PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

ESCUELA DE INGENIERIA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERIO DE SISTEMAS

"SEGURIDAD DE ARCHIVOS EN LA BIBLIOTECA VIRTUAL DE LA PUCESA PARA LA PROTECCIÓN DEL DERECHO INTELECTUAL"

Miguel Angel Rodríguez Pérez

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
PROGRAMAS ACADEMICOS AMBATO
BIBLIOTECA

DIRECTOR DE LA DISERTACIÓN: Ing. Víctor Chuncha

AMBATO, 2004

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
DIRECCION
ESCUELA DE INGENIERIA DE SISTEMAS

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
SECRETARIA
ESCUELA DE INGENIERIA DE SISTEMAS

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

ESCUELA DE INGENIERIA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERIO DE SISTEMAS

"SEGURIDAD DE ARCHIVOS EN LA BIBLIOTECA VIRTUAL DE LA PUCESA PARA LA PROTECCIÓN DEL DERECHO INTELECTUAL"

Miguel Angel Rodríguez Pérez

DIRECTOR DE LA DISERTACIÓN: _____

Ing. Víctor Chuncha

AMBATO, 2004

DEDICATORIA

Primero a Dios, quien me ha iluminado en todos los momentos de mi vida.

A mis queridos padres por su apoyo y sacrificio que han hecho para culminar con éxito mi carrera estudiantil.

A mi hermana por darme un buen ejemplo para seguir adelante y así darme ánimos de conseguir mi objetivo principal.

A mi sobrina Andrea Micaela por ser parte de mi vida.

Miguel

AGRADECIMIENTO

En primer lugar a Dios por haberme guiado e iluminado para la realización de este trabajo.

A mis padres por su cariño y apoyo incondicional.

A la Pontificia Universidad Católica del Ecuador Sede Ambato por haberme dado la oportunidad de formarme y ser profesional.

Y un agradecimiento muy especial al Ing. Victor Chuncha por su enseñanza que ha sabido brindar en este tiempo de estudio para culminar con éxito este trabajo.

Miguel

INTRODUCCIÓN

A partir de los años 80, el uso de los archivos ha generado gran preocupación debido a los ataques que han sufrido, y es por esto que se toma conciencia del peligro que ocasionan a los usuarios y a computadoras que están conectados a Internet.

Es por esto que los usuarios reconocen la necesidad de un estudio que permita proteger los archivos para que no sean modificados y se aplique los derechos de propiedad intelectual.

En nuestro medio informático, existen técnicas que nos permite proteger los archivos de una forma eficaz, y se lo puede realizar mediante un criptoanálisis de los diversos algoritmos de cifrado.

Los sistemas más antiguos de cifrado se basaban en transformación de unas letras por otras. Posteriormente se pasó a hacer trasposiciones de filas y columnas del texto o a cambiar sílabas en función de tablas. En la actualidad la transformación del texto utiliza unos algoritmos o funciones matemáticas muy complejas.

Los algoritmos de encriptación actuales se agrupan en dos grandes clases según que el proceso de encriptación y descifrado use la misma clave o use claves distintas. Si usan la misma clave se denominan algoritmos de claves simétricas; por el contrario, si utilizan claves distintas se les denomina algoritmos de claves asimétricas o algoritmos asimétricos.

Con estas características se ve en la necesidad de implementar un sistema de protección criptográfico en la Biblioteca Virtual de la PUCESA, para lograr la satisfacción del usuario y la excelencia académica de los estudiantes.

Es por todo esto la investigación y se propone algoritmos de análisis para aplicar al sistema de protección de la Biblioteca Virtual de la PUCESA.

INDICE

CAPITULO I

1.1 ANTECEDENTES Y JUSTIFICACIÓN.....1

1.2 OBJETIVOS.....3

1.2.1 Objetivo General.....3

1.2.2 Objetivo Específico.....3

1.3 HIPÓTESIS.....3

1.4 ASPECTOS METODOLÓGICOS.....4

1.4.1 Métodos de Investigación.....4

1.4.2 Técnicas de Investigación.....4

1.5 FUNCIONAMIENTO DE LA BIBLIOTECA VIRTUAL DE LA PUCESA.....4

1.5.1 Hardware.....5

1.5.2 Software.....6

1.5.3 Software con licencias libres.....6

1.5.4 Sistema Operativo.....6

1.6 ORGANIZACIÓN DEL TRABAJO.....6

CAPITULO II

LEGISLACIÓN.....7

2.1 PROTECCIÓN DEL DERECHO A LA INTIMIDAD Y PRIVACIDAD.....7

2.2 ACTOS Y NEGOCIOS JURÍDICOS ELECTRÓNICOS.....8

2.2.1 La confidencialidad.....9

2.2.2 Seguridad técnica.....9

2.2.3 Seguridad jurídica.....9

2.3 CONTRATACIÓN ELECTRÓNICA INFORMÁTICA.....10

2.3.1 La autenticidad de la identidad de las partes.....10

2.3.2 La integridad del documento electrónico.....10
2.3.3 La prueba de la transacción electrónica.....11
2.3.4 Marco legal del comercio electrónico.....11
2.3.5 Contratos informáticos.....12
2.4 PROTECCIÓN JURÍDICA DEL SOFTWARE Y HARDWARE.....13
2.4.1 Protección del software por medios diferentes del derecho de autor.....13
2.5 DELITOS INFORMÁTICOS.....13
2.5.1 Sujeto pasivo en el delito informático.....14
2.5.2 Sujeto activo en el delito informático.....14
2.5.3 Clasificación del delito informático.....14
2.5.4 Fraudes cometidos mediante manipulación de computadoras.....15
2.5.4.1 Manipulación de los datos de entrada.....15
2.5.4.2 Manipulación de programas.....15
2.5.4.3 Manipulación de los datos de salida.....15
2.5.4.4 Fraude efectuado por manipulación informática.....16
2.5.4.5 Falsificaciones informáticas.....16
2.5.4.6 Daños o modificaciones de programas o datos computarizados...16
2.5.4.7 Acceso no autorizado a servicios y sistemas informáticos.....16
2.5.4.8 Reproducción no autorizada de programas informáticos de protección legal.....17
2.6 TELECOMUNICACIONES Y DERECHO.....17
2.7 DERECHO INFORMÁTICO E INTERNET.....18
2.7.1 ¿El Derecho Informático es una Ciencia?.....18
2.8 DERECHOS DE AUTOR DE LAS PÁGINAS WEB.....19
2.8.1 La Página Web como Obra Protegida por la Propiedad Intelectual.....21

2.8.2 Protección de la Página Web.....21

Inscripción en el Registro de Propiedad Intelectual (IEPI).....22

Depósito notarial.....22

CAPITULO III

SEGURIDAD.....24

3.1 INTRODUCCIÓN.....24

3.2 SEGURIDAD INFORMÁTICA.....24

3.2.1 Intrusos.....24

3.2.1.1 Acceso - Uso – Autorización.....24

3.2.1.2 Detección de Intrusos.....25

3.2.1.3 Identificación de Amenazas.....25

3.2.1.4 Tipos de Ataque.....25

3.2.1.5 Ingeniería Social.....26

3.2.1.6 Ingeniería Social Inversa.....26

3.2.1.7 Ataques de Monitorización.....26

3.2.1.8 Ataques de Autenticación.....27

3.2.1.9 Spoofing – Looping.....27

3.2.1.10 Ataques de Modificación – Daño.....27

3.2.1.11 Borrado de huellas.....28

3.2.2 Políticas de Seguridad.....28

Integridad.....28

Confidencialidad.....29

Disponibilidad.....29

3.2.2.1 Control de Acceso a los Datos.....30

3.2.2.2 Largo mínimo de claves de acceso (password).....30

UNIVERSIDAD CATÓLICA DEL ECUADOR
PROGRAMAS ACADÉMICOS A DISTANCIA
BIBLIOTECA

3.2.2.3 Es obligatorio capacitar a todos los usuarios sobre la seguridad de la información.....30

3.2.2.4 Control de acceso físico a las áreas con información sensitiva....31

3.3 SEGURIDAD EN INTERNET.....31

3.3.1 Motivación.....31

3.3.2 Riesgos de Internet.....32

3.4 SEGURIDAD EN LOS SERVICIOS DE CONEXIÓN (SSL).....32

3.5 SEGURIDAD DE SOFTWARE.....33

3.6 LICENCIAS.....33

3.6.1 Tipos de licencias para software redistribuible libremente.....33

3.6.2 Las licencias de uso.....34

CAPITULO IV

FICHEROS.....35

4.1 SEGURIDAD DE ARCHIVOS.....35

4.1.1 ¿Porqué realizar un Test de Intrusión periódicamente?.....35

4.1.2 ¿Cómo se realiza el Test?.....35

4.1.3 ¿Cómo encaja un Test de Intrusión en el conjunto de seguridad?.....36

4.1.4 Objetivo.....36

4.2 PAQUETES INFORMÁTICOS.....37

4.3 FORMATOS DE PROGRAMAS.....37

4.3.1 Portable Data File (PDF).....37

4.3.1.1 Problemas Comunes.....38

4.3.2 Postscript (PS).....39

4.4 ESTRUCTURA INTERNA DE PROGRAMAS.....41

Formato PDF.....42

Formato PS....42

PostScript como lenguaje de programación....43

CAPITULO V

TÉCNICAS EN PROTECCIÓN DE ARCHIVOS Y SOFTWARE....44

5.1 CONTRASEÑAS....44

5.1.1 Importancia de las contraseñas....46

5.2 ENCRIPTACIÓN Y FIRMAS DIGITALES....49

5.2.1 Encriptación de comunicaciones....50

5.2.2 Criptografía Simétrica....50

5.2.3 Criptografía Asimétrica....51

5.2.4 Encriptación de Documentos y mensajes de correo....52

5.2.5 Firmas Digitales....52

5.3 CLAVES PÚBLICAS Y PRIVADAS....53

5.3.1 La clave pública....55

5.3.2 La clave privada....56

5.4 CANDADOS PARA LA PROTECCIÓN DE SOFTWARE....56

Protecciones Físicas – Candados Electrónicos....56

Candados programables con memoria....57

NetHasp....57

Aladdin Card....58

5.5 FORMATOS DE ARCHIVOS PDF....58

CAPITULO VI

ANÁLISIS....60

6.1 CARACTERÍSTICAS DE LA APLICACIÓN....60

6.1.1 Propuesta de la Aplicación....60

6.1.2 Confidencialidad e Integridad....61
6.1.3 Clasificación de los Criptosistemas....62
6.1.4 Cifrado con Criptosistemas Simétricos de Clave Secreta....62
6.1.5 Cifrado Tipo Feistel....63
6.1.6 Algoritmos de Cifrado más Conocidos....64
6.1.6.1 Algoritmo de la Serpiente (Blowfish)....64
6.1.6.2 Algoritmo Estandar de Encriptación de Datos (DES)....66
6.1.6.3 Algoritmo GOST....67
6.1.6.4 Algoritmo CAST....69
6.1.6.5 Algoritmo de Encriptación Avanzada (RIJNDAEL)....70
6.1.6.6 Algoritmo SKIPJACK....71
6.1.6.7 Algoritmo IDEA....72
6.1.6.8 Algoritmo TwoFish....74
6.1.7 RECURSOS....77
6.1.7.1 Recurso Humano....77
6.1.7.2 Recursos Materiales....78
6.1.7.3 Recursos Económicos....78
6.2 ESTRUCTURA DE LA APLICACIÓN....79
6.2.1 Diagrama de Flujo de Datos....79
6.2.2 Descripción General del Sistema....80
6.2.3 Diccionario de Datos....82
6.3 DETERMINACIÓN DE RECURSOS UTILIZADOS....82
6.3.1 Recursos Materiales....82
6.3.2 Requisitos de la Aplicación....83

CAPITULO VII

EVALUACIÓN.....**84**

7.1 METODOLOGÍA PARA REALIZAR PRUEBAS.....84

7.2 RESULTADOS DE LA METODOLOGÍA.....85

7.3 CONCLUSIONES Y RECOMENDACIONES.....**87**

BIBLIOGRAFÍA.....**89**

ANEXOS.....**91**

GLOSARIO DE TÉRMINOS.....**105**

CAPITULO I

1.1 ANTECEDENTES Y JUSTIFICACION

La seguridad de archivos es un tema amplio. Este capítulo se va a enfocar en la definición y la discusión de la seguridad de archivos, confiabilidad del software, la responsabilidad del desarrollador y de la responsabilidad del usuario.

La seguridad de archivos es un proceso continuo, que requiere tener previsto hasta lo imprevisible.

Tener unos buenos hábitos y tomar ciertas precauciones nos ayudarán mucho.

Lo primero es determinar qué es lo que se quiere proteger. No será lo mismo una estación de trabajo personal aislada con conexiones a Internet esporádicas que un servidor web con conexión permanente.

La seguridad de archivos aplica los principios de la seguridad de información al desarrollo de software. Es decir se refiere a la seguridad de información comúnmente como la protección de sistemas de información contra el acceso desautorizado o la modificación de información, si está en una fase de almacenamiento o de procesamiento. También la protege contra la negación de servicios a usuarios desautorizados y la provisión de servicio a usuarios desautorizados, incluyendo las medidas necesarias para detectar, documentar, y contrariar tales amenazas.

Muchas preguntas con respecto a la seguridad de archivos, son relacionadas al ciclo vital de software. En particular, la seguridad del código y el proceso de software; deben ser considerados durante la fase del diseño y desarrollo. Además, la seguridad de archivos debe ser preservada durante la operación y el mantenimiento para asegurar la integridad de una parte del software, y proteger los derechos de autor.

Una gran cantidad de seguridad usada en los sistemas de redes de hoy, nos pueden engañar en la creencia que nuestros trabajos como diseñadores de sistemas de seguridad ya han sido realizados. Sin embargo, las cadenas y computadoras son increíblemente inseguras. La falta de seguridad se origina en dos problemas fundamentales: los sistemas que son teóricamente seguros pueden ser inseguros en la práctica. Además los sistemas son cada vez más complejos. La complejidad proporciona más oportunidades para poder modificar.

En particular, se puede mejorar la confiabilidad de software. También se puede mejorar la comprensión de los requisitos de un pedazo de software.

Desactive todos los servicios que no vaya a prestar. No tiene sentido tener abierto un servicio del que no va a hacer uso ningún usuario legal. Puede que esté consumiendo recursos de su sistema para ofrecer a algún atacante la posibilidad de violarlo.

Debido a que en la Biblioteca Virtual de la PUCESA, es un área donde se tiene acceso a Internet con la finalidad de consultar, ya sean los estudiantes, profesores, u otro tipo de personas que estén interesados en utilizar los servicios que presta la Biblioteca Virtual de la PUCESA.

Existe la necesidad de realizar una aplicación que permita proteger los archivos que son utilizados en la Biblioteca Virtual, y que han sido realizados por los estudiantes o profesores de la PUCESA; ya sean estos mediante la creación de páginas Web, documentos de tipo pdf, ppt, doc, xls, etc.

Estos documentos no podrán ser modificados, plagiados bajo ningún aspecto según las leyes existentes tanto de propiedad intelectual como los derechos de autor, y otros más que serán expuestos en los siguientes capítulos.

1.2 OBJETIVOS

1.2.1 Objetivo General

Elaborar un estudio acerca de la seguridad de archivos y programas tanto en la parte técnica como en lo legislativo, y desarrollar un proyecto que permita publicar archivos en forma segura en la Biblioteca Virtual de la PUCESA mediante la aplicación de formatos de archivos y algoritmos de seguridad.

1.2.2 Objetivo Específico

- Realizar un estudio de la tecnología que implica la seguridad de archivos.
- Realizar un estudio de la tecnología que implica la seguridad de software.
- Investigar las diferentes aplicaciones de seguridad que existen en ficheros, paquetes y plataformas más conocidas en nuestro medio.
- Investigar la parte legislativa, que involucra en el ámbito informático, en relación a la seguridad de archivos.
- Estudiar los formatos Portable Data File (PDF) y Postcript (PS) para archivos documentales.
- Estudiar algoritmos de encriptación y firmas digitales.
- Estudiar que acciones se debería tomar cuando se intente copiar información o programas.

1.3 HIPÓTESIS

La implementación del proyecto de seguridad de archivos y software proporcionará a la Biblioteca Virtual de la PUCESA una gran ayuda en la obtención de información

confiable y en tiempo prudente, permitiendo de esta manera publicar revistas técnicas, artículos, libros digitalizados y aplicaciones informáticas.

1.4 ASPECTOS METODOLÓGICOS

1.4.1 Métodos de Investigación.

Entre los principales métodos de investigación se utilizarán las siguientes: Investigación Documental o Bibliográfica; se realiza mediante fuentes impresas (libros, revistas, folletos, internet), el procedimiento a utilizar es la consulta.

Investigación Aplicada; se utiliza la Investigación Documental para luego aplicarla en situaciones prácticas.

Asesoramiento y entrevistas con profesionales especializados en el tema.

1.4.2 Técnicas de Investigación.

- Libros, CDs, programas y tutoriales de apoyo sobre las seguridades de archivos.
- Investigación de temas por medio de Internet.
- Toda información que se investigue se realizará para su uso posterior de la investigación.

1.5 FUNCIONAMIENTO DE LA BIBLIOTECA VIRTUAL DE LA PUCESA

Los archivos de la Biblioteca se han venido obteniendo desde Internet, pero sin ninguna seguridad para evitar que dicha información sea modificada por algún usuario que no tenga nada que ver en la Administración de la Biblioteca Virtual, para esto es necesario

crear una aplicación para proteger los archivos que son utilizados por los usuarios de la Biblioteca Virtual de la PUCESA.

1.5.1 Hardware

La Biblioteca Virtual cuenta el siguiente Hardware:

- Un Servidor con las siguientes características:

  Intel Pentium III de 650 MHZ

  Con 256 MB de Memoria RAM y Disco Duro de 30 GB

  Monitor de 17'' marca Qbex

  1 Impresora Lexmark Z32 la misma que esta compartida

  Tarjeta de video de 32 MB

  CD-ROM de 52X

  1 HUB encore de 16 puertos

  1 (Ethernet – USB) 128 x 192 Mbps

  Cable UTP categoría 5 (8 hilos)

  7 supresores de picos de 4 tomas

  1 UPS de 6 tomas que van conectados al servidor.

- 6 terminales con las siguientes características:

  Intel Pentium II (r) de 600 MHz

  Con 256 MB de Memoria RAM y Disco Duro de 20 Gb

  Monitor de 14" marca Qbex

  Multimedia y CD-Rom de 56X

1.5.2 Software

El software que se utiliza es:

Internet Explorer 6.0

Microsoft Office 2000 Profesional

Proxy Wingate 4.4

1.5.3 Software con licencias libres

Messenger MSN 6.2

Winzip 9.0

AnalogX 1.4

Antivirus

1.5.4 Sistema Operativo

Windows XP Profesional (Servidor)

Windows 98 Segunda Edición (Terminales)

1.6 ORGANIZACIÓN DEL TRABAJO

La organización del trabajo se refiere a los documentos, presentaciones y diseños que son realizados por los estudiantes y profesores de la PUCESA.

Estos documentos necesitan de algunas seguridades con el fin de que no puedan ser modificados, borrados o copiados sin la autorización de la persona o personas que hayan realizado dicho trabajo, o de la persona de la Biblioteca Virtual de la PUCESA.

Una forma de prevenir los ataques locales y también de red en los archivos que se utilizan en la Biblioteca Virtual es desarrollando una aplicación que verifique la integridad de la información almacenada en los archivos.

CAPITULO II

LEGISLACIÓN

2.1 PROTECCIÓN DEL DERECHO A LA INTIMIDAD Y PRIVACIDAD

Se considera a los derechos de autor como una moderna disciplina jurídica que nace de la necesidad de regular la particular relación del autor con su creación intelectual y de ésta con la sociedad.

En la actualidad los derechos de autor tienen gran importancia principalmente por el desarrollo tecnológico y considerable crecimiento del comercio internacional que se ha experimentado en las últimas décadas; por ello surge la necesidad de contar con una legislación adecuada para enfrentar estos fenómenos y los próximos desafíos que vendrán; pues se han generado problemas nuevos relativos a los derechos de autor, sobre categorías de obras y nuevos modos y medios de utilización de obras existentes.

La protección legal a los autores viene a constituirse en un estímulo para la creación intelectual por ello los derechos de autor, persiguen una compensación por el esfuerzo desplegado en la producción, y esa retribución que reciben los autores sirve de estímulo para el esfuerzo creativo, fomenta el progreso intelectual de nuestro país y le añade una ventaja comparativa en el nuevo orden económico mundial.

(Referencia Bibliográfica: Manual Legal para el Empresario).

Por otro lado, antes de llegar a los tribunales cabe la opción del arbitraje y la mediación en el Centro de mediación y Arbitraje, a nivel internacional aunque ya existen este tipo

de instituciones a nivel nacional como es la Comisión Mediadora y Arbitral de la Propiedad Intelectual.

El objetivo consiste en lograr que los archivos permanezcan invisibles a los ojos del pirata o que si resultan detectadas sean imposibles de eliminar sin deteriorar la calidad del objeto que las contiene.

2.2 ACTOS Y NEGOCIOS JURÍDICOS ELECTRÓNICOS

Siendo el Internet la fuente principal de los archivos de consulta para la Biblioteca Virtual, se hace referencia el tema del comercio electrónico y los negocios jurídicos que ahí se realizan, aclarando que parte de estos negocios es el software de consulta.

Desde una perspectiva jurídica, el comercio electrónico plantea nuevos problemas cuya solución puede canalizarse por medio de tres vías, independientes pero complementarias entre sí; a saber, por la adaptación de los institutos jurídicos aplicables al comercio tradicional, por el establecimiento de un marco jurídico propio y por la autorregulación de los sectores implicados mediante la adopción de códigos de conducta. El comercio electrónico está supeditado, en gran medida, a la creación de una normativa específica apta para fomentar la seguridad y la confianza de los actores involucrados y resolver así ciertos problemas de dimensión global (por ejemplo, la protección de la propiedad intelectual, la privacidad de los datos personales, la autenticación y la seguridad en las transacciones electrónicas, la protección de los consumidores y la tributación, por citar los más significativos).

Para lograr que las redes de comunicaciones libremente accesibles, como Internet, se conviertan en un canal adecuado para el desarrollo del comercio electrónico es necesario que se den las siguientes condiciones:

2.2.1 La confidencialidad:

Una condición elemental para que el público confíe en el comercio electrónico es que los datos, los mensajes y, en general, la información que circula por las redes no sea inteligible para terceros no autorizados que tengan acceso a ella voluntaria o accidentalmente. No obstante, la confidencialidad de las comunicaciones electrónicas es fácilmente alcanzable gracias a los diversos sistemas de cifrado o encriptación existentes en la actualidad.

2.2.2 Seguridad técnica:

Se trata, por una parte, de que el ordenamiento jurídico reconozca y regule los métodos técnicos que garantizan la confidencialidad y la integridad de la información que circula por las redes, principalmente los métodos criptográficos que permiten ocultar el verdadero contenido de un mensaje o documento electrónico a aquellas personas que carecen de determinada información, generalmente denominada clave.

2.2.3 Seguridad jurídica:

En este caso se trata, con carácter general, de que el ordenamiento jurídico reconozca el fenómeno social y económico que representa el comercio electrónico y "legalice" las nuevas vías de contratación electrónica.

En particular, resulta necesario que el marco legal reconozca la eficacia de los negocios jurídicos que se realizan por medios electrónicos, asimile la validez y

eficacia de la firma electrónica y determine los derechos y obligaciones de los consumidores, usuarios y empresarios electrónicos.

2.3 CONTRATACIÓN ELECTRÓNICA INFORMÁTICA

El Comercio Electrónico, puede definirse como todo intercambio de datos por medios electrónicos, esté asociado o no con la actividad comercial en sentido estricto. De forma más estricta, puede definirse como toda transacción o intercambio de información comercial realizada por vías electrónicas como Internet, el comercio electrónico no sólo comprende la compra-venta electrónica de bienes y servicios, sino también las actividades previas y posteriores al negocio propiamente dicho (por ejemplo, la publicidad, la atención al cliente antes y después de la venta y los pagos electrónicos).

2.3.1 La autenticidad de la identidad de las partes:

Se trata, por ejemplo, de que las partes de un contrato formalizado electrónicamente tengan la seguridad que el consentimiento es prestado por quien debe hacerlo y no por un tercero que desde un computador pretende usurpar la identidad de otro.

2.3.2 La integridad del documento electrónico:

Si es necesario conocer de forma inequívoca la identidad del transmisor y el receptor de un documento electrónico, también lo es que éstos tengan la seguridad de que el contenido de ese documento no ha sido alterado durante el uso por las redes públicas o, cuanto menos, que tengan conocimiento de que las alteraciones se han producido.

2.3.3 La prueba de la transacción electrónica:

En toda transacción electrónica es igualmente importante tener la certeza de que el documento ha sido efectivamente enviado y recibido por todas las partes que intervienen en ella, así como tener la posibilidad de demostrarlo. En esta ocasión, la firma electrónica, gracias a un sistema de claves, permite vincular a una persona concreta con un texto determinado y probar que ha sido aquella la remitente o receptora de este último.

En conclusión, resulta fundamental dotar a los negocios jurídicos electrónicos, y en especial a los que se canalizan a través de redes abiertas como Internet, de un marco legal que proporcione el adecuado grado de seguridad técnica y jurídica.

2.3.4 Marco legal del comercio electrónico:

Antes de iniciar una actividad de comercio electrónico, las empresas deben tener en cuenta los siguientes aspectos jurídicos con el propósito de tomar las medidas preventivas necesarias para evitar los denominados "costes de error".

- La protección de los distintos elementos que integran un sitio Web;
- El conflicto entre marcas y nombres de dominio;
- La publicidad comercial;
- La protección de los datos automatizados de carácter personal;
- La contratación electrónica;
- La prueba de la aceptación del contrato.

2.3.5 Contratos Informáticos:

En un sentido amplio, se consideran contratos informáticos aquellos que tienen por objeto la prestación de bienes y servicios informáticos.

- La protección del software a través del derecho de autor

Nuestra legislación considera al software como obras literarias y los protege como tales. La protección se otorga independientemente de su incorporación en un computador y cualquiera sea la forma legible por el hombre (código fuente) o en forma legible por computador (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

- Categorías de los programas protegidos y condiciones para su protección
- Software creado por autores independientes (por encargo, en colaboración, colectivo)
- Software creado por autores asalariados
- Contenido y Duración de estos derechos
- Medidas de protección en el ámbito penal
- Medidas de protección en el ámbito civil

2.4 PROTECCIÓN JURÍDICA DEL SOFTWARE Y HARDWARE

El propósito es regular el uso legítimo de programas de computación a fin de evitar la copia ilegítima de los mismos, para lo cual se deberá verificar previamente la titularidad del programa del computador.

2.4.1 Protección del software por medios diferentes del derecho de autor

- Protección del Software por el Derecho de Patentes
- Protección del Software por el Derecho de Marcas
- Protección del Software por el Derecho sobre Dibujos y Modelos Industriales y Artísticos
- Protección Jurídica del Software por la vía Civil
- Protección Jurídica del Software por la vía Penal

2.5 DELITOS INFORMÁTICOS

Se puede definir al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático contra los derechos y libertades de los ciudadanos".

Se entenderán como "delitos informáticos" por tanto todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, y que hacen uso indebido de cualquier medio informático.

2.5.1 Sujeto pasivo en el delito informático

El sujeto pasivo del delito, es sumamente importante; se deduce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro, una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento, por ello se cree que la formación del usuario es una clave primordial para su eficaz protección, y permitir al usuario saber como actuar en caso de que su sistema sea atacado.

2.5.2 Sujeto activo en el delito informático

Los sujetos activos tienen habilidades o son expertos para el manejo de los sistemas informáticos y generalmente se encuentran en lugares estratégicos donde se maneja información de carácter sensible. Sin embargo, la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" e incluso despiertan cierta simpatía.

2.5.3 Clasificación del delito informático

- **Como método**.- actos en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

- **Como medio**.- actos en donde para realizar un delito utilizan un computador como medio o símbolo.

- **Como fin**.- actos dirigidos contra la entidad propietaria del sistema informático para causarle daños o perjuicios.

2.5.4 Fraudes cometidos mediante manipulación de computadoras

2.5.4.1 Manipulación de los datos de entrada.- Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

2.5.4.2 Manipulación de programas.- Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

2.5.4.3 Manipulación de los datos de salida.- El ejemplo más común es el fraude de que se hace a los cajeros automáticos mediante la falsificación de instrucciones al computador en la fase de adquisición de datos. En la actualidad se usan ampliamente equipos y programas especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

2.5.4.4 Fraude efectuado por manipulación informática.- Aprovecha las repeticiones automáticas de los procesos de cálculo y transferencia. Es una técnica especializada apenas perceptible que hace que en el proceso de grandes transacciones financieras, se vayan sacando cantidades repetidamente de una cuenta y se transfieren a otra.

2.5.4.5 Falsificaciones informáticas.

2.5.4.5.1 Como objeto.- Cuando se alteran datos de los documentos almacenados en forma automatizada.

2.5.4.5.2 Como instrumentos.- Son las fotocopiadoras que pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

2.5.4.6 Daños o modificaciones de programas o datos computarizados.

Sabotaje informático.- Es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático con intención de obstaculizar el funcionamiento normal del sistema.

2.5.4.7 Acceso no autorizado a servicios y sistemas informáticos.

- Piratas informáticos o hackers.- el acceso se efectúa a menudo desde un lugar exterior, situado en la red, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar

la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

2.5.4.8 Reproducción no autorizada de programas informáticos de protección legal.- Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Quizás sea este el delito mejor tipificado actualmente de todos los mencionados hasta el momento. El problema ha alcanzado dimensiones internacionales con el tráfico de esas reproducciones no autorizadas a través de Internet en muchos de los casos.

2.6 TELECOMUNICACIONES Y DERECHO

La Ley de Telecomunicaciones vigente se expidió el año 1992 y fue objeto de reformas en los años 1995 y 1997; además de las reformas introducidas en el año 2000, mediante la Ley para la Transformación Económica del Ecuador y la Ley para la Promoción de las Inversiones, con las cuales se abrió este sector a la libre competencia. Sin embargo, no hay que olvidar que, en agosto de 1998 se expidió la actual Constitución, lo cual implicó un cambio radical, puesto que durante la vigencia de la Constitución de 1979, las telecomunicaciones eran un monopolio del Estado, mientras que en la actualidad, deberán desarrollarse bajo los principios de la libre competencia. Como consecuencia de la vigencia de la actual Constitución la Ley Especial de Telecomunicaciones ha quedado obsoleta, el espíritu original, de ser un instrumento que consagra el monopolio estatal, todavía no ha sido totalmente eliminado con las reformas, ni se ha establecido herramientas que permitan la regulación y el control de un mercado en libre competencia.

La Ley Especial de Telecomunicaciones, vigente desde agosto de 1992, separó por primera vez en el país, el Control y la Regulación de la Operación de los servicios de telecomunicaciones. Para el Control y la Regulación se creó la Superintendencia de Telecomunicaciones.

2.7 DERECHO INFORMÁTICO E INTERNET

Derecho Informático es una disciplina inequívocamente integrada por las sentencias de los tribunales sobre materia informática y las proposiciones normativas, es decir, los razonamientos de la ciencia del derecho dirigidos al análisis, interpretación, exposición, sistematización y critica del autor normativo que regula la informática.

En el concepto de derecho informático se mencionará las diferentes fuentes y estructuras temáticas en el ámbito del derecho público (regulación del flujo intersección de datos informáticos, libertad informática o los delitos informáticos) y del Derecho Privado (contratos informáticos), sistema de protección jurídica de los programas de computadoras.

2.7.1 ¿El Derecho Informático es una Ciencia?

El derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal es el caso de lo civil, penal y contencioso administrativo.

Por lo tanto el Derecho Informático cumple con los principios básicos de toda ciencia: posee conocimientos, principios, doctrinas, y que tienen como marco amplio a la cibernética.

2.8 DERECHOS DE AUTOR DE LAS PÁGINAS WEB

Las páginas Web permiten darnos a conocer a la comunidad internacional y comercializar nuestros productos o servicios a través de la red, o simplemente proveer de información para que otros la puedan tener en sus manos cuando la necesiten. Los documentos no solo incluyen texto, sino además gráficos, sonido o imágenes en movimiento.

Aunque la información disponible es ya abundante, no será fácil encontrar justo lo que queremos porque en ocasiones no está la información que buscamos.
Este desarrollo hace necesario regular y reconocer "nuevas" propiedades, como parte de nuevos mercados, que toman cada día mayor relevancia desde un punto de vista económico y comercial, nace el régimen del derecho de autor.

Como todo derecho, el derecho de autor toma su valor no sólo de sus efectos sino principalmente por la aceptación de medios jurídicos, establecidos por el Estado o reconocidos por toda la sociedad, tendientes a protegerlo frente a terceros y a regular su transferencia y transmisión para bien.

La difusión "inevitable" de la información y consecuentemente de las obras del intelecto, hace necesaria una protección eficaz que se hace difícil frente a un bien especialísimo que no entiende de soportes ni de limitaciones físicas, como es la creación intelectual.
Se hace necesario controlar en forma efectiva la reproducción no autorizada, circulación, edición, modificación y en general todo acto que afecte o restrinja, ilícitamente, derechos que emanan del reconocimiento que la sociedad hace al autor de la obra.

La gestión colectiva "se impuso por necesidad" dada la limitación física del autor de controlar su obra en el mercado. Este control puede hacerlo de mejor manera un organismo dedicado, la sociedad de gestión colectiva, que pueda defender los derechos de sus asociados. Una defensa más factible, económica y "publicitada" que aquella individual del autor o creador.

Por último estas sociedades están obligadas a contratar, con quién lo solicite, la concesión de autorizaciones no exclusivas de los derechos de autor y conexos que administren, de acuerdo con tarifas generales que determinen.

Las sociedades de gestión colectiva ejercen la representación judicial y extrajudicial de asociados tanto nacionales como extranjeros.

Las razones que imperan a la hora de optar por un sistema de gestión colectiva en materia de derecho de autor son claras: la posición de "inferioridad económica del creador respecto a la explotación de sus obras"; como también una posición de inferioridad técnica y jurídica, respecto a la gestión misma como a su defensa por el derecho.

Las características principales de los derechos de autor son las siguientes:

"los derechos de autor nacen y se protegen por el solo hecho de la creación de la obra"

"se protegen todas las obras sin importar cual sea el país de origen de la misma, la nacionalidad o domicilio del autor"

"la duración de la protección es limitada en el tiempo"

(Referencia Bibliográfica: "Manual Legal para el Empresario")

Internet es sinónimo de multimedia y de digital. La obra multimedia es esencialmente una elaboración integrada por partes diversas. Un obra de obras que implica su percepción por más de un sentido. La obra multimedia pide por esencia una actividad de colaboración entre varios agentes y en ciertos casos en la formación de una verdadera comunidad creadora.

Así, se comenzará refiriendo a la Página Web como obra protegida, centrándose en su encuadre dentro de la Propiedad Intelectual, así como en los mecanismos de protección que ofrece el Derecho.

El otro aspecto al que se hace mención es el de los Contratos de desarrollo de Páginas Web, como contratos característicos y muy relacionados con los derechos de Propiedad Intelectual.

2.8.1 La Página Web como Obra Protegida por la Propiedad Intelectual.

Es necesario indicar que en una Página Web se deben tener en cuenta tres elementos esenciales:

- La información contenida en la Página.
- El diseño.
- El software que va a permitir al usuario el acceso y visualización de la misma.

2.8.2 Protección de la Página Web.

Una Página Web está formada por elementos preexistentes y por elementos de nueva creación.

Los preexistentes pueden ser susceptibles de protección intelectual por ejemplo: dibujos, videos, texto o fotografías. Con ello se quiere decir que para poder incluir estos elementos en un Sitio Web es necesario la autorización del titular, a no ser que estas obras sean de dominio público. Esta autorización es aconsejable se realice por escrito y recopile las actividades que se pueden realizar, es decir, si se autoriza o no una comunicación pública o una reproducción.

Cuando ya se hayan obtenido las respectivas autorizaciones sobre las obras que van a estar recogidas en la Página Web, es necesario protegerla en su conjunto, para poder probar la titularidad de la misma. Esto se puede realizar a través de dos mecanismos:

- **Inscripción en el Registro de Propiedad Intelectual (IEPI):** Se pueden inscribir los contenidos, el código fuente y el diseño. El inconveniente de este mecanismo está en que cada vez que cambie alguno de estos elementos, será necesario inscribirla nuevamente.

- **Depósito notarial:** El Acta que se levante deberá recoger los elementos que se depositan, es decir, contenidos, código fuente, diseño y las circunstancias que hacen de la Página Web como una obra única. El inconveniente de este mecanismo radica en su alto coste en relación con el mecanismo anterior.

El desarrollo de una Página Web es un aspecto crucial en el comercio electrónico, ya que es a través de ella que los usuarios interactúan con la empresa y adquieren sus productos o servicios, considerando que en muchos casos, la Página Web es el producto o el servicio. Además de esto, la Página Web es un producto de marketing porque un diseño atractivo es capaz de atraer a más clientes. En definitiva, en el comercio electrónico, la Página Web es "la cara de la empresa en Internet".

Tanto el proyecto, como la materialización del mismo van a aparecer en un mismo contrato que es el de desarrollo de Página Web que, en definitiva, es un contrato por el que una entidad diseña una Página Web para otra.

Se pueden revisar, reproducir o traducir extractos de la información del sitio web con fines de investigación o de estudio personal, pero no para la venta u otros usos relacionados con fines comerciales. Siempre que se utilice información del sitio web deberá indicarse la dirección URL del artículo.

Para reproducir o traducir una gran porción del sitio web, o para toda utilización que no sea con fines educativos o fines no comerciales, deberá obtenerse previamente una autorización explícita por escrito. Las solicitudes o consultas al respecto deben dirigirse al programa responsable de la página en mención.

Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto.

La reproducción de un programa de computación, incluso para uso personal, exigirá la autorización del titular de los derechos, con excepción de la copia de seguridad.

No constituye reproducción ilegal de un programa de computación, la introducción del mismo en la memoria interna del respectivo computador, para efectos de su exclusivo uso personal.

CAPITULO III

SEGURIDAD

3.1 INTRODUCCIÓN

En términos generales, la seguridad de archivos se considera la "libertad para usar las computadoras sin temor a interrupciones o interferencias consideradas externas".

(Referencias Bibliográficas: www.Kriptopolis.com)

Todos desean estar libres de las consecuencias negativas.

El preocuparse por la seguridad implica que hay algo valioso que necesita protección.

¿Cuales son los principales problemas de seguridad a los que se enfrentan los responsables de los sistemas de información o de archivos de las agencias gubernamentales? la respuesta sería la falta de conciencia entre los usuarios de las computadoras.

3.2 SEGURIDAD INFORMÁTICA

3.2.1 INTRUSOS

3.2.1.1 Acceso - Uso - Autorización

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

· Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.

· Pero, cuando un intruso hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

3.2.1.2 Detección de Intrusos

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron web sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realiza comparaciones. El estudio se realizó empleando técnicas sencillas y no intrusivas.

3.2.1.3 Identificación de Amenazas

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del intruso.

3.2.1.4 Tipos de Ataque

Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los operadores, programadores utilizaban sus permisos para alterar archivos o registros.

Cabe destacar que para la utilización de estas técnicas no era necesario contar con grandes centros de cómputos, lo que queda fehacientemente demostrado al saber que algunos Hackers más famosos de la historia hackeaban con computadoras (incluso armadas con partes encontradas en basureros) desde la habitación de su hogar.

3.2.1.5 Ingeniería Social

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele tolo lo necesario para superar las barreras de seguridad. El atacante puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

3.2.1.6 Ingeniería Social Inversa

La Ingeniería Social Inversa es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados acerca de las técnicas de Ingeniería Social.

3.2.1.7 Ataques de Monitorización

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

3.2.1.8 Ataques de Autenticación

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

3.2.1.9 Spoofing-Looping

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios.

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

Looping es donde una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacados por un Insider, o por un estudiante a miles de Km de distancia, pero que ha tomado la identidad de otros.

3.2.1.10 Ataques de Modificación - Daño

Se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluso el borrado de archivos). Los atacantes tienen la capacidad de disparar cualquier

comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

3.2.1.11 Borrado de Huellas

El borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema.

3.2.2 POLÍTICAS DE SEGURIDAD

Los sistemas informáticos, además de ser eficientes, deben brindar condiciones de seguridad para garantizar la privacidad de los datos confidenciales, el mantenimiento de la integridad de los datos y de los programas que los manejan, y la disponibilidad de la información para los usuarios autorizados. Esto se logra implementando políticas de seguridad adecuadas que contemplen los siguientes conceptos fundamentales:

1. Identificación y autenticación de los usuarios.
2. Autorización de acceso a la información.
3. Encriptado de los datos confidenciales.

La seguridad informática es el conjunto de técnicas y procedimientos que garantizan la integridad, confidencialidad y disponibilidad del sistema:

- **Integridad:** el sistema debe funcionar conforme a las especificaciones de diseño, garantizando un sistema consistente, de forma que la información sea

exacta (para lo que debe estar actualizada), autorizada y completa (previniendo eventuales pérdidas), por consiguiente, absolutamente fiable.

- **Confidencialidad:** el sistema debe ser accesible sólo por las partes autorizadas, de forma que cada persona acceda únicamente a la información que le corresponde.

- **Disponibilidad:** el sistema debe proporcionar servicios y datos a los usuarios en un periodo de tiempo aceptable.

El desarrollo creciente e imparable de las tecnologías de la información y las comunicaciones, amenaza al menos potencialmente la esfera de la privacidad personal, en mayor medida que los anteriores métodos manuales. La informática posibilita, hoy en día, la transmisión, almacenamiento y consulta de datos, en apenas segundos, en rápido viaje a través del tiempo y el espacio.

Una de las claves de una seguridad efectiva en informática personal para una organización es una normativa de seguridad. Esta puede definir reglas, principios y procedimientos que regulen la forma en que la organización gestiona, protege y controla sus recursos de informática personal y la información que contienen.

Obviamente una normativa de seguridad no ofrece seguridad por sí misma, pero se trata de una herramienta muy efectiva, es un estándar que puede dar un nivel de cumplimiento y la base de posteriores mejoras.

Al crear tu cuenta, puedes proporcionar una pregunta y respuesta secreta (que sólo tú puedas contestar), para definir una nueva clave de acceso, en el caso de que se te olvide.

3.2.2.1 Control de Acceso a los Datos

Los controles de acceso a los datos se diseñan para prevenir accesos no autorizados, debiendo poner especial cuidado en la protección de información confidencial.

3.2.2.2 Largo mínimo de claves de acceso (password)

Es conocido que un atacante tratará de capturar y/o descifrar el password con distintos métodos, "manuales" o con herramientas de "cracking" como los programas de ataque con diccionario. Las claves con solo algunos caracteres son fáciles de descubrir que con aquellas que tienen al menos ocho caracteres.

3.2.2.3 Es obligatorio capacitar a todos los usuarios sobre la seguridad de la información

La intención de esta política es requerir el suficiente entrenamiento y documentación para todos aquellos que manejan información de la empresa. El nivel de capacitación necesario deberá ser acordado por un responsable designado o en empresas más grandes, por el departamento de seguridad informática, quien deberá asegurar que ese nivel se mantenga permanentemente.

3.2.2.4 Control de acceso físico a las áreas con información sensitiva

La intención de esta política es antes que nada requerir la restricción física a cualquier sitio o área donde la información estratégica pueda ser expuesta a robo o ataque, sin especificar tecnología o método de protección ya que la información puede estar expuesta en listados, viajar a través de la línea telefónica o en cualquier otro lugar.

3.3 SEGURIDAD EN INTERNET

En Internet, y otras redes electrónicas, es vital disponer de seguridad para las comunicaciones y más aun cuando se realizan transacciones.

El manejo de la seguridad implica varios componentes fundamentales. Se requiere de Hardware y software adecuado, pero principalmente de procedimientos que se observen y políticas de seguridad que sean ejecutadas sin excepciones.

3.3.1 Motivación

Tradicionalmente la seguridad de las conexiones a Internet se basa solo y exclusivamente en la compra e instalación de un cortafuego.

Los Administradores de Seguridad expertos saben que la existencia de un cortafuego ayuda, pero está muy lejos de ser la solución definitiva.

Se deben configurar de forma adecuada todos los dispositivos o servidores involucrados en dicha conexión, de forma continua y profunda.

3.3.2 Riesgos de Internet

Casi todas las compañías proporcionan a los empleados acceso al Internet y acceso remoto a las redes corporativas.

Todavía, menos de la mitad de las compañías realizan los cheques rutinarios de seguridad, sólo el 44 % tienen la capacidad para seguir el acceso a los datos sensibles y solamente una mitad usa el cifrado de datos (encriptación).

Mientras que el 75 % dicen que ellos quisieran restringir el acceso solamente a ciertas partes del Internet, sólo el 62 % tienen las políticas que gobiernan el acceso Internet, el 42 % no vigilan el uso de Internet del empleado y solamente 30 % aplican realmente los controles de acceso.

3.4 SEGURIDAD EN LOS SERVICIOS DE CONEXIÓN: SSL

Se ha desarrollado un protocolo denominado Secure Sockets Layer (SSL), que gestiona la seguridad en el nivel inmediatamente superior al Network Layer (niveles OSI en los servicios de red), es decir, entre la conexión a Internet (protocolo TCP/IP) y las aplicaciones (servicios) que utiliza el usuario. De esta forma es posible garantizar una conexión segura para distintos servicios de red.

Básicamente, el SSL facilita un canal de comunicación seguro, con encriptación y certificación de los datos que se transmiten.

Las características del SSL son las siguientes:

- puede ser utilizado por los servicios principales: SMTP (mail), HTTP (web), FTP (transferencia de archivos)

- autentificación (comprobación de la firma digital) bidireccional mediante certificados RSA, etc.
- facilita un canal encriptado para el envío de datos "sensibles"
- es posible usar SSL combinado con otros sistemas de seguridad, por ejemplo, sockets

Los programas modernos con los que se accede a los distintos servicios, también pueden utilizar los protocolos SSL de forma transparente para el usuario final. Obviamente, antes de cada conexión es necesario facilitar la contraseña correspondiente para poder utilizar el certificado personal, firma digital, encriptación, etc.

3.5 SEGURIDAD DE SOFTWARE

En términos generales se puede definir que el Software es un conjunto de programas para llevar a cabo un objetivo específico y a su vez un programa es un conjunto de instrucciones que realizan una tarea para cumplir dicho objetivo.

3.6 LICENCIAS

3.6.1 Tipos de licencias para software redistribuible libremente.

Los autores de software redistribuible libremente (SRL) han decidido distribuir su trabajo bajo varias licencias diferentes. Los propósitos filosóficos y/o económicos han conducido a diferentes licencias de

redistribución libre (LRL), variando en función de las actividades que requieren, permiten o prohíben respecto al uso y distribución.

3.6.2 Las Licencias de Uso

Uno de los aspectos más importantes en el uso y desarrollo de software son las licencias de uso.

La licencia de uso es el contrato legal que el usuario acepta cumplir en el uso y desarrollo de un programa informático. En lo que se refiere a uso, las licencias pueden limitar lo que se puede hacer con los programas, y en lo que se refiere a desarrollo, es posible que la licencia imponga condiciones sobre la distribución de programas desarrollados con una herramienta particular.

Antes de discutir lo que una licencia permite, es bueno aclarar el significado de: Copyright (c).

¿Qué quiere decir esa línea? Simple: que los derechos de copia pertenecen a una compañía, empresa o institución.

CAPITULO IV

FICHEROS

4.1 SEGURIDAD DE ARCHIVOS

La seguridad de archivos permite a los usuarios impedir que intrusos no deseados alteren o destruyan su información. De esta manera se asegura la integridad de la información entre la red privada e Internet u otras redes públicas.

La seguridad interna permite que el acceso a los datos sea realizado únicamente por personal autorizado dentro de una red de área local. Para ello, es determinante establecer los controles más adecuados.

Se requiere entonces crear infraestructuras complementarias que ofrezcan altos niveles de seguridad.

Para garantizar la óptima implementación de un sistema de seguridad se requiere que la organización tenga claramente definidas las políticas, procedimientos y controles necesarios para el acceso a la información dentro de un ambiente seguro.

Un Test de Intrusión confirmará que sus sistemas están configurados correctamente.

4.1.1 ¿Por qué realizar un Test de Intrusión periódicamente?

Mediante un Test de Intrusión regular se asegurará de que la seguridad de los archivos utilizados en la Biblioteca Virtual de la PUCESA sea siempre la óptima.

4.1.2 ¿Cómo se realiza el test?

En un Test de Intrusión se analiza la red que está instalada en la PUCESA desde el exterior, tal y como un hacker lo haría. El test puede dividirse en 2 fases:

1.- Obtención de información: Mediante el uso de varias herramientas y utilidades se recopila información sobre los sistemas operativos y servicios visibles desde el exterior.

2.- Identificación y explotación de vulnerabilidades: Con esta información se confecciona una lista de posibles vulnerabilidades y se recopila las herramientas necesarias para "explotar" dichas vulnerabilidades.

4.1.3 ¿Cómo encaja un Test de Intrusión en el conjunto de seguridad?

Representa una parte de una solución de seguridad completa, midiendo el nivel de riesgo de los sistemas expuestos a Internet. Es necesario adoptar una política de seguridad correcta, para proteger su información y el tipo de riesgo al que se enfrenta.

Realizar un Test de Intrusión periódicamente es el único método efectivo de comprobar la integridad de los archivos que se utilizan en la Biblioteca Virtual de la PUCESA, garantizando que cumplen con los niveles de seguridad para los que fueron diseñados.

4.1.4 Objetivo

El objetivo de un Test de Intrusión es el de ver la Biblioteca Virtual de la PUCESA desde el punto de vista del atacante externo que intenta penetrar en su red corporativa. De esta forma, se puede evaluar el riesgo al que se enfrentan los archivos conectados a Internet y las posibilidades reales de acceder, interceptar y modificar la información que contiene los archivos.

4.2 PAQUETES INFORMATICOS

Los paquetes informáticos permiten tener mayor profundidad en los estudios, rapidez al evaluar alternativas, y considerar más variables, que antes eran imposibles, con procedimientos manuales o con programas de cómputo elementales y computadoras de menos capacidad.

El comercio de paquetes informáticos es globalizado y puede adquirirse cualquier software mediante transacciones por Internet. Además, la oferta mundial de paquetes informáticos es grande y de alta movilidad; de manera que es necesario tener identificadas revistas, instituciones, congresos, exposiciones y otros apoyos especializados, dirigidos a ayudar a conocer que existe algo "nuevo" para la ingeniería, y facilitar las evaluaciones y comparaciones entre paquetes relativamente equivalentes.

4.3 FORMATOS DE PROGRAMAS

4.3.1 Portable Data File (PDF)

El formato del documento portable de Adobe, (Portable Document Format, PDF) es uno de los formatos estándares utilizados mundialmente en la distribución de documentos electrónicos. PDF de Adobe es un formato de archivo universal que conserva todas las fuentes, formatos, colores y gráficos de cualquier documento de origen creado en cualquier aplicación y plataforma.

Los archivos PDF son compactos y cualquiera puede compartir, visualizar, explorar e imprimir tal y como fueron creados con dicho software antes mencionado.

Dicho software protege en parte a los derechos de propiedad literaria de autores y publicadores.

Está diseñado para satisfacer los requisitos de almacenamiento seguro de datos en formatos PDF.

4.3.1.1 Problemas Comunes

- Los destinatarios no pueden abrir los archivos porque no tienen las aplicaciones que se utilizaron para crear los documentos.
- Debido a la incompatibilidad entre plataformas, software y versiones se pierde formato, fuentes y gráficos.
- Algunos documentos no se imprimen de forma correcta debido a limitaciones del software o de la impresora.

El Software que proporcionan es "Tal Cual" y Adobe no le proporciona garantía alguna en lo relacionado con su utilización o rendimiento.

Una gran parte de los datos se tienen que almacenar durante largos periodos de tiempo en cumplimiento de normas estrictas, o para su utilización como pruebas en casos de posibles violaciones de patentes o de protección de propiedad intelectual.

4.3.2 Postscript (PS)

La idea principal sobre la que está basado el PostScript, fue creada hace veinte años por John Gaffney en la Evans & Sutherland Computer Corporation.

Al principio se llamaba "Design System" pero más tarde fue desarrollado bajo el nombre de PostScript por Adobe Systems Incorporated como una herramienta independiente de la plataforma y del dispositivo para la descripción de páginas. Actualmente es una de las herramientas de preparación de documentos más importantes, aunque no es utilizada directamente por la mayoría de usuarios. Sus capacidades están completamente a alto nivel, sin embargo muchos usuarios que no quieren entrar en los detalles de este potente lenguaje prefieren usar las otras herramientas de usuario final.

Ha sido especialmente diseñado para comunicar un documento creado por un computador a un dispositivo de impresión. Es una descripción de alto nivel, ya que describe las páginas como una serie de objetos abstractos, es decir, en base a coordenadas, formas, curvas y funciones en lugar de describirlas a un nivel detallado enviando el valor de cada píxel de la página.

El PostScript es una tecnología independiente del dispositivo y la plataforma que sirve para describir documentos. Los programas PostScript son interpretados, y pueden ser generados de tres formas distintas: directamente por un programador, generados por un programa de aplicación o introducidos en aquellas impresoras que soportan un modo interactivo.

Los operadores gráficos de que dispone PostScript permiten trabajar con tres tipos de objetos:

- **Texto**, que puede presentarse en una gran variedad de fuentes, situado en cualquier punto de la página, con cualquier orientación y a cualquier escala.
- **Figuras geométricas**, formadas por líneas rectas, así como curvas de cualquier tamaño, orientación y grosor, así como rellenos de cualquier forma, tamaño y color, con una gran variedad de tramas.
- **Imágenes procedentes de programas de aplicación o fotografías digitalizadas.** Que pueden colocarse en cualquier sitio, con cualquier orientación y escala.

Para PostScript, la composición de una página se asienta en tres conceptos fundamentales:

- **La página actual**. Es una página virtual en donde PostScript dibuja. Al comienzo de un programa, la página actual se encuentra vacía. Los operadores PostScript rellenan la página, que una vez compuesta es enviada a la impresora.
- **La trayectoria actual**. Es el conjunto de puntos, conectados o no, líneas y curvas, con la descripción de formas y tamaños. Este conjunto puede definirse independientemente de la resolución de la impresora.
- **La zona activa.** Es el contorno del área que va a ser dibujada. Inicialmente, la zona activa coincide con el tamaño por defecto del papel para la impresora. La zona activa puede ser dimensionada a cualquier tamaño y forma. Si un operador trata de dibujar fuera de la zona actual, es ignorado.

4.4 ESTRUCTURA INTERNA DE PROGRAMAS

Se inventa un documento técnico generalmente de elementos diferentes que se crean con diferentes aplicaciones. Por consiguiente se trata de desarrollar el documento con una aplicación baja y manejar elementos diferentes.

Windows da resultados buenos para desarrollar texto documental, por compartir información con otras aplicaciones, y por la inserción de gráficos.

Hoy, el más extensamente medio de comunicación de la distribución usada es el World Wide Web, y los formatos que recomienda esta Web compatible.

Es importante mantener el esquema y apariencia del documento, ya sea Portable Document Format (PDF) o PostScript (PS) ambos formatos son satisfactorios. Si la apariencia no es esencial y la naturaleza del documento es dinámico se debe convertir a HTML.

Crear Texto.- Se escribirá todo el texto en la aplicación Microsoft Word. Pero más tarde se convertirá el documento a cualquiera de los formatos más conocidos como: **PDF o PS**, se debe estar informado de algunas restricciones para obtener buenos resultados.

Recomendaciones Generales.- Independientemente del formato que se escoja para archivar se recomienda lo siguiente:

- **Conjuntos de Caracteres en Documentos:** Use un solo tipo de caracteres, especialmente a lo que se refiere a la familia Times.
- **Estilos:** Use la opción del Estilo en el menú del formato, especialmente por Titulos.

- **Tablas:** Si quiere realizar una tabla sin bordes, use el menú de la tabla, no usar tabulaciones o espacios del cursor.

A continuación se explica las recomendaciones particulares y restricciones con cada formato de archivo.

Formato PDF

Si se usa el escritor Acrobat para convertir el documento que fue realizado en Word a formato PDF, no se tendrá muchos problemas, debido a que el PDF copia será idéntico al documento original en este caso de Word.

Para un archivo PDF, se debe tomar aflicción a las mismas restricciones como en traducir documentos de Word a formato PS.

Formato PS

Para crear un archivo PS, se necesita imprimir un archivo PS copia a disco, pero PS impresoras no tienen todos los conjuntos de caracteres que Word u otras aplicaciones dejan que sean usadas por el usuario.

Así, cuando se usa por un documento un conjunto de caracteres que la impresora no tiene, usualmente la impresora usará una tabla de la sustitución del conjunto de caracteres. Así el archivo PS copia usará conjuntos de caracteres diferentes que del documento original. Es por esto necesario utilizar un solo tipo de conjunto de caracteres.

Por consiguiente, si se hace documentos para ser archivados en una estructura PS, también se debe tener en cuenta que se pueda transformar a una estructura PDF.

PostScript como lenguaje de programación.

- Los programas PostScript están escritos en caracteres ASCII imprimibles, y por tanto pueden ser editados prácticamente por cualquier editor y procesador de textos.

CAPITULO V

TÉCNICAS DE PROTECCIÓN DE ARCHIVOS Y SOFTWARE

5.1 CONTRASEÑAS

Las contraseñas juegan hoy en día el papel más importante en el problema de la seguridad informática en Internet. Aunque se pueda usar la tecnología y nuevas políticas para hacer las contraseñas más fuertes.

Siempre se advierte de la necesidad de elección de las contraseñas correctas, sin embargo, ocurre que, por muy creativos que se intente ser, el comportamiento puede ser analizado, y por tanto, para algo tan delicado como la forma de proteger un sistema, la educación es inevitable. Más aún, cuando circulan ciertos mitos y creencias incorrectas acerca de algo tan sencillo como la elección de una palabra.

- D+##yU&?23 es una gran contraseña.

En realidad, es muy buena, pero ¿qué ser humano puede recordarla con facilidad? Ciertamente cabe la posibilidad de que acabe escrita en algún lugar, o que incluso algún generador de claves sea capaz de adivinarla.

Existen técnicas mejores para elegir claves, por ejemplo:

a) MeCreo1ClaveO2@PorQueQuiero.yo

Esta clave tiene muchas más letras, lo que se lo pone complicado a una máquina que intente usar la fuerza bruta, mantiene un par de símbolos y otros tantos números, siendo muchísimo más fácil de recordar.

Lo importante, es la estructura de la contraseña, más que la posible complejidad. Combinar una estructura fácil de recordar, la longitud adecuada, con caracteres simbólicos y números puede ser lo más apropiado.

b) PUCESAO99 es una buena contraseña?

Cuando algunas máquinas crackeadoras pueden realizar millones de intentos por segundo, cambiar la letra "O" por el número "0" y añadir números al final, son de las primeras combinaciones con las que arremete contra el sistema. Una mejor inspiración podría ser sustituir la letra "O" por "()" (paréntesis) que resultaría menos predecible. Aún así lo mejor contra los ataques de fuerza bruta son las contraseñas largas.

c) A la larga, cualquier contraseña puede ser violada.

Si la contraseña es suficientemente larga, requeriría tanto poder de proceso y tiempo que es prácticamente igual a ser inviolable. Por supuesto, a medida que mejoran los equipos informáticos, este mito puede que se haga realidad, aunque con la mejora en los métodos de crackeo se produce simultáneamente la mejora en los métodos de encriptado, con lo que la lucha entre ellos suele estar siempre al mismo nivel.

d) Las contraseñas deberían ser cambiadas cada 30 días.

Aunque esto pudiera parecer un buen consejo, habría que pensar en sus desventajas. Obligar a cambios frecuentes de contraseña, deriva inevitablemente en patrones predecibles en los usuarios a la hora de elegir nueva clave, con lo que

se estará restando efectividad a nuestra protección. La mejor opción sería elegir mejores claves y mantenerlas más tiempo (entre 3 y 6 meses).

e) Nunca se deben apuntar las contraseñas.

Esto tiene un 99% de cierto. Resulta una muy mala política el hecho de escribir en cualquier lugar la contraseña, pues existen altas probabilidades de que acabe en la papelera o en manos de personas ajenas a dicha clave. Al tener un software donde se guarde las claves, puede volverse el propio blanco principal de ataques, y además ya sólo sería necesario conocer una sola clave que daría vía libre a todas las demás.

5.1.1 Importancia de las Contraseñas

Cuando se **comparte** un recurso se lo hace **para toda la red**. Es así que una carpeta la puede utilizar todas las computadoras que estén en red. Al poner las contraseñas, sólo podrán utilizar las personas o usuarios a los que se les ha proporcionado dichas contraseñas y nadie más. Adicionalmente existen algunas alternativas para seguridad:

- **Los controles basados en la posesión.**- tiene que ver con objetos que posee el usuario, como una llave física o una tarjeta magnética. A veces hay un clip metálico de una forma peculiar que debe encajar en un agujero de la computadora para que la computadora funcione.

- **Los instrumentos biométricos.-** son los que examinan ciertos rasgos de un usuario potencial y lo comparan con rasgos ya registrados tales como huellas digitales, firma o geometría de la mano.

- **Las contraseñas y los códigos al azar generados por el sistema.**

La programación del sistema puede suministrar una secuencia totalmente al azar de caracteres, al extremo de que letras, dígitos, signos de puntuación y extensión son todos los determinados en el momento o pueden usarse límites en los procedimientos de generación tales como que cada código de acceso se conforme a un formato fijo (como "abc-12345-defg") donde las letras y los números son generados al azar.

- **La Híbrida.-** es en parte suministrada por el usuario, mediante cierto proceso al azar. Esto significa que incluso si un usuario elige la contraseña muy fácil de adivinar como "secreto", la computadora le agregará alguna palabra compleja al final, formando una contraseña más segura como "secreto/5rh11".

- **Las frases de acceso.-** son buenas en el sentido de que son largas y difíciles de adivinar, pero fáciles de recordar. Por lo tanto no es muy aconsejable que los sistemas exijan frases de acceso.

- **Las secuencias de preguntas y respuestas.-** exige que el usuario suministre respuestas a varias preguntas por lo común personales. La computadora tendrá archivada las respuestas a muchas preguntas de este tipo y durante el "ingreso" pedirá la respuesta de dos o tres de ellas.

- Las contraseñas que están predeterminadas por coordenadas generadas por códigos.- los códigos pueden ser empleados por el sistema para permitir a los usuarios verdaderos hacer el "ingreso" por primera vez; se esperará entonces que los usuarios cambien la contraseña que se asignó a una más segura, personal.

- Contraseña suministrada por el usuario.- el pedido está en pantalla, y con una sensación mental de urgencia. El usuario escribe lo primero que se le pasa por la mente, lo primero que ve o escucha. La contraseña es ingresada con apuro y rara vez se la cambia por una contraseña más segura.

- Restricción de Contraseñas.- la mayoría de las contraseñas no son seguras, así que muchos han instalado programas que impiden que se generen contraseñas obvias. Entonces se fuerza a las contraseñas a que se adecuen a ciertas características.

- Las contraseñas más utilizadas.- un estudio realizado por científicos considera que el cerebro humano no es receptivo a las combinaciones contextuales aleatorias. Es decir, la mente humana por naturaleza intenta establecer un orden lógico en los impulsos que recibe.

- Las Imágenes Sustituirán las Contraseñas.- Microsoft desarrolla un nuevo sistema de validación, mediante el cual los usuarios de sistemas informáticos podrán identificarse pulsando en distintos lugares de una imagen en lugar de digitar difíciles contraseñas alfanuméricas.

Asimismo, el nuevo método hará más difícil para los hackers conseguir acceso a los sistemas.

5.2 ENCRIPTACIÓN Y FIRMAS DIGITALES

Se trata de una alta ciencia de la informática, que pasa por arte, inclusive hoy se trata de una tecnología. Encriptación es una palabra rara en español, quizá fea, no obstante se emplea en documentación técnica.

Como elemento clave en las comunicaciones, la importancia de mantener la privacidad de la información, aumenta día a día.

Se comentaba que codificar era muy sencillo, simplemente se cambian unas letras por otras, y el receptor del mensaje conoce este secreto. También, aumentar o disminuir un número discreto a los códigos ASCII, suele ser otra sugerencia. Estas estrategias pasan a ser infantiles tratamientos del problema, y no presentan problema alguno para un decodificador experto y malo.

La encriptación se hace a través de la aplicación de cierto tratamiento a los códigos ASCII de los mensajes, de manera que el tratamiento inverso será el único camino práctico para decodificar el mensaje.

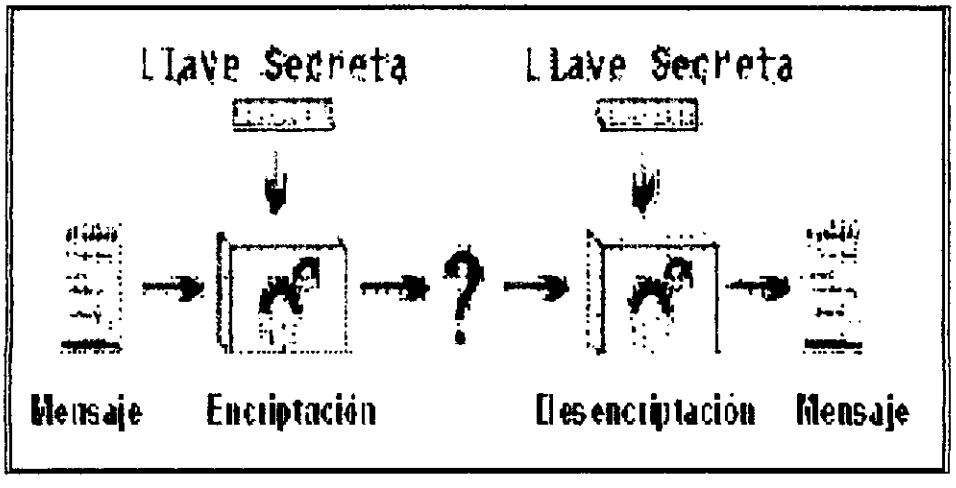
¿Cómo se mantiene indescifrable una cadena codificada? Se trata de combinar la clave de encriptación con el mensaje de manera que las probabilidades de decodificar el mensaje, sin conocer la clave, sean virtualmente muy bajo, es decir, el tan prolongado trabajo de desciframiento de que existan pocas esperanzas.

5.2.1 Encriptación de Comunicaciones.

Las herramientas de encriptación utilizan operaciones matemáticas complejas para conseguir intercambiar información confidencial entre dos personas, que se conectan a través de una red insegura como Internet. En la red, no se tiene conocimiento ni control del camino que siguen los datos para llegar a su destino, por lo que técnicamente es posible interceptar una comunicación, "escuchar" lo que se dice o alterar la información.

5.2.2 Criptografía Simétrica.

Los métodos criptográficos tradicionales operan a partir de una palabra o frase (llave), que sirve para codificar y decodificar información, el conocido password. Esta llave debe ser conocida por los dos extremos de la comunicación, por lo que el punto débil de este método es justamente el proceso de difusión de la llave.

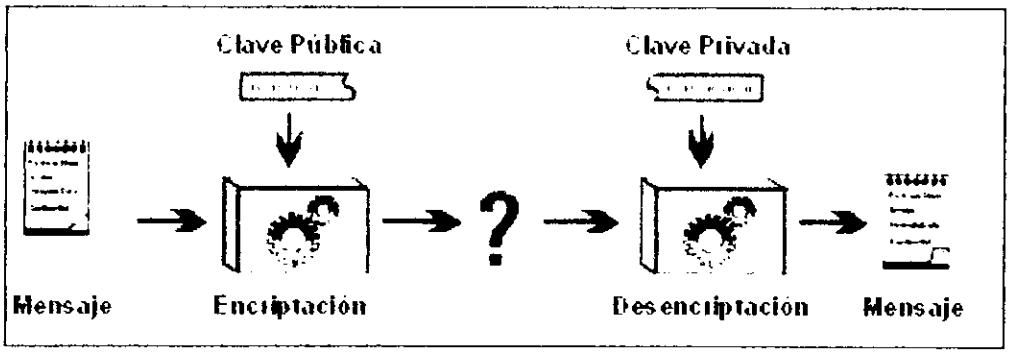


5.2.3 Criptografía Asimétrica.

La Criptografía asimétrica asigna a cada extremo de la comunicación un par de llaves, es una llave pública que cualquiera puede solicitar y conocer, y otra llave privada, cuya seguridad es fundamental para el éxito de la codificación.

Las llaves son una secuencia bastante larga de caracteres y números, generadas por un procedimiento matemático.

Para enviar un mensaje seguro a una persona, se codifica con la clave pública del destinatario. El sistema garantiza que el mensaje resultante sólo puede ser decodificado con la clave privada del destinatario (confidencialidad). Como se tiene la seguridad de la identidad del destinatario gracias a su clave pública, se asegura que el mensaje va al sitio correcto (autentificación).



La encriptación es una herramienta de seguridad que va incrementando su nivel de utilización, a medida que el comercio electrónico continúa su expansión. Se dice que si la comunicación en Internet fuera completamente segura, quizás no sería necesario encriptar los mensajes de correo, pero conforme está estructurada dicha comunicación, hoy por hoy los mensajes pasan por muchos sitios antes de llegar a su destino. Por otro lado, también es interesante poder disponer de una

herramienta que proteja ciertos archivos o documentos que, aunque no vayan a ser enviados a ninguna parte, convenga tenerlos a cubierto de miradas indiscretas.

5.2.4 Encriptación de Documentos y Mensajes de Correo.

Para que la transferencia de un correo electrónico sea segura, tendrá que contemplar estos aspectos:

a) La Autenticidad.- se refiere a los documentos de correos que utilizan el método de firma digital, empleando llaves o claves.

b) La Confidencialidad.- se asegura mediante la encriptación del texto o archivo objeto de la comunicación.

c) La Integridad.- es la no alteración del mensaje desde su salida hasta la llegada. También se basa en el empleo de firmas electrónicas, por lo que si un documento cumple la característica de Autenticidad, ello implica que es íntegro.

d) El No Repudio.- se utiliza la posibilidad de firmar virtualmente los mensajes. El destinatario aplicará entonces la llave pública del remitente, única manera de desencriptar el mensaje y por tanto, la garantía de que éste está expedido por él.

5.2.5 Firmas Digitales.

La seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y particularmente en el comercio electrónico, ésta genera confianza, y hace que los usuarios al depositar sus datos en la red, estén seguros de que no serán alterados ni desviados a usuarios no autorizados.

Los Certificados electrónicos son documentos digitales que sirven para asegurar la veracidad de la Clave Pública perteneciente al propietario del certificado ó de la entidad, con la que se firman digitalmente documentos que puedan proporcionar las más absolutas garantías de seguridad.

¿Qué es una firma electrónica?

Es aquél conjunto de datos, como códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, guardado en un soporte magnético, disquete o disco duro de un computador y no de papel), que permite identificar a su autor.

El procedimiento de firma digital de un mensaje consiste en extraer un "resumen" (o hash en inglés) del mensaje, cifrar el resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envía con la clave pública del destinatario. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente. (Nótese que la firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado).

5.3 CLAVES PÚBLICAS Y PRIVADAS.

La criptografía de claves públicas ofrece grandes ventajas de seguridad cuando se implementa correctamente. Al igual que sucede con otras tecnologías, la criptografía de claves públicas requiere una infraestructura para ofrecer sus

ventajas. Sin embargo, la infraestructura de claves públicas, o PKI, no es un objeto físico ni un proceso de software; se trata de un conjunto de servicios útiles proporcionados por una colección de componentes interconectados. Estos componentes funcionan conjuntamente para proporcionar servicios de seguridad basada en claves públicas a las aplicaciones y a los usuarios.

El propósito de una infraestructura de claves públicas (PKI) es facilitar a las organizaciones el uso de la criptografía de claves públicas. La criptografía de claves públicas resulta esencial para el comercio electrónico, Internet, intranet y otras aplicaciones que requieran seguridad. La criptografía de claves públicas proporciona tres capacidades que son muy valiosas para las organizaciones.

1) Privacidad

- Cifrar mensajes de correo electrónico que se enviarán a través de Internet con el fin de evitar que se lean durante su transmisión.
- Cifrar el tráfico de red cuando un cliente visita el sitio Web para proteger su información de pedido y los números de tarjeta de crédito.

2) Autenticación

- Comprobar la identidad de un visitante en una intranet para permitir que lea determinados archivos.
- Demostrar a un cliente que se encuentra en su sitio Web y no en un sitio malintencionado que enmascare el suyo.

3) Sin rechazo

- Crear un registro obligatorio y que no se pueda modificar de los pedidos de compra de un cliente en el sitio Web de comercio electrónico.
- Firmar contratos electrónicos con vinculación legal.

5.3.1 La Clave Pública.

Se utiliza para **encriptar** datos del dueño de la clave (que van a ser enviados a esta persona) y para verificar algo firmado digitalmente.

- **Administrar claves**: una PKI hace que sea fácil emitir claves nuevas, revisar o revocar claves existentes y administrar el nivel de confianza adjuntado a las claves de emisores distintos.

- **Publicar claves**: una PKI ofrece una forma bien definida para que los clientes busquen y recuperen claves públicas y la información acerca de si una clave específica es válida o no. Sin la posibilidad de recuperar claves y averiguar si son válidas, los usuarios no pueden utilizar los servicios de claves públicas.

- **Usar claves**: una PKI proporciona una forma sencilla para que los usuarios utilicen las claves, no sólo moviéndolas donde se necesiten, sino también proporcionando aplicaciones fáciles de usar que realicen las operaciones criptográficas de claves públicas, lo que permite proporcionar seguridad al correo electrónico, el comercio electrónico y las redes.

- **Aplicaciones compatibles con claves públicas**

No es necesario que el usuario sepa cómo funciona la criptografía, dónde se almacenan los certificados o ningún otro detalle; sólo debe indicar qué desea hacer y dejar que las aplicaciones y la PKI se ocupen del resto.

5.3.2 La Clave Privada.

Se utiliza para desencriptar datos utilizando la clave pública de quien encriptó estos datos originalmente y para crear firmas digitales.

Solamente hay que tener la posibilidad de desencriptar datos dirigidos a la persona únicamente, y debe ser la única persona que pueda firmar algo que los demás vean como privado.

5.4 CANDADOS PARA LA PROTECCIÓN DE SOFTWARE.

Protecciones Físicas - Candados Electrónicos.

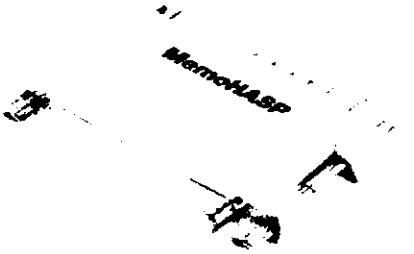
- El candado electrónico es un conector de tamaño menor a una cajetilla de cigarros que se coloca en el puerto paralelo o serie y que contiene una clave que protege a los programas de alguna ejecución no autorizada.

- El dispositivo, en combinación con software, protege a los programas contra copias ilegales y permite al usuario legal una mayor comodidad en la ejecución de su programa, sin afectar el funcionamiento del puerto de impresora donde se conectó.

- Con este esquema de seguridad, el desarrollador tiene la certeza del 100% que tendrá una venta por cada computadora en la que se ejecute su programa, ya que el dispositivo necesita estar conectado en todo momento en el que el sistema esté funcionando y no sólo al arranque del mismo.

Candados programables con memoria:

MemoHASP combina la tecnología ASIC con hasta 496 bytes de memoria de lectura y escritura. Un solo candado puede controlar el acceso a múltiples aplicaciones o módulos. MemoHASP abre nuevas oportunidades: rentar software, distribuir demos con activaciones limitadas, actualizar software remotamente y mucho más. Para una flexibilidad extra, cada candado MemoHASP contiene un número ID único.



NetHASP

- Es lo último en Administración Segura de Licencias para ambientes de red. Se requiere un solo candado NetHASP para activar un programa protegido desde cualquier estación de la red. Instalado en el Servidor o en cualquier estación de la red, NetHASP administra el uso concurrente de su aplicación en un ambiente de red.

Con 496 bytes de memoria le permite proteger múltiples aplicaciones, limitando en número de licencias y/o activaciones para cada programa.



Aladdin Card

– Solución alterna para conectar candados de protección de software en su PC. Aladdin CARD es una tarjeta paralela que puede instalarse en un slot de expansión estándar de su PC, permitiéndole instalar los candados dentro de la misma. Ideal para grandes organizaciones, Aladdin CARD protege al candado y también funciona como un puerto de impresión estándar.



5.5 FORMATOS DE ARCHIVOS PDF.

El formato de archivo PDF es una variante del lenguaje de descripción impreso Postscript de Adobe, el formato dominante en las publicaciones impresas de la actualidad.

El PDF permite que los documentos electrónicos sean visualizados e impresos con resultados consistentes en distintos tipos de computadoras y sistemas operativos, utilizando el software.

Los documentos PDF preservan el aspecto y el contenido exactos de los originales, junto con sus fuentes e imágenes. Diversas herramientas y funciones le permiten agregar elementos interactivos a un documento, desde hipervínculos personalizados y clips multimedia, hasta campos y botones. También se puede crear una biblioteca electrónica de archivos y poder ver la información que se requiera; incluso se puede colocar "candados" de seguridad en archivos confidenciales.

¿Cómo funcionan los archivos PDF?

El Acrobat Reader sólo sirve para visualizar, recorrer e imprimir documentos (pero no para modificarlos ni crearlos); en cambio el Acrobat no sólo sirve para visualizar, recorrer e imprimir documentos sino también para crear y modificar los archivos PDF.

El PDF de Acrobat es, entre todos los formatos de archivo, uno de los más importantes y versátiles.

El formato continúa extendiéndose por diferentes contextos. Otros usos habituales incluyen su utilización como medio para publicaciones basadas en la Web, libros electrónicos descargables, presentaciones en pantalla, formato obligado para el intercambio de documentos.

Fundamentalmente, lo que hace que el PDF sea tan poderoso es el hecho de que está construido sobre PostScript, que es un PDL (Page Description Language o Lenguaje de Descripción de Páginas), un lenguaje de programación optimizado para describir correctamente la presentación y la apariencia visual de una página, incluyendo todos los vectores, mapas de bits y muy importante las fuentes.

El principal inconveniente del sistema de colaboración basado en comentarios de Acrobat es que para realizar cualquier cambio se tiene que volver a la aplicación original con la impresión en PDF. En el más simple de los niveles, se puede establecer una contraseña para abrir un PDF y, al mismo tiempo, controlar las posibilidades del usuario final para editarlo, copiarlo e imprimirlo una vez abierto.

CAPITULO VI

ANÁLISIS

6.1 CARACTERÍSTICAS DE LA APLICACIÓN

En la aplicación desarrollada se trabajó con la Criptografía, dicha aplicación será utilizada en la Biblioteca Virtual de la PUCESA, se puede decir además que a pesar de que existen distintos tipos de aplicaciones como cifrados, estos son generalizados y no específicamente desarrollados para la PUCESA.

Por esta razón se trabajó en una aplicación propia para atender parte de las necesidades criptográficas de la Biblioteca Virtual de la PUCESA.

6.1.1 Propuesta de la Aplicación

Consiste en que los archivos que se utilizan dentro de la Biblioteca Virtual de la PUCESA estén protegidos de personas que desean destruir o alterar cierta información existente en los archivos que son importantes para el autor o persona que utiliza dicho archivo.

En la aplicación se utilizará algoritmos y funciones matemáticas que servirán para transformar la información en un conjunto ilegible, en donde solo la persona autorizada podrá saber su contenido verdadero del archivo original que anteriormente fue transformado.

Todos los algoritmos pueden usarse aplicando diversos modos de cifrado, entre ellos:

ECB: Electronic CodeBook (libro electrónico de códigos).- Cifra cada bloque con la clave k de forma independiente. Por lo tanto, el resultado es como si se codificara mediante un gran libro electrónico de códigos.

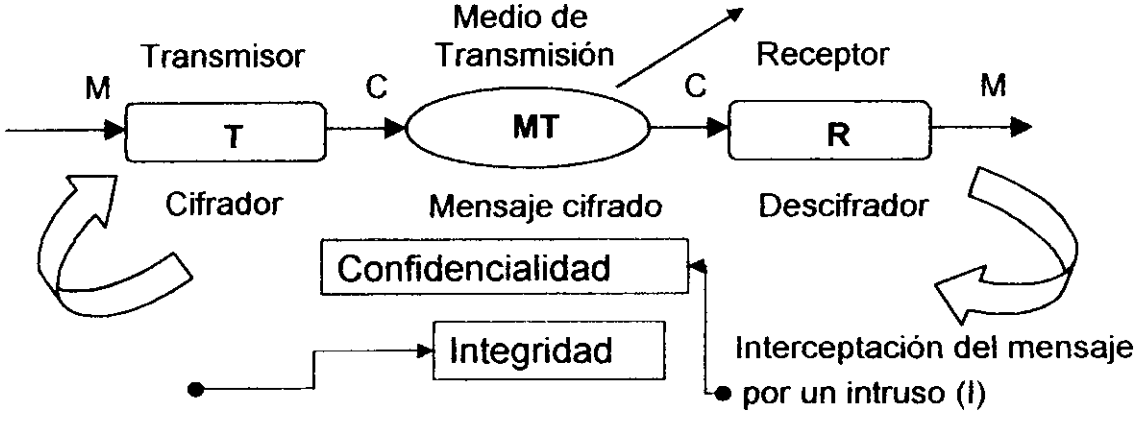
CBC: Cipher Block Chaining (encadenamiento de bloques).- Se encadenan los bloques de texto en claro con el bloque del criptograma anterior. Usa un vector de inicialización IV de 64 bits que se guarda en secreto.

CFB: Cipher FeedBack (realimentación de bloques).- Se pueden cifrar unidades de datos más pequeñas que bloques, por lo general un byte. Se usa un registro de desplazamiento de 64 bits como vector inicial IV.

OFB: Output FeedBack (realimentación bloque de salida).- La realimentación de la señal se realiza antes de la operación XOR.

6.1.2 Confidencialidad e Integridad.

Criptosistema



6.1.3 Clasificación de los Criptosistemas.

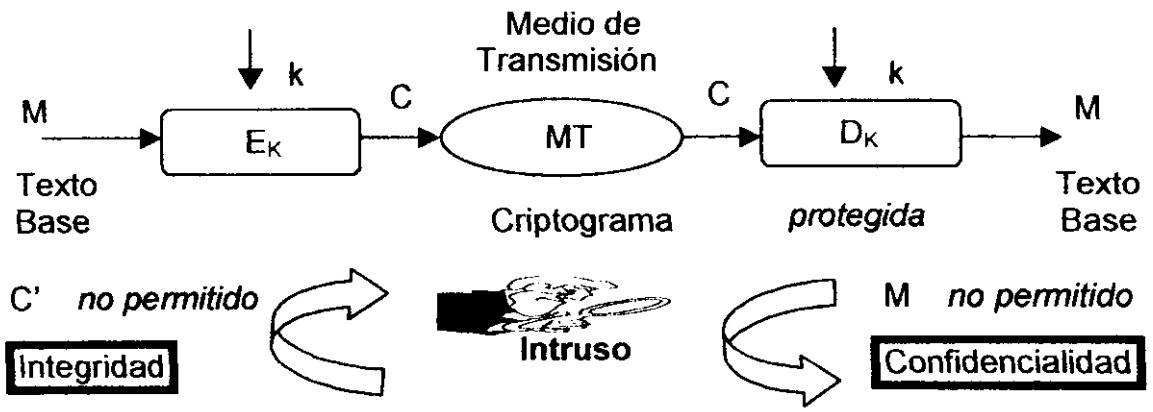
Según el tratamiento del mensaje se dividen en:

- Cifrado en bloque (DES, IDEA, CAST, RIJNDAEL: 64 - 128 bits)
- Cifrado en flujo (A5) cifrado bit a bit

Según el tipo de claves se dividen en:

- Cifrado con clave secreta (Sistemas Simétricos).
- Cifrado con clave pública (Sistemas Asimétricos).

6.1.4 Cifrado con criptosistemas simétricos de clave secreta



Dicha aplicación es una seguridad lógica la misma que protege su información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía y políticas de seguridad.

Existen varios algoritmos de cifrado de los cuales se tiene como ejemplo:

6.1.5 Cifrado Tipo Feistel.

Horst Feistel: inventor (IBM) del algoritmo LUCIFER a comienzos de los años 70. El algoritmo fue utilizado por el Reino Unido. En 1974 se propone a la NSA (Agencia Nacional de Seguridad) como estándar y en ese año dará origen al DES (Estandar de Encriptación de Datos).

- Dado un bloque de N bits (típico 64) éste se dividirá en dos mitades.
- Existirá una función unidireccional F (muy difícil de invertir).
- Se realizan operaciones con la clave ki sólo con una mitad del bloque, y se permutan en cada vuelta las dos mitades, operación que se repite durante n vueltas.

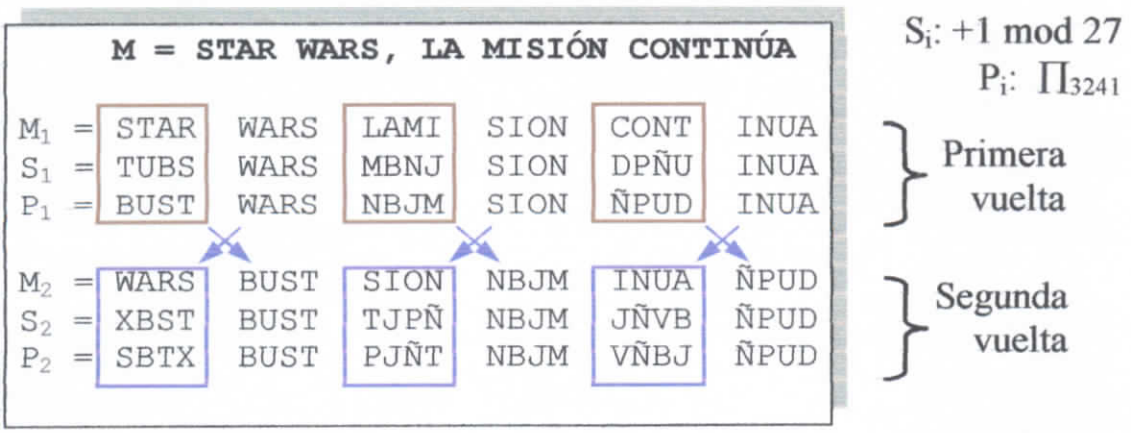
Ejemplo básico de cifra tipo Feistel

El algoritmo usará bloques de tamaño 8 caracteres. Tendrá dos vueltas y en cada vuelta realizará una operación de sustitución **S** y una permutación **P** sobre la primera mitad.

Sustitución S: Desplazamiento +1 mod 27

Permutación P: $\prod 3241$

Mensaje: M = STAR WARS, LA MISIÓN CONTINÚA



C = SBTX BUST PJÑT NBJM VÑBJ ÑPUD

6.1.6 ALGORITMOS DE CIFRADO MÁS CONOCIDOS

Algoritmo	Bloque (bits)	Clave (bits)	Vueltas
Blowfish	64	variable	16
DES	64	56	16
CAST	64	64	8
Gost	64	256	32
RIJNDAEL	128	128 o más	flexible
Skipjack	64	80	32
IDEA	64	128	8
Twofish	128	variable	variable

Dentro de la aplicación se implementaron algunos algoritmos que son:

Todos los valores en valor absoluto y binario de 8, 32, 64 ó 128 bits respectivamente dependiendo del tamaño del bloque.

6.1.6.1 Algoritmo de la Serpiente (Blowfish).

- Cifrador tipo Feistel de clave variable (Bruce Schneier).
- Cifra bloques de texto de 64 bits.
- Tamaño de clave: de 32 hasta 448 bits. Se generan 18 subclaves de 32 bits
- Número de vueltas: 16, en cada una de ellas se realiza una permutación función de la clave y una sustitución que es función de la clave y los datos.
- Operaciones básicas: or exclusivo y suma módulo 2^{32}.
- Características: compacto porque necesita sólo 5 K de memoria, es muy rápido (5 veces más veloz que DES), es conceptualmente simple y su

fortaleza puede variarse según longitud de la clave. Usa una función F y operaciones básicas de suma y or exclusivo que provocan un efecto de avalancha.

Ejemplo:

Muchos de los cifrados de producto tienen en común que dividen un bloque de longitud n en dos mitades, L y R. Se define entonces un cifrado de producto iterativo en el que la salida de cada ronda se usa como entrada para la siguiente según la relación (ver figura):

$$\left.\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} + f(R_{i-1}, K_i) \end{aligned}\right\} \text{ Si } i < n$$

$$L_n = L_{n-1} + f(R_{n-1}, K_n)$$

$$R_n = R_{n-1}$$

Este tipo de estructura se denomina Red de Feistel, y es empleada en multitud de algoritmos, como **DES, Lucifer, FEAL, CAST, Blowfish, etcétera**. Tiene la interesante propiedad de que para invertir la función de cifrado es decir, para descifrar basta con aplicar el mismo algoritmo, pero con las K_i en orden inverso. Además, que esto ocurre independientemente de cómo sea la función f.

Se puede emplear la inducción matemática para comprobar esta propiedad. Sea $E_n(L, R)$ la función de cifrado para una red de Feistel de n rondas y $D_n(L, R)$ la función de descifrado análoga. Dividir cada función en sus bloques izquierdo y derecho y se observará con superíndices:

$E^{I}{}_{n}(L,R)$, $E^{R}{}_{n}(L,R)$, $D^{I}{}_{n}(L,R)$ y $D^{R}{}_{n}(L,R)$ Se ha de demostrar que:

$D^{I}{}_{n}(E^{I}{}_{n}(L,R), E^{R}{}_{n}(L,R)) = L$ y $D^{R}{}_{n}(E^{I}{}_{n}(L,R), E^{R}{}_{n}(L,R)) = R$ para cualquier valor de n.

6.1.6.2 Algoritmo Estandar de Encriptación de Datos (DES).

A mediados de 1998, se demostró que un ataque por la fuerza bruta a DES era viable, debido a la escasa longitud que emplea en su clave. No obstante, el algoritmo aún no ha demostrado ninguna debilidad grave desde el punto de vista teórico, por lo que su estudio sigue siendo plenamente interesante.

Ejemplo:

El algoritmo DES codifica bloques de 64 bits empleando claves de 56 bits. Es una Red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio (P_i) y otra que se aplica al final (P_f), tales que $P_i = P^{-1}{}_f$.

La función f se compone de una permutación de expansión (E), que convierte el bloque de 32 bits correspondiente en uno de 48. Después realiza un or-exclusivo con el valor K_i, también de 48 bits, aplica ocho S-Cajas de 6*4 bits, y efectúa una nueva permutación P.

Se calcula un total de 16 valores de K_i , uno para cada vuelta, efectuando primero una permutación inicial **EP1** sobre la clave de 64 bits, llevando a cabo desplazamientos a la izquierda de cada una de las dos mitades de 28 bits resultantes, y realizando finalmente una elección permutada (**EP2**) de 48 bits en cada ronda, que será la K_i. Los desplazamientos a la izquierda son de dos bits, salvo para las vueltas 1, 2, 9 y 16, en las que se desplaza sólo un bit. Nótese que aunque la clave para el algoritmo DES tiene en principio 64 bits, se ignoran

ocho de ellos un bit de paridad por cada byte de la clave, por lo que en la práctica se usan sólo 56 bits.

Para descifrar basta con usar el mismo algoritmo (ya que $P_i = P^{-1}{}_f$).

6.1.6.3 Algoritmo GOST.

El algoritmo Gost, consiste en ordenar todos los puntos alrededor de un vértice en cuestión, p, de forma circular, es decir, según el argumento de la coordenada polar de cada vértice respecto de p y, en caso de empate, según su distancia a este. Tras hacer esto, realizar un barrido rotatorio parando en cada vértice, determinando la visibilidad del mismo. Así, se puede construir un árbol de búsqueda equilibrado para realizar la consulta de visibilidad, y determinar la visibilidad en un tiempo logarítmico.

El algoritmo de la línea de barrido rotatoria (Rotational Sweep Line) queda de la siguiente forma:

Entrada: Un conjunto de obstáculos poligonales S y un conjunto de puntos Q.

Salida: Un grafo de visibilidad G = (V, E).

Sea W la unión de los vértices de S y los puntos de Q, sea E el conjunto de aristas, y sea T un árbol de búsqueda equilibrado.

1.- Para cada vértice w de V:

2.- Ordenar todos los vértices de W en sentido horario según la semi-línea P, y, en caso de empate, ordenar según distancia al punto p.

3.- Ordenar las aristas que intersectan con P e insertarlas en el árbol equilibrado T.

4.- Para cada vértice w de la lista ordenada W:

5.- Si w es visible desde p, entonces añadir la arista e=(p, w) al grafo G.

6.- Insertar en el árbol los obstáculos que incidan en w y que estén en el lado horario de P.

7.- Eliminar del árbol los obstáculos que incidan en w y que estén en el lado antihorario de P.

El paso 2 se puede realizar en tiempo O(n log n) en el número de vértices con una ordenación por comparaciones, por lo que el coste mínimo del algoritmo es $O(n^2 \log n)$. El paso 3 puede ejecutarse en tiempo O(n), por lo que el coste total no se ve incrementado.

Los pasos 5, 6 y 7 se repiten n^2 veces, por lo que su coste debe ser, a lo sumo, O(log n), para no incrementar el orden total del algoritmo. Efectivamente, al usar un árbol equilibrado, las búsquedas, inserciones y borrados son de orden O(log n), por lo que el orden resultante es $O(n^2 \log n)$, como se esperaba.

El algoritmo en definitiva, es una variante del algoritmo por fuerza bruta, solo que, en el bucle más interno, en el que se determinan las aristas de visibilidad, se usa un árbol de búsqueda binario, que permite hacer búsquedas en tiempo O(log n) para determinar si dos aristas intersectan o no. Y, dado que las aristas que no pueden intersectar con la línea de barrido son eliminadas del árbol al procesar el vértice en el que inciden, resulta que la complejidad del algoritmo queda reducida a $O(n^2 \log n)$. Nótese que es necesario el uso de un árbol equilibrado, pues de otro modo el árbol podría degenerar y se obtendrá búsquedas de orden lineal.

Ejemplo:

Sean a y b dos números enteros positivos, ambos menores o iguales que n. Entonces se necesita aproximadamente log 2 (n) bits para representarlos hay que tomar encuenta que, en este caso, log 2 (n) es el tamaño de la entrada. Según este

criterio, las operaciones aritméticas, llevadas a cabo mediante los algoritmos tradicionales, presentan los siguientes órdenes de complejidad:

Suma (a + b): $O(\log 2 (a) + \log 2 (b)) = O(\log 2 (n))$

Resta (a - b): $O(\log 2 (a) + \log 2 (b)) = O(\log 2 (n))$

Multiplicación (a · b): $O(\log 2 (a) \cdot \log 2 (b)) = O((\log 2 (n))2)$

División (a/b): $O(\log 2 (a) \cdot \log 2 (b)) = O((\log 2 (n))2)$

6.1.6.4 Algoritmo CAST.

- Cifrador Feistel propuesto por C. Adams y S. Tavares (Canadá).
- Cifra bloques de texto de 64 bits con claves de 40 hasta 128 bits en incrementos de octetos.
- Cifra en 16 vueltas.
- Usa ocho cajas S de 8 bits de entrada y 32 bits de salida con unas funciones no lineales óptimas (funciones bent), cuatro cajas en procesos de cifra y las otras cuatro para la generación de claves. Cada caja es un array de 32 columnas y 256 filas. Los 8 bits de entrada seleccionan una fila y los 32 bits de ésta es la salida.
- Operaciones básicas: suma y resta módulo 2^{32}, or exclusivo y rotaciones circulares hacia la izquierda.
- Características: inmune a ataques por criptoanálisis diferencial y lineal; algoritmo estándar de cifra en últimas versiones de PGP.

6.1.6.5 Algoritmo de Encriptación Avanzada (RIJNDAEL).

Características.

- No es de tipo Feistel.
- Implementado para trabajar en los procesadores de 8 bits usados en tarjetas inteligentes y en PCs de 32 bits.
- Tamaño de clave variable: 128, 192 y 256 bits (estándar) o bien múltiplo de 4 bytes.
- Tamaño del bloque de texto: 128 bits o múltiplo de 4 bytes.
- Operaciones modulares a nivel de byte (representación en forma de polinomios) y de palabra de 4 bytes: 32 bits.
- Número de etapas flexible según necesidades del usuario.

a.- Transformaciones o capas de RIJNDAEL

- Hay tres transformaciones distintas llamadas capas en las que se tratan los bits. Estas constan de:
  - Capa de Mezcla Lineal: en ella se busca la difusión de los bits.
  - Capa No Lineal: se trata de una zona similar a las cajas S del DES.
  - Capa Clave: operaciones con una función Xor de la subclave y la información de esta etapa intermedia.
- Las transformaciones realizadas en cada paso del algoritmo se denominan estados y se representa por un array de 4 filas.

b.- Operaciones con bytes en RIJNDAEL

- Operaciones a nivel de byte en $GF(2^8)$

- **Suma y multiplicación.-** Son cálculos en Campos de Galois $GF(2^8)$ con 8 bits. Para la reducción de exponente se usará un polinomio primitivo p(x).

- **Producto por x.-** Esta operación conocida como xtime(a) al igual que en el caso anterior usa la reducción de exponente. Puede implementarse fácilmente con desplazamientos y operaciones or exclusivo.

Ejemplo de suma en $GF(2^8)$

Vamos a sumar los valores hexadecimales 57 y 83:

$A = 57_{16} = 0101\ 0111_2$ $B = 83_{16} = 1000\ 0011_2$

que expresados en polinomios dentro de $GF(2^8)$ serán:

$A = 0101\ 0111_2 = x^6 + x^4 + x^2 + x + 1$

$B = 1000\ 0011_2 = x^7 + x + 1$

Sumando: $A+B = (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) \bmod 2$

$A+B = (x^7 + x^6 + x^4 + x^2 + 2x + 2) \bmod 2$

$A+B = x^7 + x^6 + x^4 + x^2 = 1101\ 0100 = D4_{16}$

Y lo mismo se obtiene con la suma Or exclusivo:

$0101\ 0111 \oplus 1000\ 0011 = 1101\ 0100 = D4_{16}$

6.1.6.6 Algoritmo SKIPJACK.

- Cifra bloques de 64 bits con una clave de 80 bits.
- Los usuarios depositan sus claves secretas en diversas agencias de gobierno.
- Usa 32 vueltas en cada bloque de cifra.

- Características: imposición de los EEUU para comunicaciones con la administración, tiene una puerta trasera que puede dejar en claro la cifra, nadie puede asegurar que el algoritmo tenga la suficiente fortaleza.

6.1.6.7 Algoritmo IDEA.

Algoritmo seguro y muy usado en correo electrónico.

- Cifra bloques de 64 bits en 8 vueltas
- Divide la entrada M en cuatro bloques de 16 bits
- Se generan 52 subclaves de 16 bits a partir de la clave maestra de 128 bits
- Usa 6 claves por vuelta
- Hay una transformación final con 4 claves para invertir operación inicial

Operaciones básicas:

- XOR

- Suma módulo 2^{16} (mod 65.536)

- Multiplicación módulo $2^{16}+1$ (65.537)

Todas las operaciones se realizan con bloques de 16 bits y el truco está en que los bloques cuyo valor sea 0 (16 bits) se cambiarán por la constante 2^{16} ...¡ de 17 bits!

Ejemplo:

Como ocurre con todos los algoritmos simétricos de cifrado por bloques, IDEA se basa en los conceptos de confusión y difusión, haciendo uso de las siguientes operaciones elementales (todas ellas fáciles de implementar):

- XOR.

- Suma módulo 2^{16}.

- Producto módulo $2^{16} + 1$.

El algoritmo IDEA consta de ocho rondas. Dividiremos el bloque X a codificar, de 64 bits, en cuatro partes X_1, X_2, X_3 y X_4 de 16 bits. Para la interpretación entera de dichos registros se empleará el criterio big endian, lo cual significa que el primer byte es el más significativo.

Se denominará Z_i a cada una de las 52 subclaves de 16 bits que se va a necesitar. Las operaciones que se llevará a cabo en cada vuelta son las siguientes:

1. Multiplicar X_1 por Z_1.
2. Sumar X_2 con Z_2.
3. Sumar X_3 con Z_3.
4. Multiplicar X_4 por Z_4.
5. Hacer un XOR entre los resultados del paso 1 y el paso 3.
6. Hacer un XOR entre los resultados del paso 2 y el paso 4.
7. Multiplicar el resultado del paso 5 por Z_5.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar el resultado del paso 8 por Z_6.
10. Sumar los resultados de los pasos 7 y 9.
11. Hacer un XOR entre los resultados de los pasos 1 y 9.
12. Hacer un XOR entre los resultados de los pasos 3 y 9.
13. Hacer un XOR entre los resultados de los pasos 2 y 10.
14. Hacer un XOR entre los resultados de los pasos 4 y 10.

La salida de cada iteración serán los cuatro sub-bloques obtenidos en los pasos 11, 12, 13 y 14, que serán la entrada del siguiente ciclo, en el que se empleará las siguientes seis subclaves, hasta un total de 48.

Al final de todo se intercambiará los dos bloques centrales (en realidad con eso se deshace el intercambio que se lleva a cabo en los pasos 12 y 13).

Después de la octava iteración, se realiza la siguiente transformación:

1. Multiplicar X_1 por Z_{49}.

2. Sumar X_2 con Z_{50}.

3. Sumar X_3 con Z_{51}.

4. Multiplicar X_4 por Z_{52}.

Las primeras ocho subclaves se calculan dividiendo la clave de entrada en bloques de 16 bits. Las siguientes ocho se calculan rotando la clave de entrada 25 bits a la izquierda y volviendo a dividirla, y así sucesivamente.

Las subclaves necesarias para descifrar se obtienen cambiando de orden las Z_i y calculando sus inversas para la suma o la multiplicación.

Puesto que $2^{16} + 1$ es un número primo, nunca se podrá obtener cero como producto de dos números, por lo que no se necesita representar dicho valor. Cuando se esté calculando productos, se utilizará el cero para expresar el número 2^{16} (un uno seguido de 16 ceros). Esta representación es coherente puesto que los registros que se emplean internamente en el algoritmo poseen únicamente 16 bits.

6.1.6.8 Algoritmo TWOFISH.

Twofish usa 40 subllaves de 32 bits, los primeros 8 bits son usados para encerar, es decir cuatro al comienzo y cuatro al final son XOR con el bloque entero.

Con cada uso de la ruta, dos de las subllaves de 32 restantes, y así es que twofish tienen 16 rutas.

Se notará que la parte como Q3 va directo a Q0.

El Programa de la Llave.- La generación significante empieza derivando tres vectores cruciales cada uno la mitad de largo de la llave original. La primera parte dos son forjadas dividiendo las llaves en partes de 32 bits. Numerando estas partes a partir del cero, los aún numerados se convierten en M(e), y los números se convierten en M(o).

Lo tercero se forma dividiendo la llave en partes de 64 bits, y produciendo un papel de 32 bits de la clave vectorial multiplicando cada parte de 64 bits por esta matriz (llamado la matriz RS).

Ejemplo:

01 A4 55 87 5A 58 DB 9E
A4 56 82 F3 1E C6 68 E5
02 A1 FC C1 47 AE 3D 19
A4 55 87 5A 58 DB 9E 03

Sobre el Galois Field GF (2^8) con el modulo polinomial x^8 + x^6 + x^3 + x^2 + 1, que significa eso después de una multiplicación XOR la configuración de bits 101001101 se usa para acomodar el resultado de vuelta a ocho bits esta vez.

Los cambios polinómicos modulares que el número hace, pero no cambia la estructura matemática subyacente del campo. Las palabras de 32 bits resultantes son entonces colocadas en el orden inverso en el vector de las llaves llamada S.

El arreglo de S-cajas con 8 bits de entrada y salida, llamó a q(0) y q(1), es cada uno construido de 4 S-cajas con 4 bit de entradas y salidas. Para q(0), las S-cajas es **por ejemplo:**

Input	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
T0	8	1	7	13	6	15	3	2	0	11	5	9	14	12	10	4
T1	14	12	11	8	1	2	3	5	15	4	10	6	7	0	9	13
T2	11	10	5	14	6	13	9	0	12	8	15	3	2	4	7	1
T3	13	7	15	4	1	2	6	14	9	11	3	0	8	5	12	10

Y, para q(1), las S-cajas, otra vez dado las mismas designaciones, es:

Input	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
T0	2	8	11	13	15	7	6	14	3	1	9	4	0	10	12	5
T1	1	14	2	11	4	12	3	7	6	13	10	5	15	9	0	8
T2	4	12	7	5	1	6	9	10	0	14	13	8	2	11	3	15
T3	11	9	5	1	12	3	13	14	6	4	7	15	2	0	8	10

Cada S-cajas se forma como se indica a continuación:

Ejemplo:

- El byte de entrada está dividido en sus mitades más significantes y menos significantes, A y B.
- El valor nuevo de A es el XOR de los viejos valores de A y B.
- El valor nuevo de B es el XOR del viejo valor de A, B alternó correcta el bit, y 8 si el viejo valor de A fue extraño.
- A y B son entonces reemplazadas por sus substitutos en la S-cajas de 16 bits T0 y T1 respectivamente.
- El valor nuevo de A es el XOR de los viejos valores de A y B.
- El valor nuevo de B es el XOR del viejo valor de A, B alternó correcta el bit, y 8 si el viejo valor de A fue extraño.
- A y B son entonces reemplazadas por sus substitutos en la S-cajas de 16 bits T2 y T3 respectivamente.
- A y B están entonces combinadas en orden inverso para formar el byte de resultado.

Las 4 claves dependientes de S-cajas son formadas de los elementos de 32 bit de la clave del vector S como se indica a continuación:

Si la clave es de 256 bits de largo, la clave del vector S tiene 4 elementos de 32 bits, S(0), S(1), S(2), y S(3).

En este caso, las 4 claves dependientes de S-cajas son equivalentes para realizar las operaciones:

output = q(0)(S(0,0) xor q(1)(S(1,0) xor q(1)(S(2,0) xor q(0)(S(3,0) xor q(1)(input))))
output = q(1)(S(0,1) xor q(1)(S(1,1) xor q(0)(S(2,1) xor q(0)(S(3,1) xor q(0)(input))))
output = q(0)(S(0,2) xor q(0)(S(1,2) xor q(1)(S(2,2) xor q(1)(S(3,2) xor q(0)(input))))
output = q(1)(S(0,3) xor q(0)(S(1,3) xor q(0)(S(2,3) xor q(1)(S(3,3) xor q(1)(input))))

Donde S(2,1) significa byte 1 de palabra 2 en la clave del vector S.

Cuando la clave es de 192 bits de largo, las definiciones de S-cajas son simplificadas:

output = q(0)(S(0,0) xor q(1)(S(1,0) xor q(1)(S(2,0) xor q(0)(input)))
output = q(1)(S(0,1) xor q(1)(S(1,1) xor q(0)(S(2,1) xor q(0)(input)))
output = q(0)(S(0,2) xor q(0)(S(1,2) xor q(1)(S(2,2) xor q(1)(input)))
output = q(1)(S(0,3) xor q(0)(S(1,3) xor q(0)(S(2,3) xor q(1)(input)))

Y, cuando la clave es solo de 128 bits de largo, las definiciones de S-cajas son simplificadas a:

output = q(0)(S(0,0) xor q(1)(S(1,0) xor q(1)(input))
output = q(1)(S(0,1) xor q(1)(S(1,1) xor q(0)(input))
output = q(0)(S(0,2) xor q(0)(S(1,2) xor q(1)(input))
output = q(1)(S(0,3) xor q(0)(S(1,3) xor q(0)(input))

6.1.7.- RECURSOS

6.1.7.1 RECURSO HUMANO

Personal	Número	Número de horas	Valor c/hora	Subtotal
Investigador	1	300	2,50	750,00
Asesor	1	100	1,00	100,00
Asesor Externo	1	80	4,00	320,00

COSTO **1,170,00**

6.1.7.2 RECURSOS MATERIALES

Materiales	Número	Valor c/hora	Valor c/u	Número de horas	Subtotal
Computadora	1	1,00		300	300,00
Copiadora	700		0,03		21,00
Hojas de papel bond A4	1500		0,008		12,00
Libros didácticos	4		5,00		20,00
Cartucho de tinta negra	2		30,00		60,00
Cartucho de tinta color	1		32,00		32,00
Cd's	6		1,00		6,00
Internet	1	1,20		60	72,00

COSTO 523,00

6.1.7.3 RECURSOS ECONOMICOS

	Subtotal
Recursos Humanos	1,170,00
Recursos Materiales	523,00

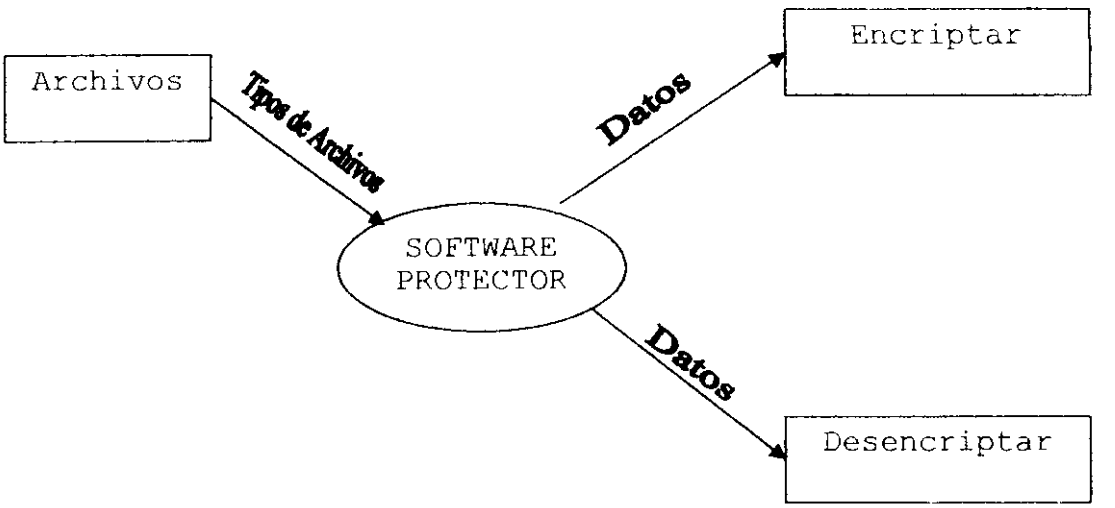
Costos Directos	1,693,00
Imprevistos 5%	84,65
Transporte 5%	84,65

COSTO TOTAL 1,862,30

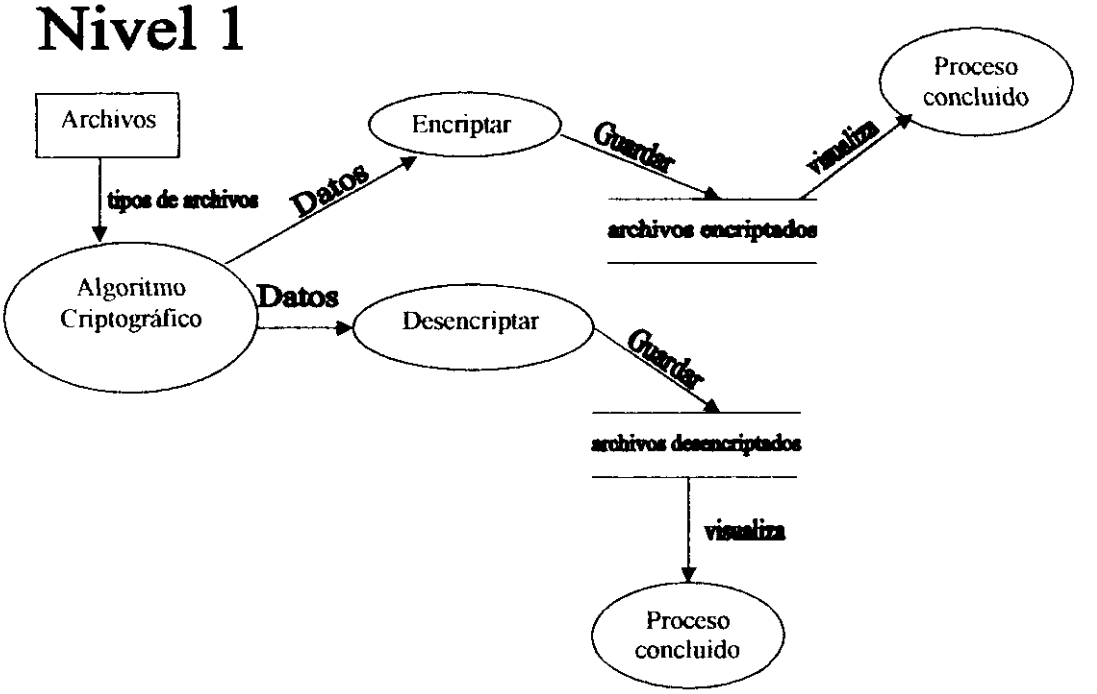
6.2 ESTRUCTURA DE LA APLICACIÓN

6.2.1 Diagrama de Flujo de Datos

Nivel 0



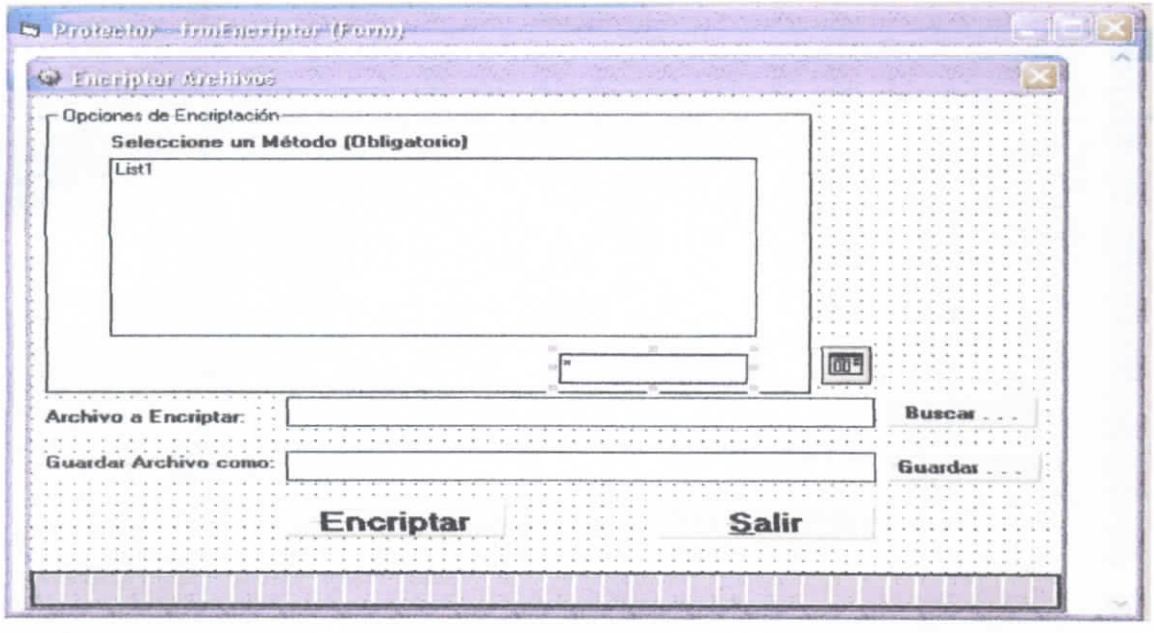
Nivel 1



6.2.2 DESCRIPCIÓN GENERAL DEL SISTEMA

El software realizado es la utilización de Métodos Criptográficos, que permiten tener una seguridad en los archivos con el objeto de que no sean alterados o modificados dichos archivos.

En el sistema se utilizan formularios tanto para encriptar como para desencriptar los archivos, realizados en un lenguaje de programación como es Visual Basic versión 6.0.



Como se observa en la imagen se utiliza algunos controles existentes en el cuadro de herramientas de Visual Basic.

Tanto el formulario de encriptar archivos como el formulario de desencriptar archivos, utilizan una interfaz estándar.

Es por esto que se utiliza en el formulario una herramienta para listar los distintos métodos que puede utilizar tanto para encriptar como para desencriptar el archivo.

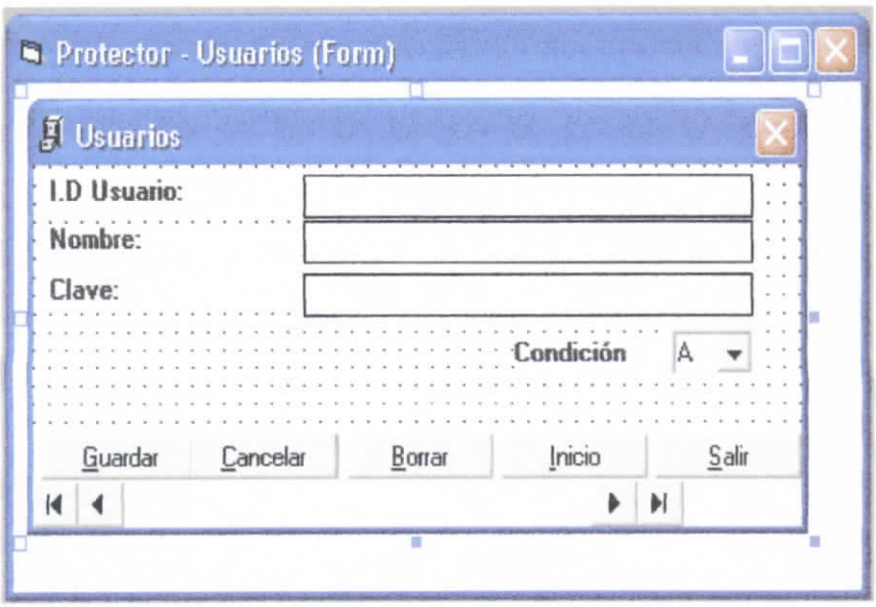
También se utiliza una contraseña interna y fija debido a que en algunos métodos es necesario ingresar la contraseña.

Se tiene un botón de Buscar para ejecutar la acción de ir a Buscar el archivo a Encriptar en el caso de que se encuentre en el formulario de encriptar archivos, caso contrario se realiza la desencriptación si está en el formulario de desencriptar archivos.

Otro botón utilizado es el Guardar con el propósito de que guarde el usuario con el nombre que más prefiere y en el lugar más apropiado, esta acción se realiza tanto para el formulario de encriptar archivos como para el formulario de desencriptar archivos.

El botón de comando Encriptar realiza el proceso deseado que es proteger nuestro archivo.

Una forma de ver si nuestro archivo esta siendo procesado, es con la utilización del ProgressBar, que permite ver dicho progreso del archivo que está siendo encriptado o desncriptado dicho archivo, dependiendo del formulario en que se encuentre.



Como se puede ver en la figura anterior, se creó un formulario de usuarios con el propósito de generar un nuevo usuario, modificar o borrar un registro existente, o simplemente permitirle al usuario que esté activo o inactivo.

6.2.3 DICCIONARIO DE DATOS

Tabla de Usuarios generada en Microsoft Access 2000

Nombre del campo	Tipo de Dato	Tamaño de Dato	Descripción
ID	Caracter	10	Código que identifica al usuario
Nombre	Caracter	40	Nombre o identificación del usuario
Password	Caracter	10	Clave del usuario para ingresar al sistema
Grupo	Caracter	50	Descripción del área al que pertenece el usuario
Activo	Caracter	1	Indica el estatus que se encuentra el usuario

6.3 DETERMINACIÓN DE RECURSOS UTILIZADOS

6.3.1 RECURSOS MATERIALES

Hardware

- Pentium IV
- RAM 256 MB
- Disco duro de 40 GB

Software

- Microsoft Visual Basic 6.0
- Microsoft Access 2000
- Microsoft Word
- Robohelp
- Windows XP

Dispositivos de entrada

- Teclado multimedia
- Ratón

Dispositivos de almacenamiento

- CDWRITE/DVD

6.3.2 REQUISITOS DE LA APLICACIÓN

Hardware

- Pentium III ó superior
- RAM 64 MB
- Disco Duro, con 500 MB de espacio libre

Sistema Operativo

- Microsoft Windows 95 ó superior

CAPITULO VII

EVALUACIÓN

7.1 METODOLOGÍA PARA REALIZAR PRUEBAS.

ENCUESTA ACERCA DEL SISTEMA PROTECTOR.

Marque con una **X** en la opción de **SI** o **NO** según su criterio

	SI	NO
1. Considera usted que el sistema protector es de fácil uso	☐	☐
2. Conoce de programas de encriptación	☐	☐
3. Constituye el sistema protector una herramienta de apoyo para el usuario de la Biblioteca Virtual de la PUCESA	☐	☐
4. Utilizaría el sistema protector como medio de protección de los archivos	☐	☐
5. Posee un ambiente agradable al utilizar el sistema protector	☐	☐
6. Considera que la ayuda del sistema protector es muy útil	☐	☐
7. Considera usted que se debe capacitar al usuario antes de utilizar el sistema protector	☐	☐
8. En la interfase de usuario del sistema protector cree usted que le hace falta agregar o quitar algún aspecto	☐	☐

Indique Cual(es) _____

_____

7.2 RESULTADOS DE LA METODOLOGÍA:

De acuerdo a la encuesta realizada a un grupo de 30 usuarios de la Biblioteca Virtual de la PUCESA en horarios diferentes, se alcanzo obtener los siguientes resultados:

	SI	NO
1. Considera usted que el sistema protector es de fácil uso.	100%	0%
2. Conoce de programas de encriptación.	60%	40%
3. Constituye el sistema protector una herramienta de apoyo. para el usuario de la Biblioteca Virtual de la PUCESA.	100%	0%
4. Utilizaría el sistema protector como medio de protección de los archivos.	100%	0%
5. Posee un ambiente agradable al utilizar el sistema protector.	97%	3%
6. Considera que la ayuda del sistema protector es muy útil.	90%	10%
7. Considera usted que se debe capacitar al usuario antes de utilizar el sistema protector.	100%	0%
8. En la interfase de usuario del sistema protector cree usted que le hace falta agregar o quitar algún aspecto.	3%	97%

Indique Cual (es):

Partiendo de la Hipótesis: se puede obtener lo siguiente.

Aplicando el Metodo Lógico y considerando que se tiene las siguientes variables:

Variable Independiente: La implementación del proyecto de seguridad de archivos y software.

Variable Dependiente: Biblioteca Virtual de la PUCESA una gran ayuda en la obtención de información confiable y en tiempo prudente, permitiendo de esta manera publicar revistas técnicas, artículos, libros digitalizados y aplicaciones informáticas.

A → B

De acuerdo al oficio entregado por la Ing. Mónica Mena, se demuestra que si se implementa más proyectos de seguridad de archivos también se incrementará la protección del Derecho Intelectual de los usuarios, y dicha información será más confiable y segura sin el peligro de que pueda ser modificada.

Ambato, Octubre 19 del 2004.

Ing. Mónica Mena.
ADMINISTRADORA DE LA BIBLIOTECA VIRTUAL PUCESA.

Certifico, que el señor Miguel Angel Rodríguez Pérez, realizó las siguientes tareas en la Biblioteca Virtual de la PUCESA, en el proceso de desarrollo de la Disertación *"Seguridad de Archivos en la Biblioteca Virtual de la PUCESA para la Protección del Derecho Intelectual"*, las mismas que detallo a continuación:

Estudio del hardware en el proceso de intalación.

Instalación de Programa Protector.

Capacitación al Personal.

El Sr. Miguel Rodríguez puede hacer uso del presente certicado, en la forma que él estime conveniente.

Ing. Mónica Mena Moreno.
CC. 050213730-0

PONTIFICIA
UNIVERSIDAD
CATOLICA
DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUT
BIBLIOTECA VIRTUAL
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telf: 593 3 416 220
Fax: 593 3 411 868 ext.102
pucesedeambato@hotmail.com
Ambato - Ecuador

Ambato, Octubre 22 del 2004

Ingeniero
Telmo Viteri
DIRECTOR ESCUELA DE SISTEMAS PUCESA
Presente

De mi consideración:

Reciba un cordial saludo, y aprovecho ésta oportunidad para comunicarle que el día jueves 21 del presente mes y año en la Biblioteca Virtual de verificó la Disertación: "Seguridad de Archivos para la Biblioteca Virtual de la PUCESA para Protección del Derecho Intelectual", correspondiente al Sr. Miguel Ángel Rodríguez Pérez, con lo cual se pudo comprobar la funcionalidad y utilidad de la aplicación tomando en cuenta los requisitos preestablecidos para su desarrollo.

Por lo tanto me permito señalar que la aplicación cumple con el objetivo propuesto y puede presentarse a su defensa respectiva.

Particular que pongo en su conocimiento para los fines consiguientes.

Atentamente,

Ing. Diego Santacruz
ADMINISTRADOR
CENTRO DE COMPUTO PUCESA

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato
ESCUELA DE INGENIERIA DE SISTEMAS
SECRETARIA
Recibido: Salud
Fecha: 22 Octubre Hora: 11:05

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUT
BIBLIOTECA VIRTUA

Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telf: 593 3 416 220
Fax: 593 3 411 868 ext.102
pucesedeambato@hotmail.com
Ambato - Ecuador

Ambato, Octubre 22 del 2004
OFIC-BV-002

Ingeniero
Telmo Viteri
DIRECTOR ESCUELA DE SISTEMAS PUCESA
Presente

De mi consideración:

Reciba un cordial saludo, y aprovecho ésta oportunidad para comunicarle que el día jueves 21 del presente mes y año en la Biblioteca Virtual de verificó la Disertación: "Seguridad de Archivos para la Biblioteca Virtual de la PUCESA para Protección del Derecho Intelectual", correspondiente al Sr. Miguel Ángel Rodríguez Pérez, con lo cual se pudo comprobar la funcionalidad y utilidad de la aplicación tomando en cuenta los requisitos preestablecidos para su desarrollo.

Por lo tanto me permito señalar que la aplicación cumple con el objetivo propuesto y puede presentarse a su defensa respectiva.

Particular que pongo en su conocimiento para los fines consiguientes.

Atentamente,

Ing. Mónica Mena Moreno
ENCARGADA
BIBLIOTECA VIRTUAL PUCESA.

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
Sede Ambato
ESCUELA DE INGENIERIA DE SISTEMAS
SECRETARIA
Recibido: Cecilia
Fecha: 22 octubre Hora: 11:06

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
CENTRO DE COMPUT
BIBLIOTECA VIRTUA
Av. Manuelita Sáenz s/n
Sector El Tropezón
Apartado Postal No.18-01-662
Telf: 593 3 416 220
Fax: 593 3 411 868 ext.102
pucesedeambato@hotmail.com
Ambato - Ecuador

7.3 CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- No existen sistemas de protección-encriptación para los documentos electrónicos de la Biblioteca Virtual de la PUCESA, por lo que son accesibles por cualquier usuario.

- La encriptación se basa en Algoritmos matemáticos, ya que mientras más complejo es el Algoritmo matemático, el Algoritmo de encriptación se vuelve más eficiente.

- Los archivos que se utilizan en la Biblioteca Virtual de la PUCESA, no garantizan la integridad de la información.

- La seguridad de la información es un tema de vital importancia en la PUCESA y no se escatima esfuerzos para protegerla.

- Para sistemas Operativos diferentes a Windows XP, se debe instalar un parche con la version de la Base de Datos de Microsoft Access.

Recomendaciones:

- Conocer la legislación que rige nuestro país, para cumplir y hacer cumplir dichas leyes.

- Crear los archivos de la Biblioteca Virtual de la PUCESA, con normas de seguridad estrictas.

- Promover el estudio de los diferentes métodos de encriptación, en los estudiantes, de la asignatura de Teoría de la Información, para que se logre aplicar los principios de seguridad con los diferentes algoritmos.

- Utilizar este trabajo de investigación como fuente de consulta de los estudiantes y público en general.

- Instalar en todas las computadoras de la Biblioteca Virtual de la PUCESA, el Sistema Operativo de Microsoft Windows XP, ya que garantiza mejor funcionamiento.

- Implementar equipos de UPS en la Biblioteca Virtual de la PUCESA, para asegurar la atención a los usuarios.

BIBLIOGRAFÍA

- Guía de Seguridad e Integridad de Datos, Farley
- Sistemas de Autentificación para Seguridades de Redes, Oppliger
- A Prueba de Hackers, Klander
- Criptografía digital. Fundamentos y aplicaciones, Pastor, José; Sarasa, Miguel Angel
- Técnicas criptográficas de protección de datos. Segunda edición, Fúster, Amparo; De la Guía, Dolores; Hernández, Luis; Montoya, Fausto; Muñoz, Jaime
- Introducción a la criptografía. Segunda edición, Caballero, Pino
- Cobb, Sthephen. Manual de Seguridad para PC y Redes Locales. McGraw-Hill, 1994.
- Fisher, Royal. Seguridad en los Sistemas Informáticos. Ediciones Díaz de Santos, 1988.

INTERNET

- Kriptópolis

  http://www.kriptopolis.com/

- CriptoRed

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

- National Security Agency (Agencia Nacional de Seguridad)

  http://www.nsa.gov/

- Página Web de Bruce Schneier

  http://www.counterpane.com/schneier.html

- Página Web de Vincent Rijmen: Rijndael

  http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

- Cryptome: documentos sobre criptografía

  http://cryptome.org/

- Delitos Informáticos y Leyes

  http://www.delitosinformaticos.com/

- Ley Orgánica de Protección de Datos LOPD

  http://www.igsap.map.es/cia/dispo/lo15-99.htm

ANEXOS

Preguntas de la encuesta para obtener el Método Gráfico son las siguientes:

1.- Considera usted que el sistema protector es de fácil uso.

2.- Conoce de programas de encriptación.

3.- Constituye el sistema protector una herramienta de apoyo para el usuario de la Biblioteca Virtual de la PUCESA.

4.- Utilizaría el sistema protector como medio de protección de los archivos.

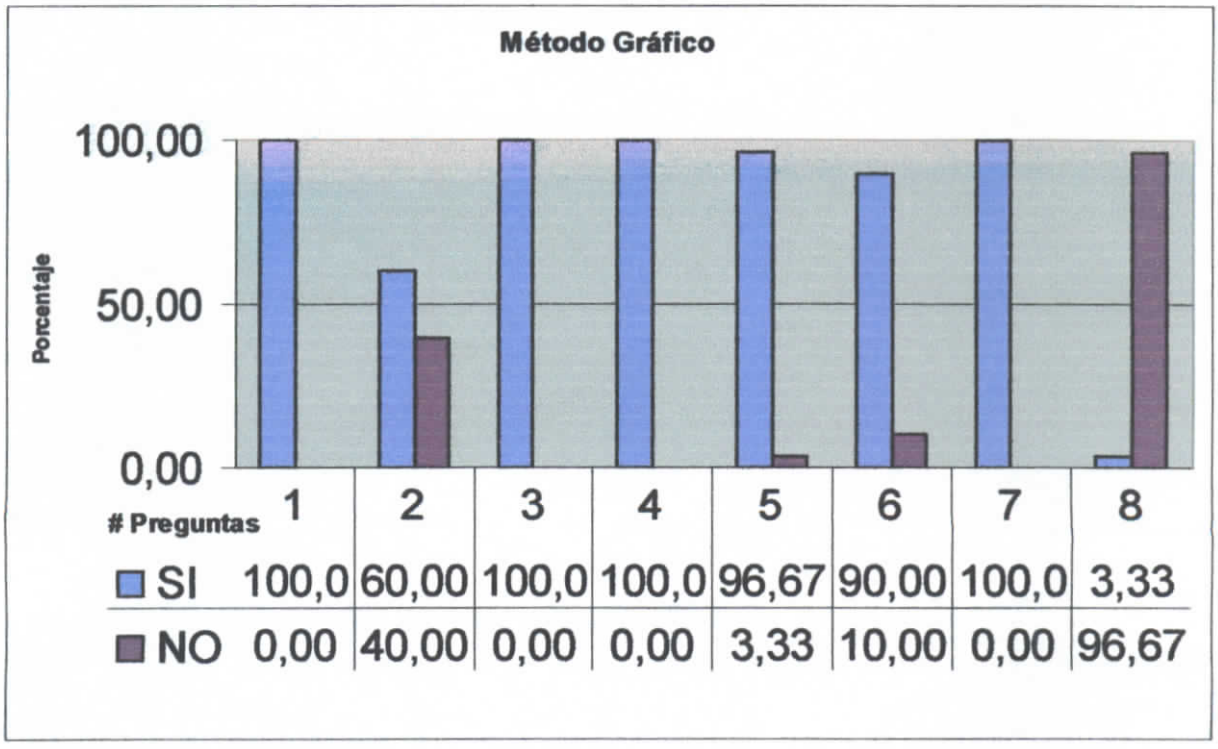
5.- Posee un ambiente agradable al utilizar el sistema protector.

6.- Considera que la ayuda del sistema protector es muy útil.

7.- Considera usted que se debe capacitar al usuario antes de utilizar el sistema protector.

8.- En la interfase de usuario del sistema protector cree usted que le hace falta agregar o quitar algún aspecto.

Indique Cual (es):

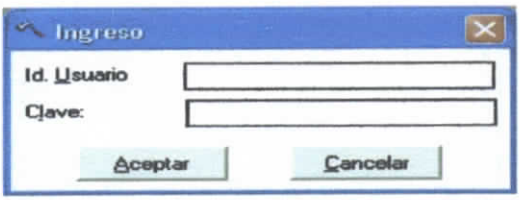


MANUAL DE USUARIO

Dentro de su estructura se puede decir que se deben seguir algunos pasos principales para la utilización de la misma, que a continuación se detalla:

Login:

- Para su utilización del sistema es necesario que conozca la identificación del usuario que se lo puede dar el Administrador del Sistema llamado Protector.exe con su respectiva Clave, de lo contrario será imposible su utilización.



- Dentro de este cuadro digitar la Identificación del Usuario que su longitud máxima es de 10 caracteres, caso contrario debe consultar con el Administrador del sistema, luego en el siguiente paso ingresar su Clave de acceso que puede ser máximo hasta 10 caracteres, si está seguro de lo que ingreso presione el botón Aceptar, caso contrario presione el botón Cancelar.
- Si presionó el botón Aceptar y los datos ingresados son correctos, usted puede utilizar el Sistema Protector.

Menú Principal:

- Dicha pantalla se refiere al Menú Principal en donde podemos elegir las opciones de **PRINCIPAL, PROCESOS y AYUDA.**
- Dentro de la opción **PRINCIPAL** tenemos las opciones de **Usuarios** y **Salir**:



Usuarios:

En la pantalla de usuarios tenemos cuatro campos que son:

I.D Usuario.- en este campo nos indica su identificación y nos permite ingresar máximo 10 caracteres.

Nombre.- en dicho campo podemos ingresar máximo 40 caracteres.

Clave.- en este campo podemos ingresar máximo 10 caracteres.

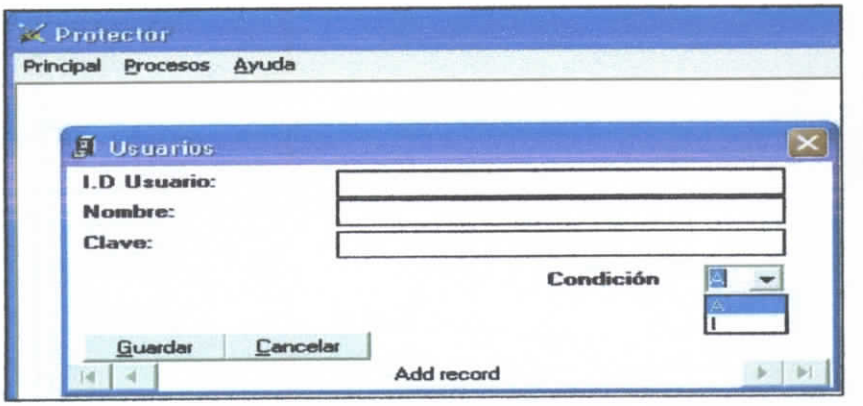
Condición.- en este campo nos indica el estatus del usuario que se encuentra por lo que la letra **A** indica en estatus Activo caso contrario la letra **I** indica en estatus Inactivo.

Una vez observado los cuatro campos, tenemos en la parte inferior cinco botones y el número de Registro al que pertenece el usuario como se observa en la siguiente imagen.



Nuevo:

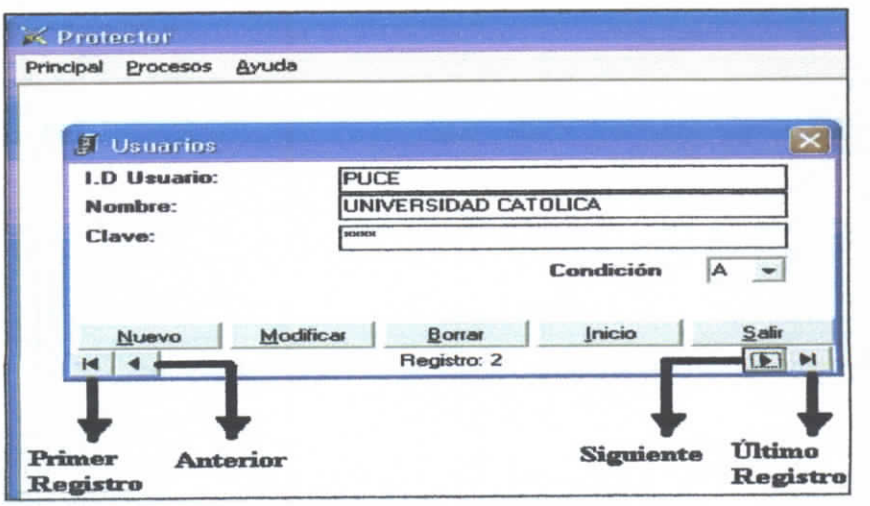
Si presiona el Botón **Nuevo** aparece la pantalla para ingresar los datos del usuario como se puede observar a continuación:



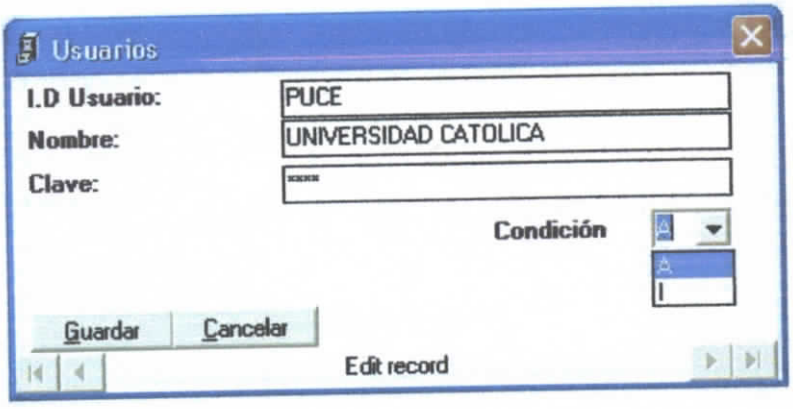
En esta pantalla tenemos las opciones de **Guardar** o **Cancelar** dichos datos del Usuario.

Modificar:

Si desea **Modificar** algún registro existente en la base de datos, primero debemos seleccionar dicho registro presionando las flechas que vemos en la siguiente pantalla:

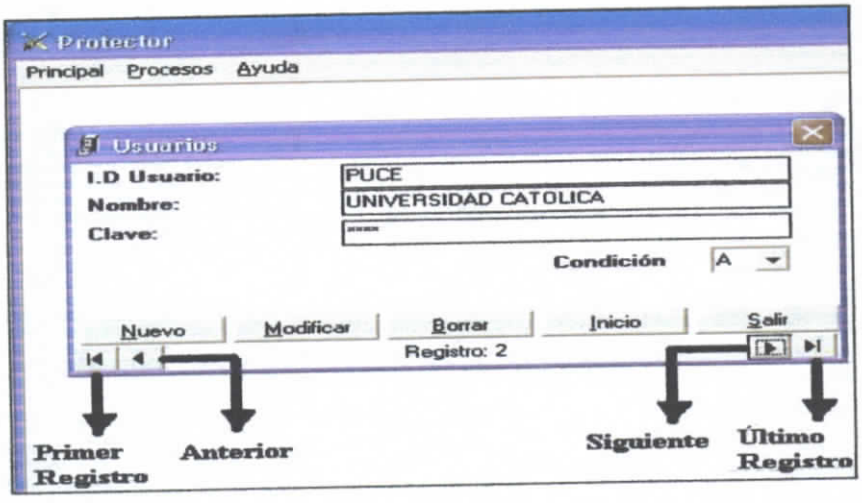


Una vez encontrado el registro presionar el botón de **Modificar** en donde aparecerá una nueva pantalla que nos permita **Guardar** o **Cancelar** dicha Modificación.



Borrar:

Si elige el botón de **Borrar,** primero debemos seleccionar el registro presionando las flechas que a continuación se detalla:



Luego presionamos el Botón **Borrar** y automáticamente se eliminará el registro.

El Botón **Inicio** permite observar el primer registro creado en la base de datos.

El Botón **Salir** nos indica cerrar la ventana de **Usuarios** y regresar al Menú Principal.

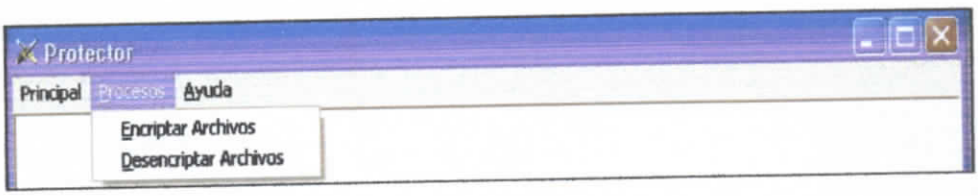


Salir:

Esta opción permite Salir del Sistema Protector.

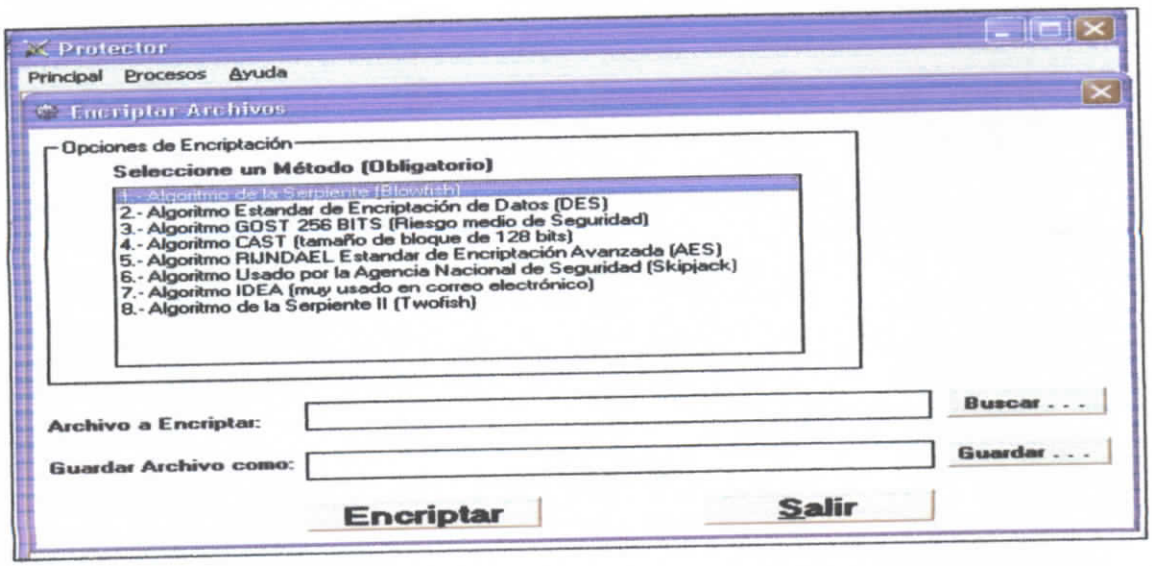
Dentro de la opción de **PROCESOS** se puede observar en la siguiente imagen:

Encriptar Archivos y Desencriptar Archivos.



Encriptar Archivos:

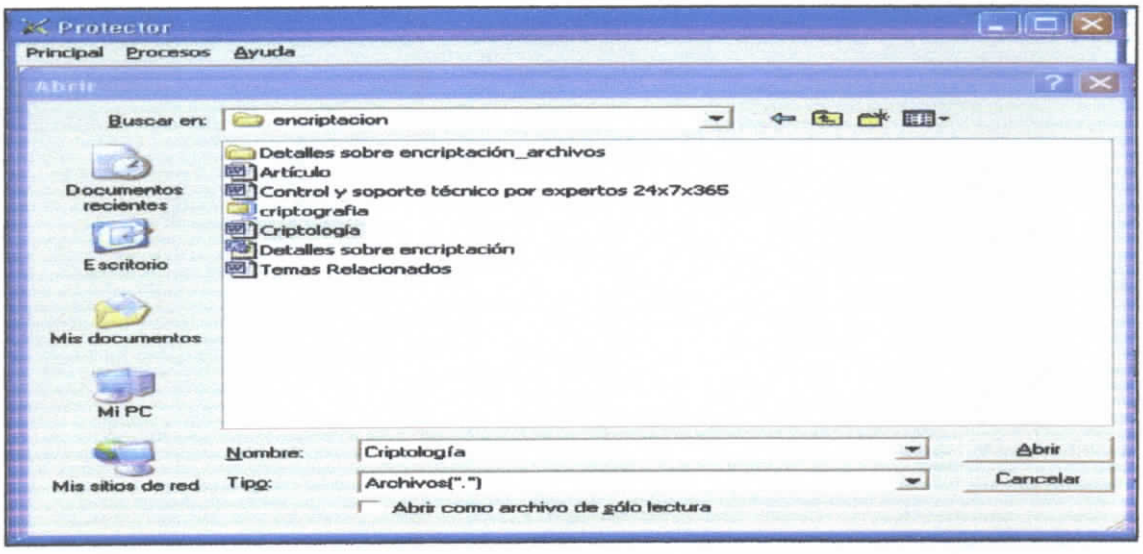
En esta opción nos permite Encriptar cualquier tipo de archivo, para lo cual existen varios Métodos o Algoritmos empleados para encriptar dichos archivos.



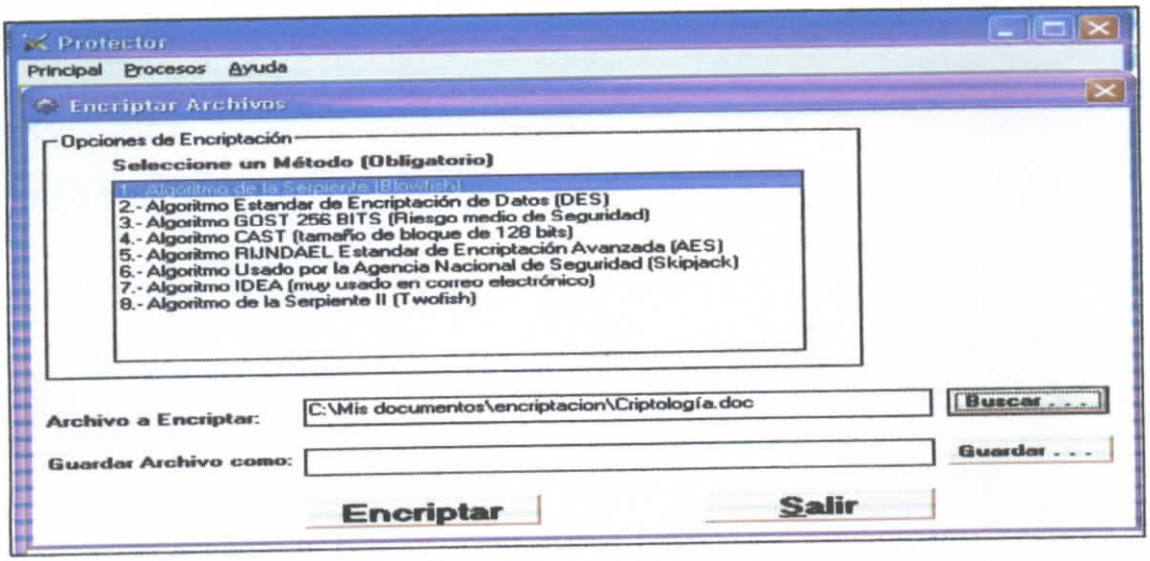
Como se puede observar en la imagen tenemos algunos Métodos de Encriptación tales como: **Algoritmo de la Serpiente (Blowfish), Cifrado DES, Algoritmo GOST, Algoritmo CAST, Algoritmo AES, Algoritmo Skipjack, Algoritmo IDEA y Algoritmo de la Serpiente II (Twofish).**

Buscar:

Una vez que haya seleccionado el Algoritmo con el que desea encriptar hacer un click en el botón **Buscar** puede seleccionar el archivo de donde desea, una vez encontrado el archivo presionar el botón **Abrir**, caso contrario presionar el botón **Cancelar** para regresar a la pantalla antes indicada.

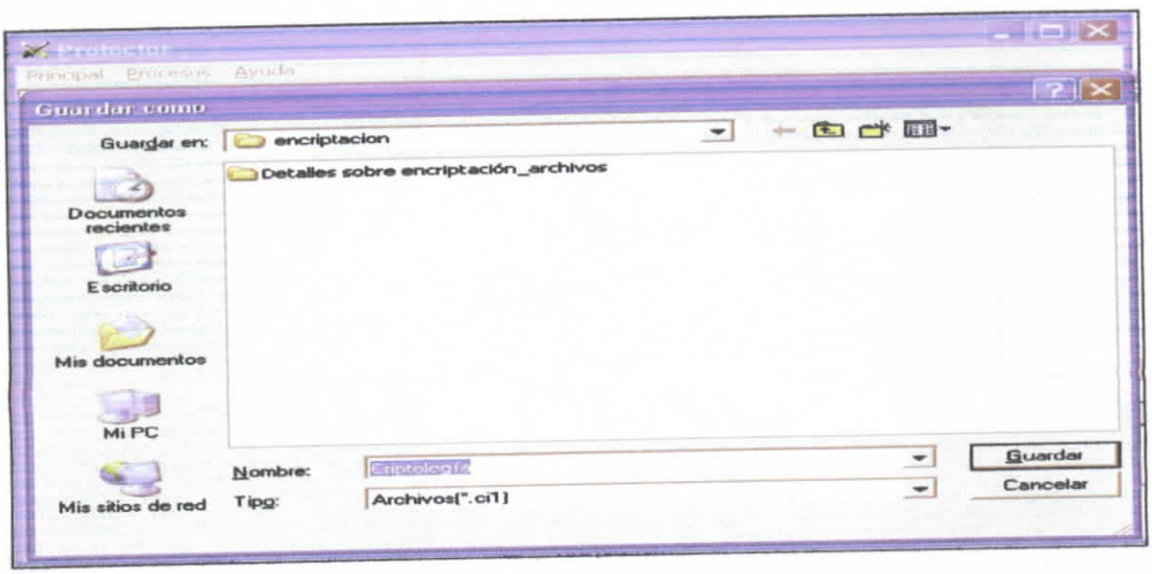


Si presionó el botón **Abrir** veremos que en el cuadro de texto Archivo a Encriptar nos indica la ruta de donde se eligió el archivo con su respectivo nombre.

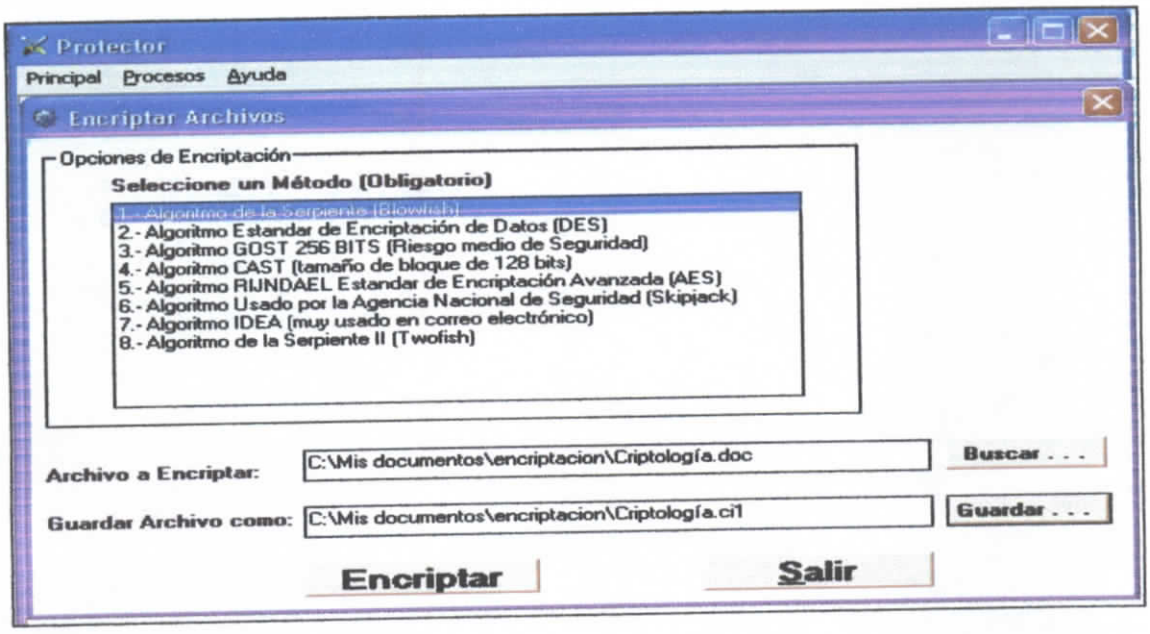


Guardar:

Luego hacemos un click en el botón **Guardar**, y nos aparece la siguiente pantalla Guardar como, es decir que puede guardar en el lugar mas adecuado y puede poner otro nombre de archivo si desea, se puede observar que el tipo de archivo se Guardará con la extensión ci y el número dependerá del Método que seleccionó anteriormente.



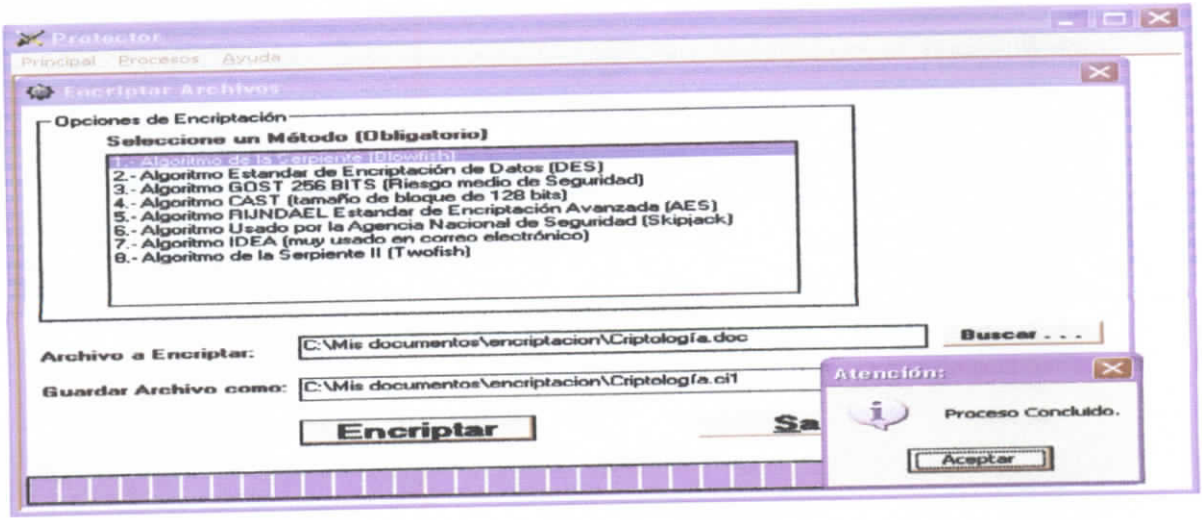
Como se puede observar en la siguiente imagen aparece el nombre del Archivo y su respectiva extensión con el que fue Guardado.



Encriptar:

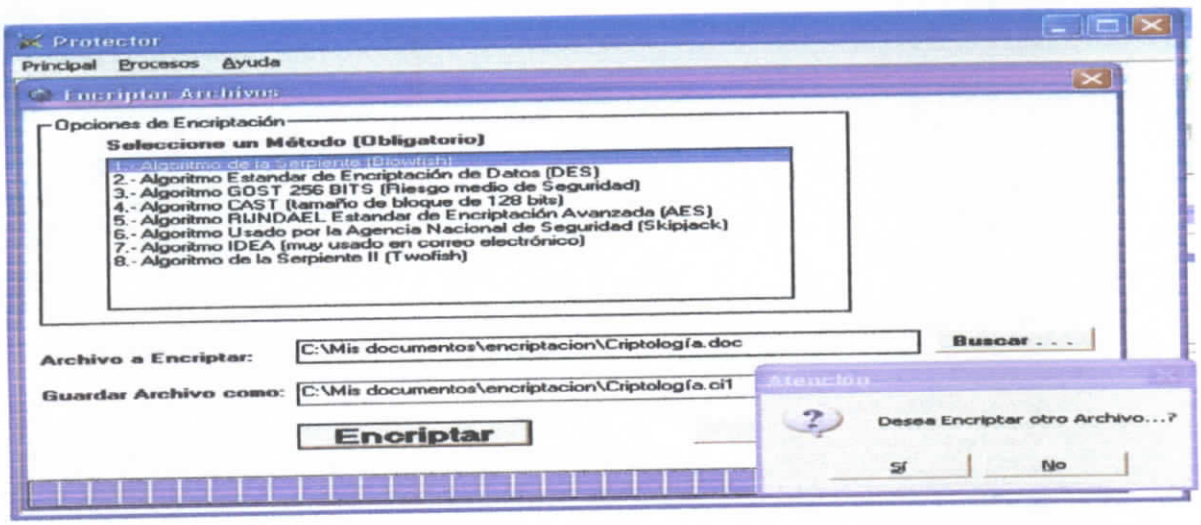
Una vez realizado los pasos anteriores presionar en el botón **Encriptar** para realizar dicho proceso.

Después aparecerá una ventana indicando **Proceso Concluido** como se puede observar en la siguiente imagen y presionar el botón **Aceptar**, esto indica que dicho proceso de Encriptación se ha realizado satisfactoriamente.



Luego de presionar el botón Aceptar aparece la siguiente imagen en la cual dice si Desea Encriptar otro Archivo.

Si presiona el botón **Si** regresa a realizar una nueva Encriptación de otro Archivo que desea, caso contrario presionar el botón **No** para salir del Proceso de Encriptación como se puede observar en la siguiente imagen.

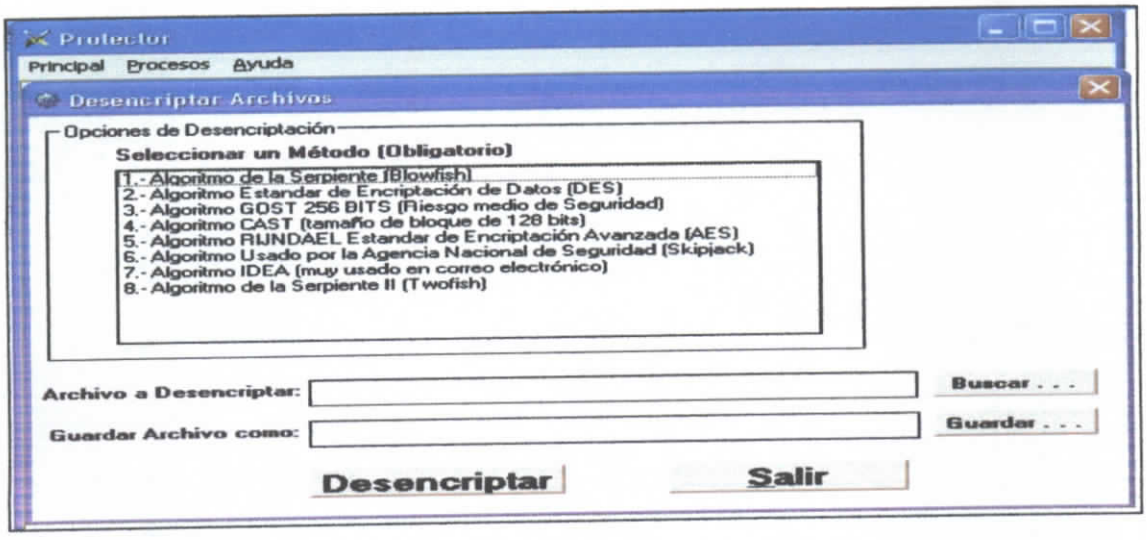


Salir:

Si presiona el botón **Salir** antes de Encriptar el Archivo, este botón permite regresar al Menú Principal.

Desencriptar Archivos:

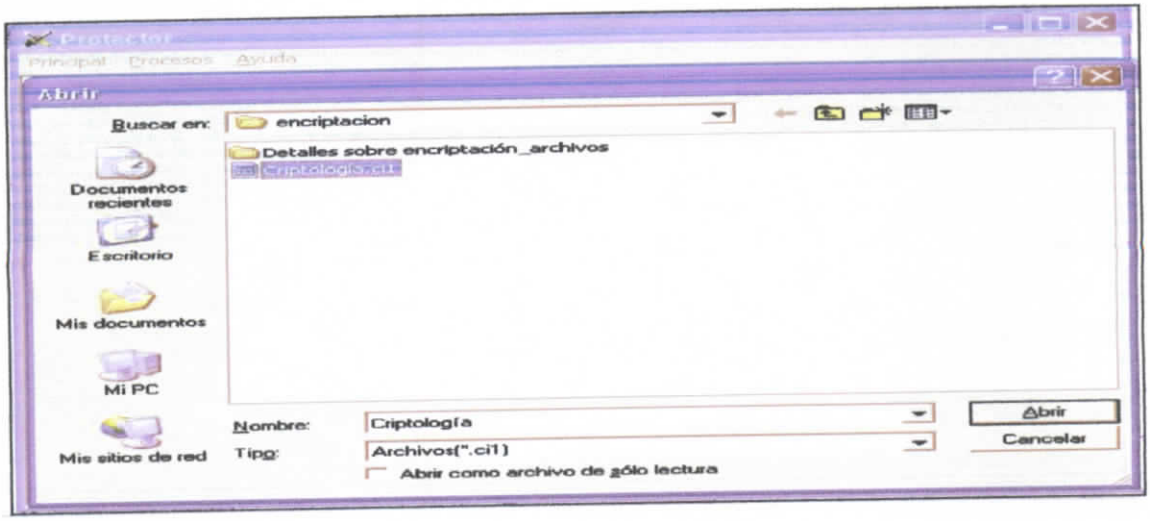
Si elige la opción Desencriptar desde el Menú Principal, tendremos la siguiente imagen, la cual permite volver a su forma inicial dicho archivo que antes fue encriptado.



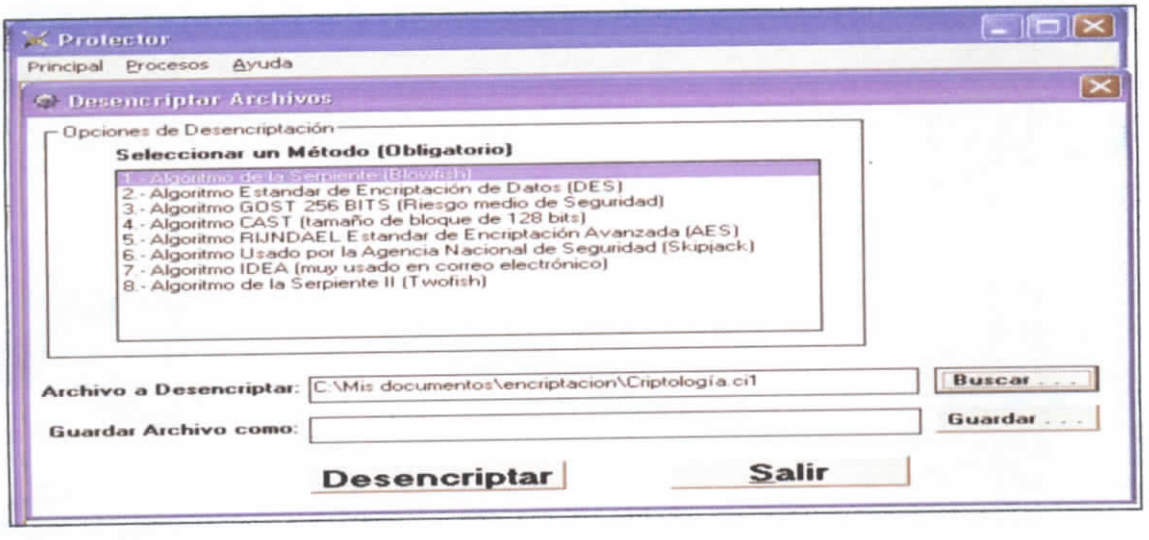
Para su efecto se debe seguir los siguientes pasos:

Buscar

Hacer un click en el botón **Buscar** de la pantalla Desencriptar Archivos, que nos permite ver la siguiente pantalla **Abrir** el archivo para poder Buscar en el lugar donde fue Encriptado anteriormente; pero antes debe seleccionar el Método con el cual fue encriptado dicho archivo que desea Buscar, caso contrario no aparecerá el Archivo y no se podrá Abrir como se puede observar en la siguiente imagen.

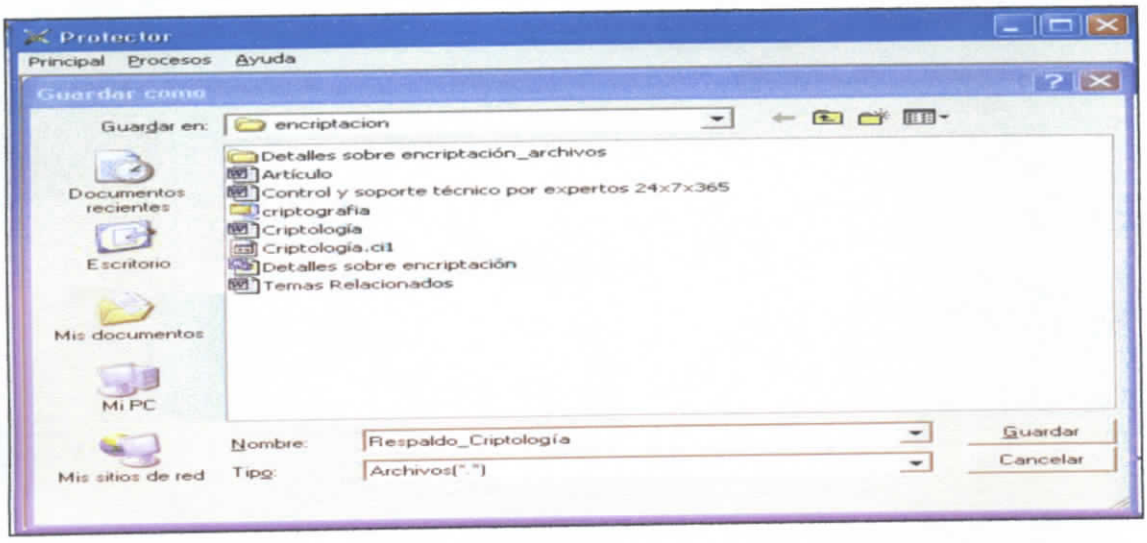


Una vez encontrado el archivo a Desencriptar, presionar el botón **Abrir** donde regresará a la pantalla de Desencriptar Archivos y como se observa en la siguiente imagen en el cuadro de texto de Archivo a Desencriptar se tiene la ruta en donde se encontraba dicho Archivo Encriptado.

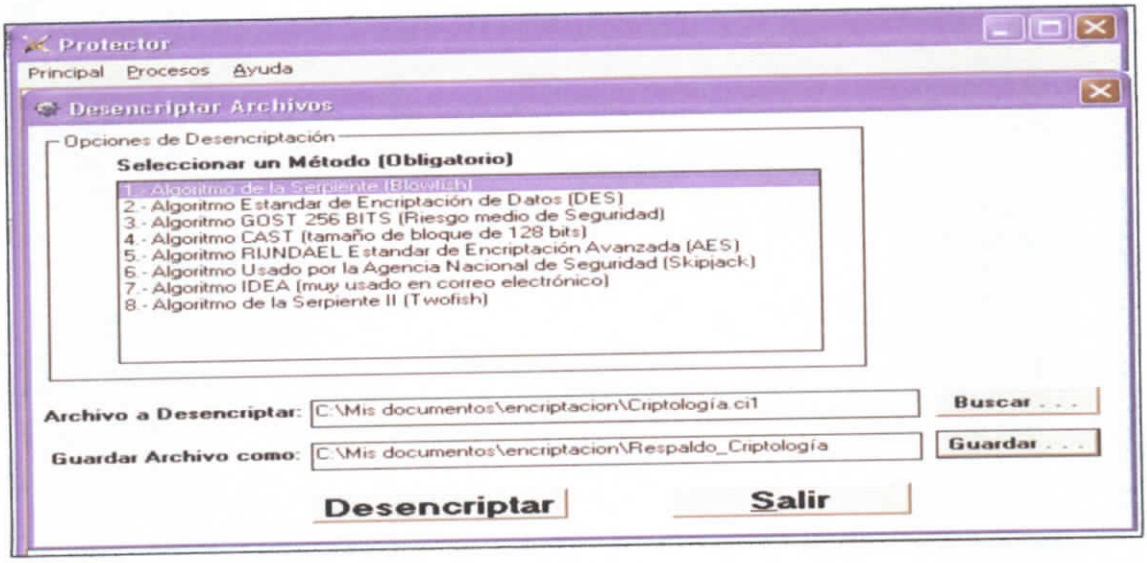


Guardar

Luego el siguiente paso presionar el botón **Guardar** con la finalidad de Guardar el Archivo en el lugar más adecuado y con el nombre que más lo identifique, después presionar el botón **Guardar,** como se observa a continuación en la siguiente imagen.

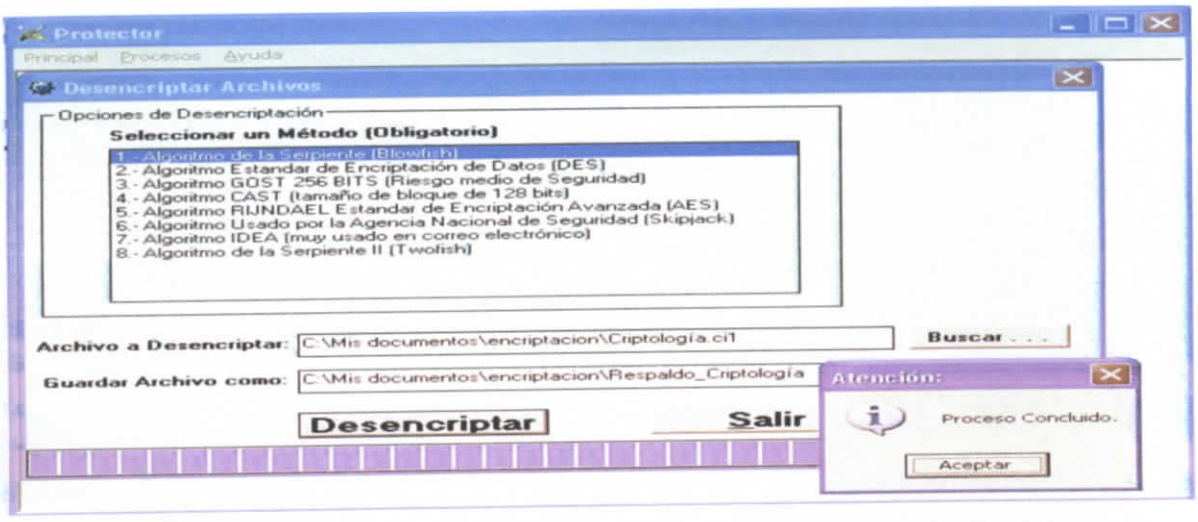


Una vez realizado los procesos antes mencionados, se observa la pantalla Desencriptar Archivos en donde se puede ver en el cuadro de texto de **Guardar Archivo como** el nombre con el que se Guardará el Archivo que va hacer Desencriptado posteriormente.

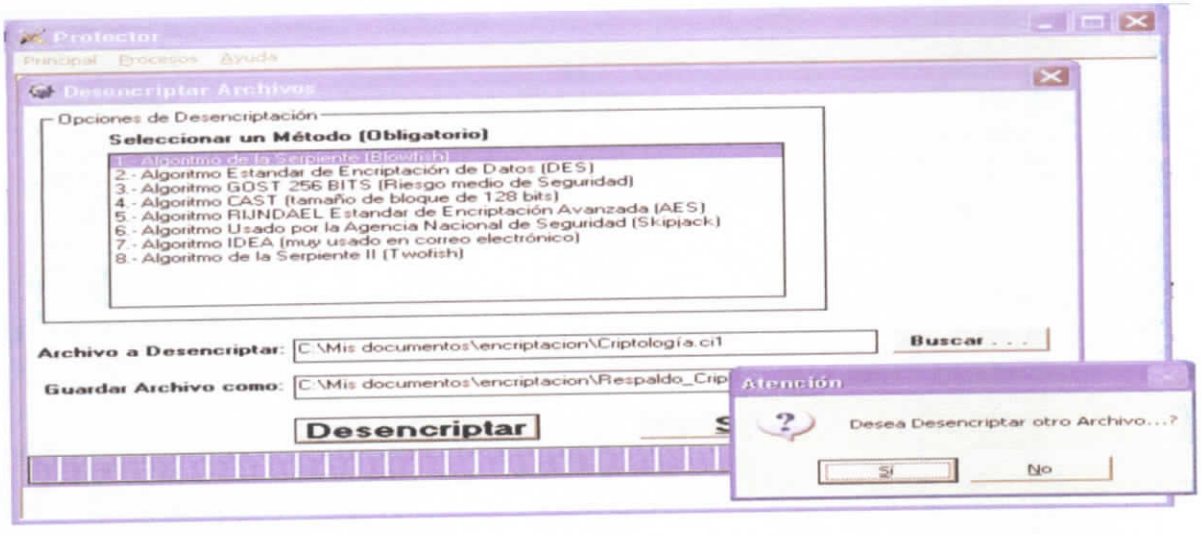


Desencriptar

Luego presionar el botón **Desencriptar** en donde indica que el Proceso ha Concluido como se observa a continuación en la siguiente imagen.



Luego presionar el botón **Aceptar** y se observará la siguiente imagen como se puede ver a continuación indicando si desea Desencriptar otro Archivo.



Ayuda:

- Dentro de la opción **AYUDA** tenemos:



Ayuda del Programa:

Esta opción permite leer los pasos que debe seguir para la utilización de forma correcta y efectiva del Sistema Protector.exe

GLOSARIO DE TÉRMINOS

CD – ROM.- Memoria de sólo lectura; memoria permanente.

CBC.- Encadenamiento de bloques.

CFB.- Realimentación de bloques.

EBC.- Libro electrónico de códigos.

GB.- Gigabytes.

GF.- Galois Field; elemento de galois.

Hackers.- Quien sin autorización trata de obtener acceso a los archivos.

Hardware.- Equipo físico.

HTML.- Lenguaje de programación; lenguaje de marcaje de hipertexto.

HTTP.- Protocolo que define las solicitudes y respuestas legales.

HUB.- Agujero de un panel de conexiones.

ID.- Identificador.

IEPI.- Inscripción en el Registro de Propiedad Intelectual.

LRL.- Licencias de redistribución libre.

MB.- Megabyte.

MHZ.- Megahertz.

OFB.- Realimentación bloque de salida.

Password.- Clave.

PC.- Computadora personal.

PCI.- Interrupción controlada por programa.

PDL.- Lenguaje de descripción de páginas.

PGP.- Pretty Good Privacy; privacidad bastante buena.

PKI.- Clave pública.

RAM.- Memoria de acceso al azar; memoria de trabajo.

RS.- Separador de registros.

SRL.- Software redistribuible libremente.

SOFTWARE.- Programas y sistemas de programación.

TEST.- Verificación.

