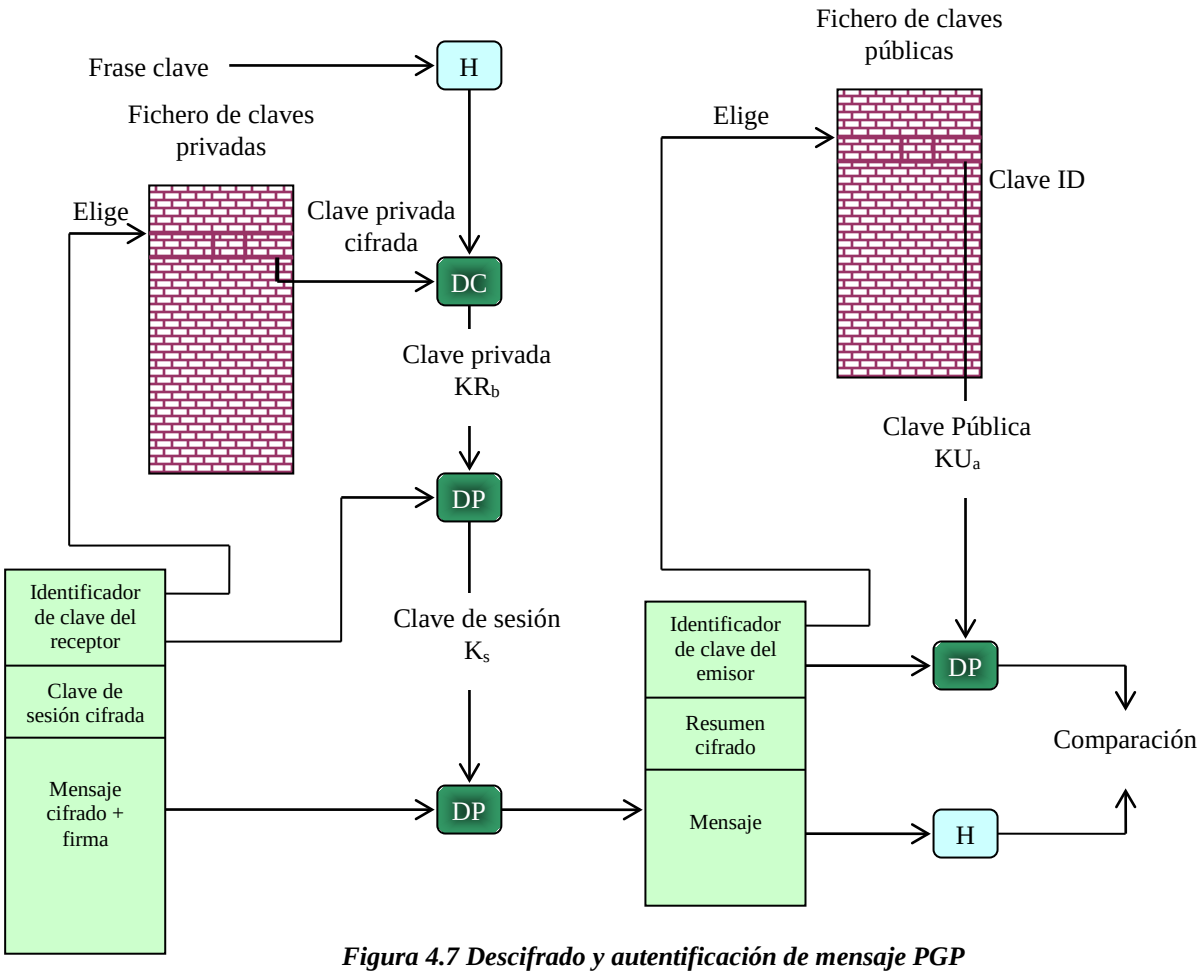


Figura 4.7 Descifrado y autentificación de mensaje PGP

4.5.2 Algoritmos que utiliza el Standard PGP

PGP emplea tres algoritmos de encriptado: RSA (generador de clave pública), IDEA (generador de clave única), y el MD5 (función hash); combinados de tal forma que se logra conseguir la máxima seguridad y la mayor rapidez y comodidad.
Además PGP, se pueden implementar en algoritmos de compresión y descompresión como: ZIP

Algoritmo RSA

Su seguridad se basa en la pertenencia al grupo de los problemas difíciles de la clase números primos (NP) del problema de factorización de números grandes. La clave pública y la privada están en función de un par de números primos grandes (de 100 o 200 dígitos).
Para hallar la clave privada supondría encontrar por factorización los dos números primos que la forman, esto es aun imposible para claves de al menos 1024 bits.

Genera las claves utilizando números aleatorios primos grandes.
Calcular n = p*q
Elegir clave de encriptación e, de manera que el máximo común divisor de e y (p-1)*(q-1) sea 1
Calcular clave de descifrado, d, d = e-1 mod ((p-1)*(q-1))
/**n* y *e* son son la clave publica, d clave privada*/
Para encriptar un mensaje m, divide en bloques numéricos M_i menores que n
La fórmula de encriptación es: $c_i = M_i e \bmod n$
Para desencriptar, se toma cada bloque ci y se calcula: $m_i = c_i d \bmod n$

Algoritmo IDEA

El algoritmo de clave única IDEA utiliza texto en bloques de 64 bits y una clave de 128 bits. Ha sido diseñado de tal forma que el proceso de encriptado consiste en ocho pasos de encriptación que son idénticos excepto en los subloques de la clave, terminando con una transformación de la salida.

En cada paso se utilizan tres operaciones:

1. Suma modular con módulo 2^{16}
2. Multiplicación modular con módulo $2^{16}+1$
3. OR exclusivo

La figura 4.8 detalla el algoritmo por ronda.

Hacer 8 rondas:
En cada ronda se divide el bloque de 64 bits en cuatro sub bloques de 16 bits.
Combinar estos con operaciones entre si con 6 sub-bloques de 16 bits de la clave.
Cambiar de posición a los bloques 2 y 3 en cada ronda.
Por ultimo se combinan los 4 sub-bloques con 4 subclaves.

Pasos en cada ronda:

1. Multiplicar el primer sub-bloque y la primera subclave.
2. Sumar el segundo sub-bloque y la segunda subclave.
3. Sumar el tercer sub-bloque y la tercera subclave.
4. Multiplicar el cuarto sub-bloque y cuarta subclave.
5. Calcular el XOR de los pasos 1 y 3.
6. Calcular el XOR de los pasos 2 y 4.
7. Multiplicar los resultados del paso 5 y la quinta subclave.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar los resultados del paso 8 y la sexta subclave.
10. Sumar los resultados los pasos 7 y 9.

11. * Calcular el XOR de los pasos 1 y 9.
12. * Calcular el XOR de los pasos 3 y 9.
13. * Calcular el XOR de los pasos 2 y 10.
14. * Calcular el XOR de los pasos 4 y 10.

La salida producida por la ronda son los 4 sub-bloques resultado de los pasos marcados con *.

Cambiar el bloque 2 por el 3, excepto en la última ronda, ésta será la entrada de la siguiente ronda.

Transformación final de la salida en la octava ronda:

1. Multiplicar X1 y la primera subclave.
2. Sumar X2 y la segunda subclave.
3. Sumar X3 y la tercera subclave.
4. Multiplicar X4 y cuarta subclave.

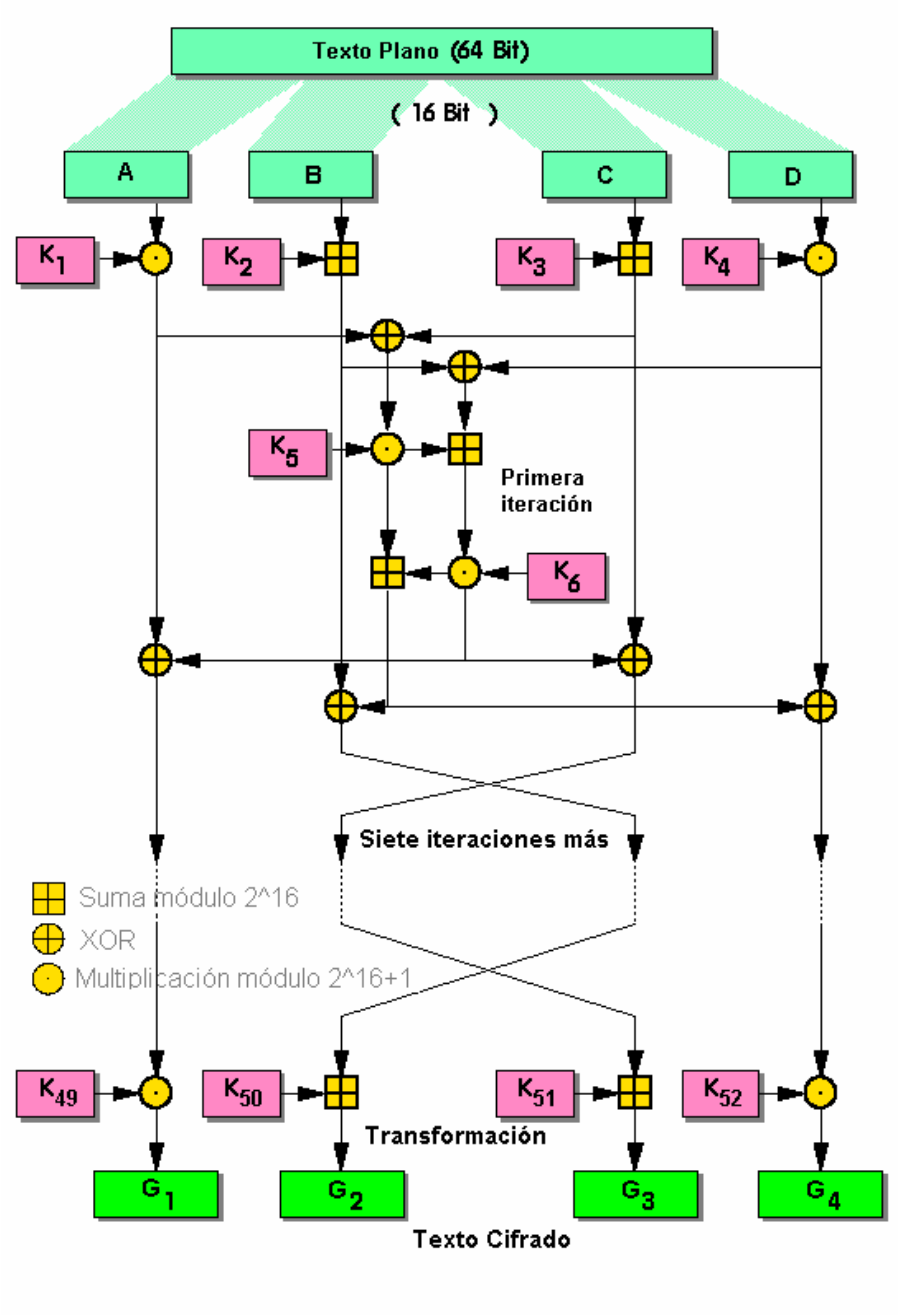
El algoritmo emplea 52 subclaves, que son creadas dividiendo la clave de 128 bits en ocho subclaves de 16 bits. Éstas son las 8 primeras subclaves del algoritmo.

Se rotan 25 bits de la clave hacia la izquierda y de nuevo se divide en 8 subclaves.

Se realiza otra rotación de 25 bits a la izquierda y se vuelve a dividir en ocho subclaves.

Esto se divide hasta finalizar el algoritmo.

El proceso de descifrado es similar el mismo que el de encriptación, con la diferencia de que las 52 subclaves son las inversas de las empleadas en la encriptación respecto de la operación, este proceso se utiliza en orden inverso.


Texto Plano (64 Bit)
(16 Bit)
A
B
C
D
K1
K2
K3
K4
K5
Primera iteración
K6
Siete iteraciones más
Suma módulo 2^16
XOR
Multiplicación módulo 2^16+1
K49
K50
K51
K52
Transformación
G1
G2
G3
G4
Texto Cifrado

Algoritmo MD5

Se comienza suponiendo que se tiene un mensaje de b bits de longitud, escritos m0, m1,...m(b-1).

El algoritmo tiene cinco pasos.

1. Adición de bits de relleno.

   El mensaje es rellenado con n bits, de tal manera que le falte a su longitud 64 bits para ser múltiplo de 512. El primer de los n bits es 1 y el resto son 0.

2. Adición de la longitud.

   La nueva longitud es una representación de 64 bits y es añadida en forma de dos palabras de 32 bits, en primer lugar se muestran los bits menos significativos. Si la longitud del mensaje es mayor que 264, se usan los 64 bits menos significativos.

3. Inicializar los cuatro bufferes, A,B,C y D, que son registros de 32 bits. Inicializados con los siguientes valores:

   A: 01 23 45 67

   B: 89 ab cd ef

   C: fe dc ba 98

   D: 76 54 32 10

4. Procesar el mensaje en bloques de 16 bits (se tendra una entrada y salida de 32 bits).

   F(X,Y,Z) = (X AND Y) OR ((NOT(X)) AND Z)

   G(X,Y,Z) = (X AND Z) OR (Y AND (NOT(Z))

   H(X,Y,Z) = X XOR Y XOR Z

   I(X,Y,Z) = Y XOR (X OR (NOT(Z)))

Se usa una tabla de 64 elementos T[1 ... 64] construida con la función seno, siendo Ti la parte entera de
294967296 * abs(sen(i)) (i en radianes).

5. Salida. Mensaje producido por A, B, C, D, empezando con los bits menos significativos de A y terminando con los más significativos de D. Independientemente de la longitud del mensaje, su tamaño será de 128 bits.

4.5.3 Consideraciones de Seguridad de los Algoritmos y PGP en general.

Seguridad RSA

La seguridad de RSA se basa totalmente en el problema de factorización de números grandes, como se ha mencionado es virtualmente imposible, descifrar claves de al menos 1024 bits. Otra opción posible es atacar RSA descubriendo el valor (p-1)*(q-1), pero este ataque equivale a una factorización de n. Otra forma de ataque es el de fuerza bruta probando cualquier d (clave privada) posible hasta dar con el valor correcto, pero es un ataque aún menos eficiente.

Seguridad IDEA

La longitud de la clave de IDEA es de 128 bits. Un ataque de fuerza bruta no es eficiente, ya que haría falta calcular 2128 (1038) encriptaciones para encontrar la clave.(Si se lograra diseñar un chip que probara mil millones de claves por segundo y se fabricaran mil millones de ellos, aún harían falta 1013 años - más que la edad del Universo. Con 1024 chips como éste se podría encontrar la clave en un día, pero no hay suficientes átomos de silicio en el Universo para construirlos). Los ataques basados en criptoanálisis, sólo unos pocos estudios, como el de Willi Meier, han logrado ataques más eficientes que el de fuerza bruta (empleando 242 operaciones). John Daemen descubrió algunas claves débiles de IDEA, pero la posibilidad de generar aleatoriamente alguna de estas claves es de 1/296.

Seguridad de MD5

Berson trató de utilizar el criptoanálisis diferencial contra una sola ronda de MD5, su ataque no es efectivo contra las cuatro rondas. Un ataque más efectivo es de Boer y Bosselaers, se producen colisiones en la función de compresión. En principio, esto no tendría un impacto práctico en la seguridad del hash, aunque se pudiera explotar esta debilidad, no afectaría a la seguridad de la encriptación, sino a la veracidad de las firmas digitales.

UNIDAD V: ASPECTOS SOCIALES

Internet y su tecnología de seguridad es una área donde confluyen los aspectos, las políticas de seguridad y la tecnología, frecuentemente con consecuencias importante. A continuación solo se examinaran con brevedad tres áreas: privacidad, libertad de expresión y derechos de autor.

Privacidad.

¿Las personas tienen derecho a la privacidad? Buena pregunta. La cuarta Enmienda de los Estados Unidos prohíbe que el gobierno busque en las casas, documento y bienes de las persona sin una razón valida y restringe las circunstancias en las que se deben emitir las ordenes de cateo. Por lo tanto, la privacidad ha estado en la agenda pública aproximadamente durante 200 años, por lo menos en Estados Unidos.

En la década pasada la facilidad con la que el gobierno puede espiar a sus ciudadanos y la facilidad con la que estos pueden evitar tal espionaje. En el siglo XVIII, para que el gobierno pudiera buscar en los documentos de los ciudadanos, tenía que enviar un policía a caballo a la granja de dicho ciudadano exigiendo ver ciertos documentos. Era un procedimiento engorroso. Hoy en día, las compañías telefónicas y los proveedores de Internet proporcionan con facilidad intervenciones telefónicas cuando se les presenta una orden de cateo. Esto facilita la vida del policía y ya no hay peligro de que se caiga del caballo.

La criptografía cambia todo esto. Cualquiera que se tome la molestia de bajar e instalar PGP y que utilice una clave bien custodiada de fuerza alien puede estar seguro de que nade en el universo conocido puede leer su correo electrónico, haya o no orden de cato. Los gobiernos entienden bien esto y no les gusta. La privacidad real para ellos significa que les será mucho más difícil espiar a los criminales de todo tipo, y todavía le será más difícil espiar a los reportes y oponentes políticos. En consecuencia, algunos

gobiernos restringen o prohíben el uso o exportación de la criptografía. Por ejemplo, en Francia, antes de 1999, la criptografía estaba prohibida a menos que se le proporcionara las claves al gobierno.

Esto no los sucedía en Francia. En abril de 1993, el gobierno de Estados Unidos anuncio su intención de hacer que un criptoprocesador de hardware, el **procesador clipper**, fuera el estándar en toda la comunicación en red. De esta manera, se dijo, la privacidad de los ciudadanos estaría garantizada. También se menciono que el procesador proporcionaría al gobierno la capacidad de desencriptar todo el tráfico a través de un esquema llamado **depósito de claves**, el cual permitiría que el gobierno accediera a todas las claves. Sin embargo, se prometió que solo se espiaría cuando por esta situación, en la que los activistas de la privacidad condenaban todo el plan y los oficiales del cumplimiento de la ley la aclamaban. En algún momento, el gobierno se retracto y abandono la idea.

Retransmisores de correos anónimos

PGP, SSL y otras tecnologías hacen posible que dos partes establezcan comunicación segura y autenticada, libre de vigilancia e interferencia de terceros. Sin embargo, algunas veces la privacidad se aplica mejor cuando *no* hay autenticación, es decir, haciendo que la comunicación sea anónima. El anonimato podría quererse para los mensajes punto a punto, grupos de noticias o ambos.

Algunos ejemplos. Primero, los disidentes políticos que viven bajo regimenes autoritarios con frecuencia desean comunicarse de manera anónima para evitar ser encarcelados o asesinados. Segundo, por lo general las acciones ilegales en muchas organizaciones gubernamentales, educacionales, corporativas, entre otras, son denunciadas por personas que con frecuencia prefieren permanecer en el anonimato para evitar represalias. Tercero, las personas con creencias religiosas, políticas y sociales impopulares podrían querer comunicarse entre ellas a través de correo

electrónico o grupos de noticias sin exponerse a si mismos. Cuarto, las personas podrían desea discutir el alcoholismo, las enfermedades mentales, el acoso sexual, el abuso a infantes o ser miembros de una minoría perseguida de un grupo de noticias sin revelar su identidad.

Consideremos un ejemplo específico. En la década de 1990 algunos críticos publicaron sus puntos de vista sobre un grupo religioso no tradicional, en un grupo de noticias de USENET a través de un **retransmisor de correo anónimo**. Este servidor permitía que los usuarios crearan pseudónimos y le enviaran correo electrónico, y después dicho servidor volvía a enviar o publicar tal correo utilizando el pseudónimo creado, de manera que nadie podía sabe de donde provenía realmente el mensaje. Algunas publicaciones revelaron información que el grupo religioso afirmaba eran secretos comerciales y documentos con derechos de autor. Por lo tanto, dicho grupo fue con las autoridades locales y les dijo que sus secretos comerciales habían sido revelados y que sus derechos de autor habían sido violados, lo cual eran delitos en el lugar donde se localizaba el servidor. En consecuencia, se produjo un juicio y el operador del servidor fue obligado a entregar la información de correspondencia, la cual revelo las verdaderas identidades de las personas quienes realizaron las publicaciones. (Incidentalmente, esta no fue la primera vez que una religión no estaba de acuerdo con que alguien revelaras sus secretos: William Tyndale fue quemado en la hoguera en 1536 por traducir al ingles la Biblia)

Un segmento considerable de la comunidad de Internet se indigno por esta brecha de confidencialidad. La conclusión a la que todos llegaron es que no sirve de nada un retransmisor anónimo que almacena una correspondencia entre las direcciones reales de correo electrónico y los pseudónimos (llamados retransmisor de correo tipo 1). Este caso estimulo a varias personas a diseñar retransmisores de correo anónimos que pudieras resistir ataques de citaciones legales.

Estos nuevos retransmisores, con frecuencia llamados **retransmisores de correo cypherpunks**, funcionan como se describe a continuación. El usuario produce un mensaje de correo electrónico, lleno de encabezados RFC 822 (excepto *From*: por supuesto), lo encripta con la clave publica del retransmisor y lo envía a este. Ahí se eliminan los encabezados externos RFC 822, el contenido se desencripta y el mensaje es retransmitido. El retransmisor no tiene cuentas ni mantiene registros, por lo que aunque el servidor se confisque posteriormente, no contiene ni una huella de los mensajes que han pasado a través de el.

Libertad de expresión

La privacidad, se refiere a los individuos que desean restringir lo que otras personas ven en ellos. Un segundo problema social clave es la libertad de expresión, y su aspecto opuesto, la censura, que tiene que ver con el hecho de que los gobiernos desean restringir lo que los individuos pueden leer y publicar. Debido a que la Web contiene millones y millones de páginas, se ha vuelto un paraíso de censura. Dependiendo de la naturaleza e ideología del régimen, entre el material prohibido podrían encontrarse los sitios Web que contengan cualquiera de lo siguiente:

1. Material inapropiado para niños o adolescentes.

2. Odio dirigido a varios grupos religiosos, étnicos o sexuales, entre otros.

3. Información sobre democracia y valores democráticos.

4. Relatos de eventos históricos que contradigan la versión del gobierno.

5. Manuales para abrir candados, construir armas, encpritar mensajes, etcétera.

La respuesta común es prohibir los sitios malos.

Algunas veces los resultados son inesperados. Por ejemplo, algunas bibliotecas publicas han instalados filtros Web en sus computadoras para que sean aptas para los niños y bloqueados los sitios pornográficos. Los filtros vetan los sitios que se encuentran en sus listas negras y también verifican las páginas antes de desplegarlas para ver si contienen palabras obscenas. En Loudoun Conuntry, Virginia, sucedió que el filtro bloqueo la búsqueda que un cliente realizo para encontrar información sobre el cáncer de mama por que el filtro vi la palabra “mama”. Dicho usuario de la biblioteca demandó al condado Loudon. Sin embargo, el Livermore, California, después de que se sorprendió a un niño de 12 años de edad viendo pornografía, su padre demando a la biblioteca por *no* instalar un filtro. ¿Qué tenia que hacer la biblioteca?

Mucha gente ha obviado el hecho de que Wold Wide Web es una red mundial. Cubre a todo el mundo. No todos los países están de acuerdo en lo que debe permitirse en Web, por ejemplo, en noviembre de 2000, una corte de Francia ordeno a Yahoo, una corporación de California, que bloqueara a sus usuarios franceses para que no pudieran ver las subastas de objetos de recuerdo nazis, por que poseer tal material viola las leyes francesas. Yahoo apelo en nunca corte de Estados Unidos, la cual le dio la razón, pero aun esta lejos de resolverse el problema de donde aplicar las leyes de quien.

Simplemente imaginese. ¿Qué pasaría si alguna corte de UTAH ordenara a Francia que bloqueara los sitios Web relacionados con el vino por que no cumplen con las muy estrictas leyes de Utah sobre el alcohol? Suponga que China demandara que todos los sitios Web que tienen que ver con la democracia fueran prohibidos por que no son del interés del Estado. ¿Las leyes iraníes sobre la religioso se aplican a la Suecia más liberal? ¿Puede Arabia Saudita bloquear los sitios Web que tienen que ver con los derechos de la mujer? Todo el problema es una verdadera caja de Pandora.

Un comentario relevante de John Gilmore es: “la red interpreta la censura como una avería y encuentra un ruta alterna”. Para una implementación concreta, considere el

servicio eternidad (Anderson, 1996). Su objetivo es asegurarse de que la información publicada no puede ser eliminada o reescrita, como era común en la Unión Soviética durante el reinado de Josef Stalin. Para utilizar el servicio eternidad, el usuario especifica cuanto tiempo se mantendrá el material, paga una cuota proporcional a su duración y tamaño, y lo carga. Después de eso, nadie puede eliminarlo o modificarlo, ni siquiera quien lo cargo.

¿Cómo se puede implementar el servicio? El modelo mas sencillo es utilizar un sistema de igual a igual en el que los documentos almacenados se coloquen en docenas de servidores participantes, cada uno de los cuales obtengan una parte de la cuota y, por lo tanto, un incentivo para unirse al sistema. Los servidores deben esparcirse a través de muchas jurisdicciones legales para obtener una máxima elasticidad. Las listas de los 10 servidores seleccionados al azar podrían almacenarse en forma segura en varios lugares, por lo que si algunos estuvieran en peligro, otros aun existirían. Una autoridad dispuesta a destruir el documento nunca estará segura de que ha encontrado todas las copias. El sistema también podría repararse a si mismo; por ejemplo, si se sabe que se han destruido algunas copias, los sitios restantes podrían intentar encontrar nuevos depósitos para reemplazarlas.

El servicio eternidad fue la primera propuesta en lo que se refiera a sistemas anticensura. Desde entonces se han propuesto otros sistemas y. en algunos casos, se han implementado. Asimismo, se han agregado algunas nuevas características, como encriptación, anonimato y tolerancia a fallas. Con frecuencia los archivos se dividen en múltiples fragmentación, los cuales se almacenan en muchos servidores.

En la actualidad, cada vez mas países tratan de regular la exportación de valores intangibles, entre los que se encuentran sitios, Web, software, documentos científicos, correo electrónico, servicios de ayuda telefónica, entre otros. Incluso en el Reino Unido , que tiene una tradición de siglos de libertad de expresión, ahora esta considerando seriamente las leyes muy restrictivas, las cuales podrían, por ejemplo, definir las

discusiones técnicas entre un profesor británico y su estudiante extranjero de la Universidad de Cambridge como exportación regulada que necesita una licencia del gobierno (Andreson, 2002). No es necesario decir que tales políticas son controversiales.

Esteganografia

En los países en donde abunda la censura, los disidentes con frecuencia tratan de utilizar la tecnología para evadirla. La criptografía permite el envío de mensajes secretos (aunque tal vez no legalmente), pero si el gobierno piensa que Alice es una mala persona, el simple hecho de que ella se este comunicando con Bob podría ponerlo a el también en esta categoría, pues los gobiernos represivos entienden el concepto de clausura transitiva, aunque no entiendan bien las matemáticas. Los retransmisores de correo anónimos pueden ayudar, pero si están prohibidos domésticamente, y los mensajes dirigidos a extranjeros requieren una licencia de exportación por parte del gobierno, no serian de mucha ayuda. Pero Web si puede.

Las personas que desean comunicarse de manera secreta con frecuencia tratan de ocultar el hecho de que se esta realizando la comunicación. La ciencia de ocultar mensaje se conoce como **esteganografia**, cuyo origen proviene de las palabras griegas correspondientes a “escritura encubierta”. De hecho, los antiguos griegos la utilizaron. Herodoto escribió sobre un general que rapo a un mensajero, tatuó un mensaje en el cuero cabelludo de este y dejo que le creciera el cabello antes de enviarlo a realizar la entrega. Las técnicas modernas son conceptualmente las mismas, solo que tienen mayor ancho de banda y una latencia menor.

Derechos de autor

La privacidad y la censura son solo dos áreas en las que la tecnología se encuentra con la política pública. Una tercera son los **derechos de autor**. Estos son el otorgamiento a los creadores de la **IP** (**propiedad intelectual**), incluyendo a los escritores, artistas, compositores, músicos, fotógrafos, cinematógrafos, coreógrafos, entre otros, del derecho exclusivo para explotar su IP por algún tiempo, generalmente durante la vida del autor mas 50 o 75 años en el caso de la propiedad corporativa. Después de que expiran los derechos de autor de algún trabajo, pasa a ser del dominio publico y cualquiera puede utilizarlo o venderlo como lo desee. Por ejemplo, el Gutenberg Project (www.promo,net/pg) ha colocado en Web miles de trabajos de dominio público (de Shakespeare, Twian, Dickens), El 1998, el Congreso de los Estados Unidos extendió por 20 años mas los derechos de autor en ese país por solicitud de Hollywood, que afirmó que si no se otorgaba una extensión, nadie crearía nada mas. En contraste, las patentes solo duran 20 años y las personas aun siguen inventando cosas.

Los derechos de autor dieron de que hablar cuando Napster, un servicio de intercambio de música, tenia 50 millones de miembros. Aunque Napster realmente no copiaba la música, las cortes aseveraron que el hecho de que mantuviera una base de datos de quien tenía las canciones era infracción contributaria.

DISEÑO METODOLÓGICO

Para la realización de este trabajo se utilizó el método de investigación documental aplicada.

La tutora, Msc. Eman Hussein Yousif estableció el tema: ***Seguridad en Internet***, el cual se dividía en los subtemas: Cifrados Simétricos, Cifrados Asimétricos, Criptografía y función HASH, Autenticación y Aplicaciones de Correos Seguros. También orientó la elaboración de una aplicación.

En la presente investigación, se trata el subtema ***Aplicaciones de Correos Seguros***.
La información se fue recopilando a través de Internet, libros y exposiciones de grupo en el orden siguiente:

- Seguridad en Internet: para identificar ¿qué es la seguridad en Internet?, ¿cuál es la importancia que tiene?, ¿qué importancia tienen los datos para cualquier usuario?, ¿de qué manera se pueden proteger las empresas?
- Establecimiento de temas a exposición: Historia de la criptografía, *Historia de los virus informáticos*, Seguridad IP, Control de acceso y Protocolo SSL.
- ¿Qué son los virus?, ¿cómo se clasifican?, ¿cómo surgieron?, ¿de qué forma se puede contagiar?, ¿cómo se puede proteger?
- Servicios de seguridad: ¿qué tipos de servicios de seguridad se pueden brindar?, ¿en qué consisten?
- Cifrados o criptogramas: ¿en qué consisten?, elección del algoritmo a emplear en la aplicación a diseñar.
- Aplicaciones o Software existentes, a través de la documentación en el *Libro electrónico de seguridad informática y criptografía* de la *Web CriptoRed*.
- Descargar aplicaciones que sirvan de ejemplo para el diseño de la aplicación orientada.
- Búsqueda y descarga de la Aplicación PGP8, versión no comercial.

Se diseñó una aplicación en lenguaje de programación Visual Basic versión 6.0, por considerarlo un lenguaje fácil de uso potente para programar y ofrece herramientas útiles para la seguridad. Además, se utilizó MS Word para la elaboración del documento.

Para ello se utilizó una computadora con las siguientes características:

- Acer modelo Aspire 3050-1092
- Procesador Dual Core 1.8 GHz
- Memoria RAM 2Gb
- Disco Duro 120 GB
- Lector Quemador DVD/CD

El diseño de la aplicación tiene como finalidad encriptar y desencriptar archivos de texto haciendo uso del **Cifrado de Vigenère**.

El **Cifrado Vigenère** es un cifrado basado en diferentes series de caracteres o letras de *Cifrado César* formando estos caracteres una tabla, llamada *Tabla de Vigenère*, usada como clave. Este cifrado es del tipo polialfabético y de sustitución. El método original de este cifrado fue descrito por Giovan Batista Belaso. Pero se le atribuye a Blaise de Vigenère, en el siglo XIX. En términos matemáticos se expresa como:

$$Y_i = (X_i + Z_i) \bmod T$$

Z_i = {F,r,a,s,e, , c, l, a, v, e}

X_i = {Texto a cifrar}

T = número de caracteres de la Tabla de Vigenère a utilizar (ASCII)

Y_i = {Texto cifrado}

En la aplicación para **encriptar un archivo** se selecciona de la Barra de Menú la opción **Encriptar**, la cual le despliega dos opciones: **Clave de Usuario** (Ctrl + U) y **Clave Sistema** (Ctrl + S).

El ***proceso de encriptado*** → $Y_i = (X_i + Z_i) \bmod T$, se realiza de la siguiente manera:

1. Convierte a mayúscula la **Frase clave**. En la aplicación, la frase clave puede ser la establecida durante la programación de la misma aplicación o bien una creada por el usuario.

2. Desde i=1 hasta la longitud del archivo de texto seleccionado:
    a. Se extrae el caracter i del archivo de texto a encriptar.
    b. Se convierte en su valor equivalente ASCII.
    c. Se extrae de la contraseña el carácter i. Para ello se toma en cuenta la longitud de la contraseña, mientras i sea mayor que la longitud de la contraseña entonces el carácter a elegir será el resultante del residuo entre i y la longitud de la contraseña.
    d. Al valor ASCII del inciso (b) se le agrega el ASCII del inciso (c).
    e. Al resultado ASCII anterior, se le calcula el residuo al dividirlo con el número de caracteres de la Tabla ASCII que es 255. Luego lo convierte a caracter y se almacena en una cadena de caracteres.

En la aplicación para **desencriptar un archivo** se selecciona de la Barra de Menú la opción **Desencriptar**, la cual le despliega dos opciones: **Clave de Usuario** (Ctrl + O) y **Clave Sistema** (Ctrl + T).

El ***proceso de desencriptado*** → $X_i = (Y_i - Z_i) \bmod T$, se realiza de la siguiente manera:

1. Convierte a mayúscula la **Frase clave**. En la aplicación, la frase clave puede ser la establecida durante la programación de la misma aplicación o bien una creada por el usuario.

2. Desde i=1 hasta la longitud del archivo encriptado:
    a. Se extrae el caracter i del archivo encriptado.
    b. Se convierte en su valor equivalente ASCII.
    c. Se extrae de la contraseña el carácter i. Para ello se toma en cuenta la longitud de la contraseña, mientras i sea mayor que la longitud de la contraseña entonces el carácter a elegir será el resultante del residuo entre i y la longitud de la contraseña.
    d. Al valor ASCII del inciso (b) se le disminuye el ASCII del inciso (c). Pero si el primero (b) es menor que el segundo (c) entonces a (b) se le agrega el número de caracteres de la Tabla ASCII que es 255 antes de calcular la diferencia.
    e. Al resultado ASCII anterior, se le calcula el residuo al dividirlo con el número de caracteres que contiene la Tabla ASCII que es 255. Luego lo convierte a caracter y se almacena en una cadena de caracteres.

Ejemplo de Cifrado de Vigenere

Pos	0	1	2	3	4	5	6	7	8	9
0		A	B	C	D	E	F	G	H	I
1	J	K	L	M	N	Ñ	O	P	Q	R
2	S	T	U	V	W	X	Y	Z		

T=28 (numero de caracteres de la tabla de Vigenere)

Frase Clave: "SEGURIDAD" → Z_1=S, Z_2=E, Z_3=G, Z_4=U, Z_5=R, Z_6=I, Z_7=D, Z_8=A, Z_9=D

Texto legible: "CORREO SEGURO" → X= { X_1, X_2,X_3…….}

Y= texto cifrado = (X + Z) mod T

Longitud del texto

Longitud de la clave

$Y_1 = (X_1 + Z_1) \bmod T = (C + S) \bmod 28 = (3+20) \bmod 28 = 23 \bmod 28 = 23$ → V

$Y_2 = (O + E) \bmod 28 = (16+5) \bmod 28 = 21 \bmod 28 = 21$ → T

$Y_3 = (R + G) \bmod 28 = (19+7) \bmod 28 = 26 \bmod 28 = 26$ → Y

$Y_4 = (R + U) \bmod 28 = (19+22) \bmod 28 = 41 \bmod 28 = 13$ → M

$Y_5 = (E + R) \bmod 28 = (5+19) \bmod 28 = 24 \bmod 28 = 24$ → W

$Y_6 = (O + I) \bmod 28 = (16+9) \bmod 28 = 25 \bmod 28 = 25$ → X

$Y_7 = (\ \ + D) \bmod 28 = (0+4) \bmod 28 = 4 \bmod 28 = 4$ → D

$Y_8 = (S + A) \bmod 28 = (20+1) \bmod 28 = 21 \bmod 28 = 21$ → T

$Y_9 = (E + D) \bmod 28 = (5+4) \bmod 28 = 9 \bmod 28 = 9$ → I

$Y_{10} = (G + S) \bmod 28 = (7+20) \bmod 28 = 27 \bmod 28 = 27$ → Z

$Y_{11} = (U + E) \bmod 28 = (22+5) \bmod 28 = 27 \bmod 28 = 27$ → Z

$Y_{12} = (R + G) \bmod 28 = (19+7) \bmod 28 = 26 \bmod 28 = 26$ → Y

$Y_{13} = (O + U) \bmod 28 = (16+22) \bmod 28 = 38 \bmod 28 = 10$ → J

Y= **"VTYMWXDTIZZYJ"**

Ejemplo de Descifrado de Vigenere

Z= Frase Clave: "SEGURIDAD" →

Y= Texto Cifrado: **"VTYMWXDTIZZYJ"**

X= texto legible = (Y - Z) mod T

Nota:

si la posición de **Y** es menor a la posición de **Z** entonces se le agrega el valor de **T** a **Y**

Longitud del texto

Longitud de la clave

X_1 = (Y_1 - Z_1) mod T = (V - S) mod 28 = (23-20) mod 28 = 3 mod 28 = 3 → C

X_2 = (T - E) mod 28 = (21-5) mod 28 = 16 mod 28 = 16 → O

X_3 = (Y - G) mod 28 = (26-7) mod 28 = 19 mod 28 = 19 → R

X_4 = (M - U) mod 28 = **(13-22)** mod 28 = **((13+28)-22**) mod 28 = 19 → R

X_5 = (W - R) mod 28 = (24-19) mod 28 =5 mod 28 = 5 → E

X_6 = (X - I) mod 28 = (25-9) mod 28 = 16 mod 28 = 16 → O

X_7 = (D - D) mod 28 = (4-4) mod 28 = 0 mod 28 = 0 →

X_8 = (T - A) mod 28 = (21-1) mod 28 = 20 mod 28 = 20 → S

X_9 = (I - D) mod 28 = (9-4) mod 28 = 5 mod 28 = 5 → E

X_{10} = (Z - S) mod 28 = (27-20) mod 28 = 7 mod 28 = 7 → G

X_{11} = (Z - E) mod 28 = (27-5) mod 28 = 22 mod 28 = 22 → U

X_{12} = (Y - G) mod 28 = (26-7) mod 28 = 19 mod 28 = 19 → R

X_{13} = (J - U) mod 28 = **(10-22)** mod 28 = **((10+28)-22)** mod 28 = 16 → O

X= **"CORREO SEGURO"**

DESCRIPCION DE APLICACIÓN

Desde el disco con el instalador ejecutar el archivo Setup, leer las instrucciones y responder a los cuadros de dialogo según corresponda. Luego, es necesario crear desde la ventana de comandos una unidad virtual **s:** a la cual se le asigna la ruta de acceso donde se encuentra la carpeta donde instaló la aplicación

….. > subst s: c:\ … \ Aplicación↵

Al ejecutar la aplicación **SED_Vigenere** de la unidad virtual aparecerá la ventana de inicio:

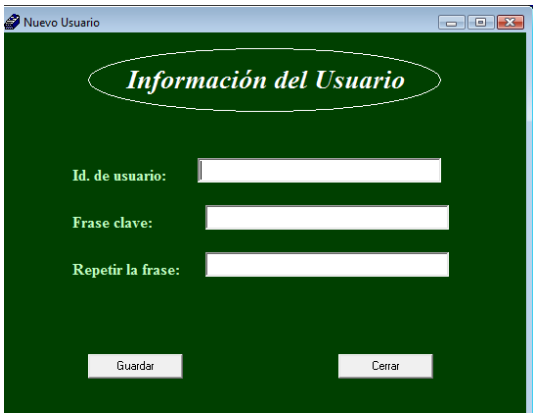
Para luego apuntar con el Mouse el logotipo y dar clic sobre él.

Inmediatamente aparecerá la ventana del Menú Principal:

La Barra de Menú contiene las opciones contiene:

- **Usuario:** esta permite trabajar con una base de datos. Cuyo objetivo es almacenar la identidad de usuario (dato que lo identifica de forma única) y una frase clave (la que puede ser compartida con otro usuario).
- **Encriptar:** permite encriptar archivos de texto ya sea haciendo uso de la frase clave del sistema o bien la frase clave almacenada en la base de datos.
- **Desencriptar:** permite desencriptar o descifrar archivos de texto que han sido encriptado con la clave del sistema o con la frase clave que se encuentra en la base de datos.
- **Acerca de:** presenta información general sobre la aplicación.
- **Salir:** equivale a cerrar la aplicación.

Al seleccionar de la Barra de Menú la opción **Usuario** se despliega el submenú con las opciones: **Nuevo** (Ctrl +N), **Modificar** (Ctrl + M) y **Eliminar** (Ctrl + E):



La opción **Nuevo** del menú Usuario, solicita ingrese la identidad de usuario, la frase clave a compartir y repetición de la frase clave. Una vez que ingresa los datos y selecciona el botón *Guardar*, el sistema se encarga de verificar que realmente se haya

ingresado información, que la identidad del usuario no exista en la base de datos y que las frases se hayan escrito idénticas. Si se cumple muestra la frase cifrada, se activa el botón *Limpiar*, el cual permite limpiar los cuadros de texto y así podrá ingresar otro usuario. El botón *Cerrar*, cierra la ventana y retorna al menú principal.

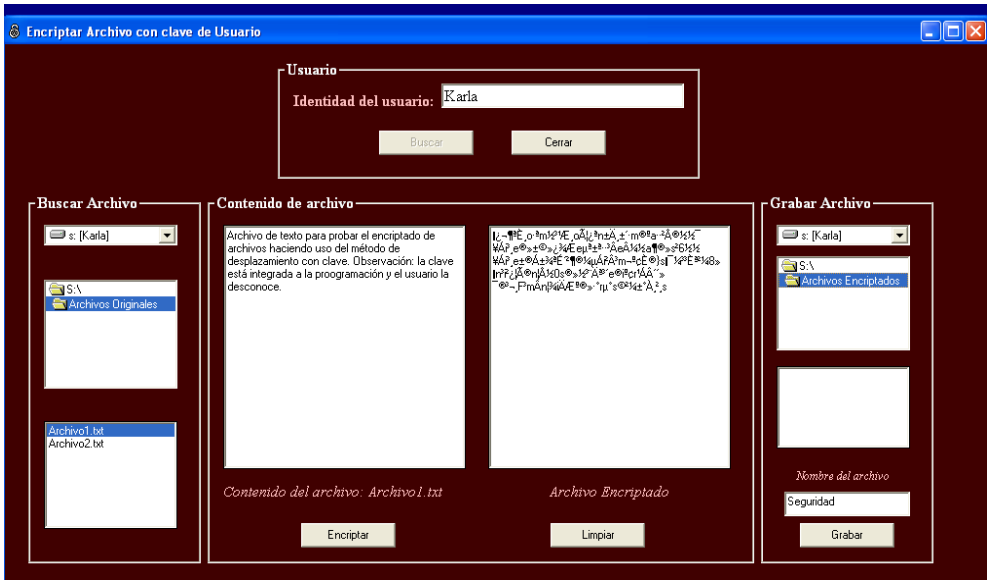
Al elegir la opción **Modificar** del menú Usuario, primero solicita la identidad del usuario, luego se debe dar clic en el botón *Buscar*. Con esto se verifica que la base de datos no esté vacía y que la identidad del usuario exista. Si cumple con lo antes mencionado entonces el usuario deberá ingresar la nueva frase y repetirla.

Solicita la nueva frase y que se repita. Se activa el botón *Guardar* para verificar que la frase y repetición realmente fueron ingresadas, es decir que no estén vacías, luego se comparan las frases y si son iguales se permitirá grabar los cambios y mostrar la nueva frase encriptada de lo contrario desplegará un mensaje haciendo la observación del error.

A continuación se activa el botón *Limpiar* que permite despajar la ventana. El botón *Cerrar* devuelve el control a la ventana del menú principal.

La opción **Eliminar** del menú Usuario, solicita la identidad del usuario que será dada de baja de la base de datos. El usuario debe dar clic en el botón *Buscar* y verifica si fue ingresada la identidad, luego que la base de datos no esté vacía y que el usuario exista en ella. Una vez que lo encuentre, se activa el botón *Eliminar* con el cual el usuario podrá confirmar con seguridad su deseo de eliminar al usuario. El botón *Cerrar* retorna al Menú principal.

Al seleccionar de la Barra de Menú la opción **Encriptar** se despliega el submenú con las opciones: **Clave de Usuario** (Ctrl +U) y **Clave Sistema** (Ctrl + S):



La opción **Clave de Usuario** del menú Encriptar, solicita la identidad del usuario luego el usuario debe dar clic sobre el botón *Buscar*, para verificar primero que se ingresó lo pedido; que la base de datos no esté vacía y que el usuario exista. Una vez que aprueba, el usuario debe seleccionar la ruta (unidad, carpeta) y el archivo de texto a cifrar.

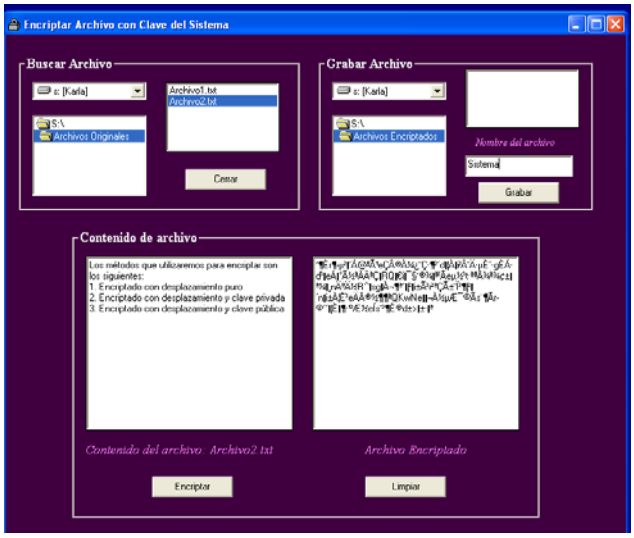
El contenido del archivo se mostrará, se activa el botón *Encriptar* para que el usuario lo elija y mostrar el archivo cifrado. Para ello, se hace uso de la frase clave almacenada en la base de datos y el texto o contenido del archivo.

El proceso de encriptado se realiza de la siguiente manera:

3. Convierte a mayúscula la contraseña del usuario.
4. Desde i=1 hasta la longitud del archivo:
    a. Se extrae el caracter i del archivo de texto.
    b. Se convierte en su valor equivalente ASCII.
    c. Se extrae de la contraseña, un carácter, que será el resultante del residuo entre i y la longitud de la contraseña.
    d. Al valor ASCII del inciso (b) se le agrega el ASCII del inciso (c).
    e. Al resultado ASCII anterior: se le verifica que no exceda los 255, lo convierte a caracter y se almacena en una cadena de caracteres.

Una vez que se obtiene la cadena encriptada resultante, ésta se despliega en otro cuadro de texto enriquecido.

Si desea grabar el archivo cifrado debe seleccionarse la unidad y carpeta donde se guardará. Digita el nombre del nuevo archivo el cual tiene programado colocársele la extensión "**.usu**" y da clic sobre el botón *Grabar*. El botón *Limpiar* despeja la ventana. El botón *Cerrar* devuelve al menú principal.

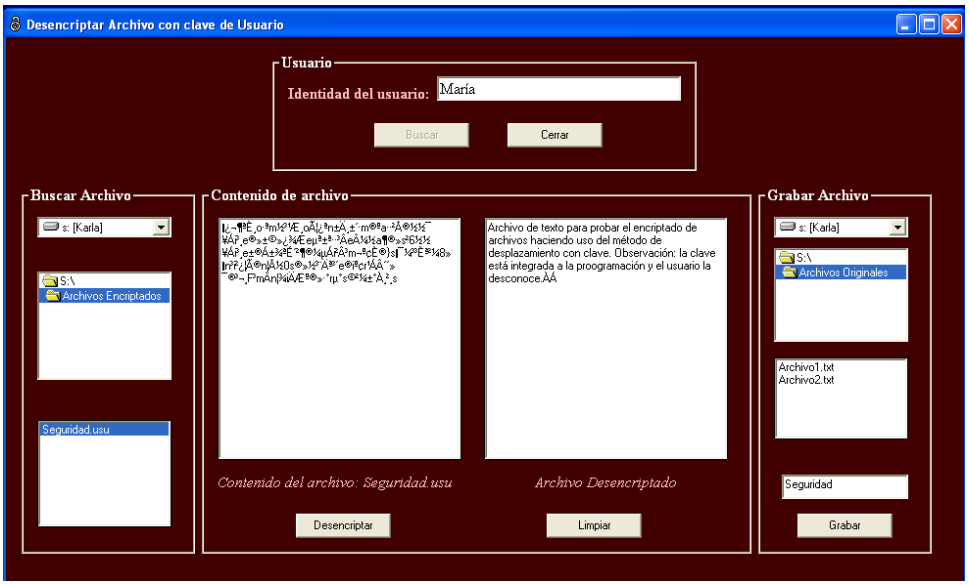


En la opción **Clave Sistema** del menú Encriptar, el usuario debe seleccionar la ruta (unidad, carpeta) y el archivo de texto a cifrar. El contenido del archivo se mostrará, se activa el botón *Encriptar* para que el usuario lo elija y mostrar el archivo cifrado.

Para ello, se hace uso de una contraseña que se encuentra en la codificación del programa y el texto o contenido del archivo. El proceso de encriptado se realiza de la misma manera descrita para la opción ***Clave de Usuario***. Una vez que se obtiene la cadena encriptada resultante, ésta se despliega en otro cuadro de texto enriquecido.

Se despliega un mensaje de texto expresando que el archivo fue encriptado. Si desea grabar el archivo cifrado debe seleccionarse la unidad y carpeta donde se guardará. Digita el nombre del nuevo archivo y da clic sobre el botón *Grabar* y automáticamente se le agregará la extensión **“.enc”**. El botón *Limpiar* despeja la ventana. El botón *Cerrar* devuelve al menú principal.

Al seleccionar de la Barra de Menú la opción **Desencriptar** se despliega el submenú con las opciones: **Clave de Usuario** (Ctrl +O) y **Clave Sistema** (Ctrl + T):



La opción **Clave de Usuario** del menú Desencriptar, solicita la identidad del usuario luego el usuario debe dar clic sobre el botón *Buscar*, para verificar primero que se ingresó lo pedido; que la base de datos no esté vacía y que el usuario exista. Una vez que aprueba, el usuario debe seleccionar la ruta (unidad, carpeta) y el archivo con extensión **".usu"** a descifrar.

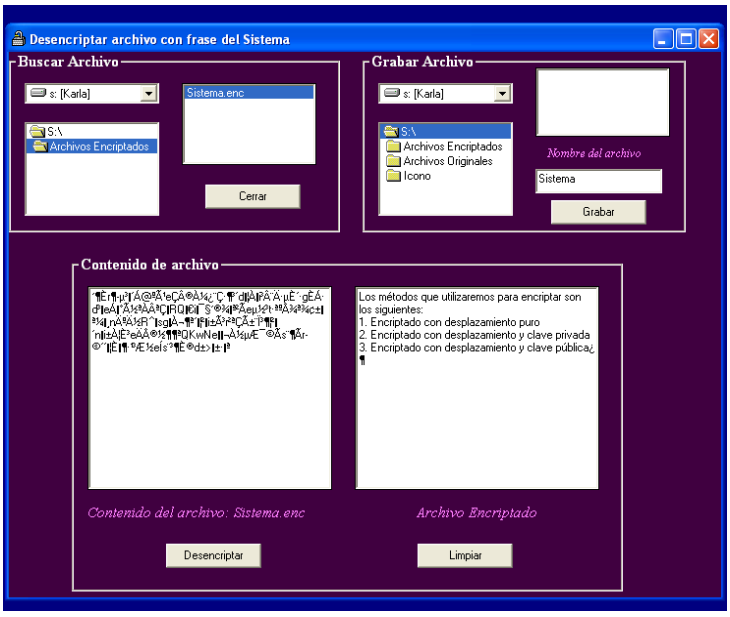
El contenido del archivo se mostrará, se activa el botón *Desencriptar* para que el usuario lo elija y muestra el archivo descifrado. Para ello, se hace uso de la frase clave almacenada en la base de datos y el texto o contenido del archivo. El proceso de desencriptado se realiza de la siguiente manera:

3. Convierte a mayúscula la contraseña del usuario.
4. Desde i=1 hasta la longitud del archivo:

f. Se extrae el caracter i del archivo de texto.
g. Se convierte en su valor equivalente ASCII.
h. Se extrae de la contraseña, un carácter, que será el resultante del residuo entre i y la longitud de la contraseña.
i. Al valor ASCII del inciso (b) se le disminuye el ASCII del inciso (c).
j. Al resultado ASCII anterior: se le verifica que no exceda los 255, lo convierte a caracter y se almacena en una cadena de caracteres.

Una vez que se obtiene la cadena desencriptada resultante, ésta se despliega en otro cuadro de texto enriquecido.

Si desea grabar el archivo descifrado debe seleccionarse la unidad y carpeta donde se guardará. Digita el nombre del nuevo archivo el cual tiene programa colocársele la extensión "**.txt**" y da clic sobre el botón *Grabar*. El botón *Limpiar* despeja la ventana. El botón *Cerrar* devuelve al menú principal.



La opción **Clave Sistema** del menú Desencriptar, permita al usuario seleccionar la ruta (unidad, carpeta) y el archivo con extensión **“.enc”** a descifrar.

El contenido del archivo se mostrará, se activa el botón *Desencriptar* para que el usuario lo elija y muestra el archivo descifrado. Para ello, se hace uso de la frase clave del sistema y el texto o contenido del archivo. El proceso es similar al explicado en la opción Clave de Usuario.

Una vez que se obtiene la cadena desencriptada resultante, ésta se despliega en otro cuadro de texto enriquecido.

Si desea grabar el archivo descifrado debe seleccionarse la unidad y carpeta donde se guardará. Digita el nombre del nuevo archivo el cual tiene programa colocársele la extensión “**.txt**” y da clic sobre el botón *Grabar*. El botón *Limpiar* despeja la ventana. El botón *Cerrar* devuelve al menú principal.

La opción **Acerca de** despliega una ventana con información de los creadores de la aplicación.

CONCLUSIONES

Se analizo la importancia que tiene establecer seguridad en las redes de computadoras.

Los sistemas de seguridad como PGP permiten encriptar archivos para luego ser enviados por correo electrónico a otro usuario quien será el único interesado y responsable del correo para luego desencriptar el archivo.

Se llego a los objetivos deseados, con el diseño de la aplicación, la cual encripta y desencripta archivos de textos.

ANEXOS

LISTA DE ABREVIATURAS

ASCII: American **S**tandard **C**ode for **I**nformation **I**nterchange — Código Estadounidense Estándar para el Intercambio de Información

AT&T: American Telephone and Telegraph

CA: Certification Authority – Autoridad de Certificación

CPU: Central Process Unit – Unidad Central de Procesos

DES: Data Encryption Standard – Estándar de Cifrado de Datos

IBM: Internacional Business Machines – Negocio Internacional de Máquinas

ICVS: Informatic Control Virus Scanner – Control Informático de Búsqueda de Virus

IETF: Internet Engineering Task Force

ISO: International Standards Organization – Organismo Internacional de Normalización

ITU: International Telecommunications Committee – Comité Internacional de Telecomunicaciones

MIME: Multipurpose Internet Mail Extensions

MIT: Massachusetts Institute of Technology – Instituto de Tecnología de Massachusetts

MOSS: MIME Object Security Services

OSI: Open Systems Interconnection –Interconexión de Sistemas Abiertos

PC-DOS: Personal Computer – Disk Operating System

PEM: (Private Enhanced Mail – Correo Privado Mejorado) Sistema de correo con encriptación

PGP: (Pretty Good Privacy – Privacidad muy buena)

PKI: Public Key Infraestructura – Infraestuctura de Clave Pública

RAM: Random Access Memory – Memoria de Acceso Aleatorio

RFC 2828: Son recomendaciones contra amenazas y ataques

SMTP: Simple Mail Transfer Protocol

TCP/IP: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP),

GLOSARIO

Amenaza:

Una posibilidad de violación a la seguridad, que existe cuando se da una circunstancia, capacidad, acción o evento que pudiera romper la seguridad y causar perjuicio. Es decir, una amenaza es un peligro posible que podría explotar una vulnerabilidad.

Ataque:

Un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema.

Ataque a la seguridad:

Cualquier acción que comprometa la seguridad de la información de una organización.

Cifrado asimétrico:

Se crea un par de claves, una privada (propia del emisor/receptor) y otra pública que es compartida por ambos.

Cifrado simétrico:

Se crea una única clave que es compartida entre el emisor y el receptor.

Cracker:

Son hackers malignos que se dedican a romper la seguridad de los sistemas informáticos para robar o destruir información. Emplean sus ataques con fines económicos.

Hacker:

Persona que rompe la seguridad de los sistemas informáticos sin causar daño alguno.

Mecanismos de seguridad:

Es un mecanismo diseñado para detectar un ataque a la seguridad, prevenirlo o restablecerse de él.

Infraestructura de Clave Pública:

Es un conjunto de servicios de seguridad que permiten el uso y administración de encriptación de clave pública y certificados.

Servicios de seguridad:

Es un servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización. Los servicios están diseñados para contrarrestar los ataques a la seguridad, y hacen uso de uno o más mecanismos para proporcionar el servicio.

X.800:

Conjunto de reglas, normas, estándares.

BIBLIOGRAFÍA

Garfinkel, Simpson y Stpaford, Gene. **Seguridad en Linux e Internet.** ***McGraw Hill.***

Perry, Grez. **Aprendiendo Visual Basic en 24 horas.** ***Prentice Hall.***

Stalling, William. **Fundamentos de Seguridad en Redes. Aplicaciones y estándares.** ***Segunda Edición.Prentice Hall.***

Tanenbaum, Andrew S. **Redes de Computadoras.** ***Cuarta Edición.***

Uyless Black. **Redes de Computadoras. Protocolos, Normas e Interfaces.** ***Primera Edición. Macrobit***

http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

http://www.bsecure.com.mx/articulo-60-6601-379.html

http://www.camerfirma.com/mod_web/aplicaciones/celecsec.html

http://www.criptored.upm.es/

http://www.jorgemachado.net/content/view/52/1/

http://www.rediris.es/rediris/boletin/31/enfoque1.html

http://www.rediris.es/rediris/boletin/32/enfoque1.html