UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA
FACULTAD DE CIENCIAS E INGENIERIA
DEPARTAMENTO DE COMPUTACION

TEMA: Seguridad de Redes

SUBTEMA: El Protocolo de Seguridad IP

TRABAJO DE SEMINARIO DE GRADUACION PARA OPTAR AL TITULO DE LICENCIADO EN CIENCIAS DE LA COMPUTACION

AUTORES:

Br. Juan Bosco Ramírez Corea.
Br. Imelda Esther Morales Morales.
Br. Mauren Jimena Somarriba Collado.

TUTOR:

Msc. Eman Hussein Yousif

Managua, 11 de Febrero del 2011.

Subtema:

El PROTOCOLO DE SEGURIDAD IP

DEDICATORIA

*A **Dios**, sobre todas las cosas, por permitirme culminar mis estudios universitarios y por darme sabiduría, entendimiento y fuerza de voluntad.*

*A mi **Madre**, por brindarme su apoyo, por depositar su confianza y sobre todo por ser la persona que me dio la vida a quien admiro mucho.*

*A mi **Esposa e Hijos**, por ser la fuente de inspiración que me impulsa a cumplir mis metas.*

Br. Juan Bosco Ramírez Corea
2011

DEDICATORIA

*A **Dios**, que me permite vivir, luchar y principalmente darme fuerzas para seguir adelante.*

*A mi **Madre**, porque me ha dado la vida, porque me ha motivado a terminar mis estudios y por su apoyo en los momentos más difíciles de mi vida.*

*A mi **Hija**, porque es la principal fuente de inspiración para luchar en la vida.*

Br. Imelda Esther Morales Morales
2011

DEDICATORIA

*A **DIOS** por estar siempre a mi lado y no permitir que abandonara, en momentos de debilidad este curso.*

*A mi **familia** por confiar en mí y por brindarme todo el cariño que necesitaba.*

*A mi **esposo,** que con su apoyo incondicional y sus consejos me ayudaron a culminar mis metas como profesional y como ser humano.*

*A mi **hijo**, porque con su presencia a llenado todo en mí, y mi mayor deseo es ser digna de ejemplo a seguir para él.*

Br. Mauren Jimena Somarriba Collado.

2011

AGRADECIMIENTO

A mi ***tutor****, Msc. Eman Hussein Yousif, por ser la guía en nuestra tesis, por dedicar su tiempo y apoyo en la realización y culminación de nuestro trabajo.*

A un ***Amigo*** *especial que nos brindó su apoyo en la realización de nuestra aplicación, por su tiempo y dedicación.*

A mis ***amigos****, que me brindaron su amistad, tiempo, conocimiento, consejos en el transcurso de mis estudios universitarios.*

Br. Juan Bosco Ramírez Corea.

2011

AGRADECIMIENTO

*A nuestro **tutor**, Msc. Eman Hussein, por el apoyo que nos ha brindado en estos meses de trabajo en equipo.*

A mis dos compañeros de grupo Mauren y Juan Bosco por su tiempo, ayuda y paciencia, ya que sin el esfuerzo que hemos realizado los 3 juntos la culminación de este trabajo no hubiera sido posible.

*A mis **amigos**, compañeros de trabajo, mi madre, mis hermanas que me brindaron su amistad, tiempo, conocimiento, consejos.*

Br. Imelda Esther Morales Morales
2011

AGRADECIMIENTO

Gracias le doy a mi ***madre*** *la Sra. Ada Rosa Collado, por confiar en mí, y darme todo el amor que solo una verdadera madre sabe dar y a mi* ***padre*** *el Sr. Felipe Somarriba por ser responsable con mis estudios.*

Le agradezco con todo mi corazón, a mi ***esposo*** *Elí Roque, que con paciencia, esmero y confianza y sobre todo amor dijo las palabras correctas en el momento que más lo necesite.*

Agradezco también a mis ***amigos y compañeros*** *Bosco e Imelda por permitirme formar este equipo y por supuesto a nuestro tutor Msc. Eman Hussein Yousif por su entrega y dedicación para sacar adelante esta investigación. Gracias.*

Br. Mauren Jimena Somarriba Collado.

2011.

INDICE

Pág.

RESUMEN

La estructura que presenta este trabajo se divide en seis capítulos que se agruparán en dos bloques. La primera parte hace referencia al trabajo de investigación teórica y se compone de los primeros cinco capítulos, mientras que la segunda parte se compone del capítulo seis dónde se presenta la parte del diseño metodológico.

Este trabajo trata de la Seguridad en Redes y específicamente de la Seguridad IP, la cual permite cifrar y/o autentificar todo el tráfico de la red en el nivel IP. Esto a través de tres mecanismos fundamentales: autentificación, confidencialidad y gestión de claves.

Teniendo en cuenta estos mecanismos, se realizó una aplicación que simula la transferencia de archivos, aplicando los mecanismos de seguridad, y se utilizó un algoritmo de cifrado que nos permitió simular el envío de un archivo a través de una dirección IP.

En la parte final de este trabajo se presentarán las conclusiones obtenidas durante la realización de esta investigación documental, así como las futuras mejoras que podrían llevarse a cabo.

INTRODUCCION

El impresionante crecimiento de Internet y su correspondiente conectividad, además del advenimiento de nuevos servicios, ha propiciado que intrusos técnicamente avanzados consideren como un reto constante el emprender ataques de índole diversa que amenacen la integridad y la privacidad de redes de comunicación de datos en general.

En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas (como por ejemplo, recordar contraseñas, cambiarlas periódicamente, etc.) y que pueden limitar las operaciones que puede realizar así como los recursos a los que se le permite acceder.

Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.

En el presente trabajo se hizo una retrospectiva acerca de las características y los beneficios de la Arquitectura del Protocolo de Seguridad IP, y sus mecanismos de seguridad.

JUSTIFICACION

Con la realización de este trabajo de investigación se intentó dar a conocer los conceptos más importantes de la Seguridad IP, así mismo los mecanismos que esta utiliza para prevenir los daños que la mayor parte de las empresas sufren por la falta de la Seguridad IP.

Por tal razón, se realizó una aplicación que simula la transferencia de archivos utilizando el método de encriptación, el cual permite dar solución a uno de los problemas más comunes de la Seguridad IP como es la Confidencialidad.

Con la realización de dicho proyecto se espera que sea de mucha utilidad para futuras investigaciones del mismo tipo que abarque de manera más amplia los mecanismos de Seguridad IP.

OBJETIVOS

Objetivo General

- Realizar una aplicación que simule la transferencia de archivos, empleando los mecanismos de la Seguridad IP, para dar solución a los problemas de seguridad más comunes.

Objetivos Específicos

- Presentar conceptos de redes, para describir de manera general que son las redes y cómo funcionan con el fin de conocer las tecnologías de comunicación.

- Conocer las generalidades sobre seguridad informática, para analizar los peligros y amenazas más comunes que existen en Internet.

- Dar a conocer en qué consisten los mecanismos de la seguridad IP, utilizando los algoritmos correspondientes, para dar solución a los problemas más comunes de la seguridad de las redes,

- Diseñar una aplicación y simular algunos mecanismos de seguridad de redes, empleando técnicas como el encriptado, para darle solución a los problemas de seguridad.

CAPITULO I: REDES DE COMPUTADORAS

1.1 Definición de una red

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en 7 capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a 4 capas.

1.2 Clasificación de las Redes

1.2.1 Por alcance

- **Red de área personal o PAN[1].**
- **Red de área local o LAN[2].**

[1] **PAN (personal área network)** es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona.

[2] **LAN (local área network)** es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización.

- **Red de área de campus o CAN.**[3]
- **Red de área metropolitana o MAN**[4]
- **Redes de área amplia o WAN**[5]
- **Red de área de almacenamiento o SAN**[6]
- **Red de área local virtual**[7]
- **Red irregular**[8]

1.2.2 Por topología

- **Una topología**[9] **de bus** usa un solo cable backbone[10] que debe terminarse en ambos extremos.
- **La topología de anillo** conecta un Host con el siguiente y al último host con el primero.
- **La topología en estrella** conecta todos los cables con un punto central de concentración.

---

[3] **CAN (campus área network)** es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.

[4] **MAN (metropolitan área network)** es una red de alta velocidad que da cobertura en un área geográfica extensa.

[5] **WAN (wide área network)** son redes informáticas que se extienden sobre un área geográfica extensa.

[6] **SAN (storage área network),** es una red concebida para conectar servidores, matrices de discos y librerías de soporte.

[7] **Virtual LAN (VLAN)** es un grupo de computadoras con un conjunto común de recursos a compartir y de requerimientos, que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras

[8] **Red Irregular** es un sistema de cables y buses que se conectan a través de un módem, y que da como resultado la conexión de una o más computadoras.

[9] **Topología** se refiere a la forma en que está diseñada la red, bien físicamente (rigiéndose de algunas características en su hardware o bien lógicamente (basándose en las características internas de su software.

[10] **Backbone** es un cable que conecta entre sí dos o más segmentos de una red local.

- **Una topología en estrella extendida** conecta estrellas individuales entre sí mediante la conexión de Hubs[11] o Switches[12]. Esta topología puede extender el alcance y la cobertura de la red.
- **Una topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los Hubs o Switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- **La topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio.

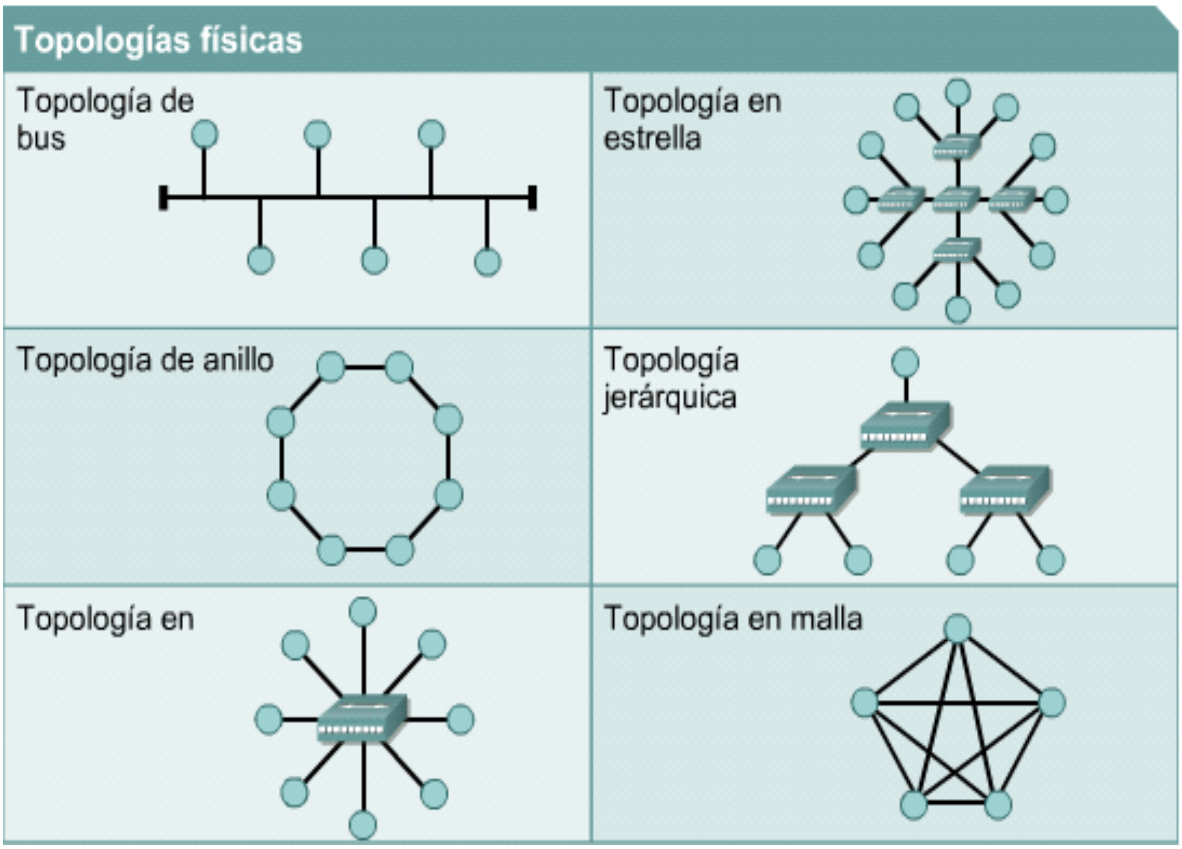


Figura 1.1: Topologías Físicas de Red

[11] **Hubs o concentrador** es un dispositivo que permite centralizar el cableado de una red.

[12] **Switches o conmutador** es un dispositivo digital que permite que varios dispositivos se conecten a un punto de la red.

1.3 Niveles de componentes de una red

Una red tiene tres niveles de componentes:

- **El software de aplicaciones:** formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos de bases de datos, de documentos, gráficos o vídeos) y recursos (como impresoras o unidades de disco). Un tipo de software de aplicaciones se denomina cliente-servidor.

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

- **El Hardware de Red:** formado por los componentes materiales que unen las computadoras. Dos componentes importantes son los **medios de transmisión** que transportan las señales de los ordenadores (típicamente cables estándar o de fibra óptica, aunque también hay redes sin cables que realizan la transmisión por infrarrojos o por radiofrecuencias) y el **adaptador de red**, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otras computadoras. La información se transfiere en forma de dígitos binarios, o bits (unos y ceros), que pueden ser procesados por los circuitos electrónicos de los ordenadores.

CAPITULO II: SEGURIDAD DE REDES

2.1 Concepto de Seguridad.

Se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

La seguridad es una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Esta característica, particularizando para el caso de sistemas operativos o redes de computadoras, se suaviza la definición de seguridad y se pasa a hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad, por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar cuatro aspectos:

- **La confidencialidad** nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.

- **La integridad** significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada.

- **La disponibilidad** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

- **La confiabilidad** entendida como el nivel de calidad del servicio ofrecido.

2.2 Clasificación de la Seguridad

2.2.1 Seguridad Informática

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida).

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software, bases de datos, meta datos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

2.2.1.1 Objetivos de la Seguridad Informática

Los objetivos de la Seguridad Informática son:

- **La información contenida**

  Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

- **La infraestructura computacional**

  Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- **Los usuarios**

  Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

2.2.1.2 Las amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la

descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

- **El usuario:** causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

- **Programas maliciosos:** programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware[13].

- **Un intruso:** persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker[14], defacer, script kiddie[15] o Script boy, etc.).

- **Un siniestro (robo, incendio, inundación):** una mala manipulación o una mala intención, derivan a la pérdida del material o de los archivos.

- **El personal interno de Sistemas:** Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

[13] **Un programa espía,** es un programa, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste. Se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

[14] **Cracker.** Viola la seguridad de un sistema informático y, toma control de este.

[15] **Script kiddie** es un término despectivo utilizado para describir a aquellos que utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes.

2.2.1.3 Tipos de amenazas

Existen 2 tipos de amenazas:

- **Amenazas internas:** Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:
  - ✓ Los usuarios conocen la red y saben cómo es su funcionamiento.
  - ✓ Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.
  - ✓ Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

- **Amenazas externas**: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

2.2.2 Seguridad de Redes

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Para entender los tipos de amenazas a la seguridad que existen, hay que partir de una definición de requisitos en seguridad. La seguridad en computadores y en redes implica:

- **Confidencialidad:** Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que

pueden ser utilizadas para inferir otros elementos de información confidencial.

- **Integridad:** Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc.

- **Autenticidad:** se requiere que un computador o servicio sea capaz de verificar la identidad de un usuario.

- **No repudio:** Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

- **Disponibilidad de los recursos y de la información:** De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

- **Consistencia:** Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas.

- **Control de acceso a los recursos:** Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

- **Auditoría:** Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas acciones.

2.2.2.1 Políticas Generales sobre la Seguridad

Diferentes políticas de seguridad, se engloban en 2 tipos.

- ✓ Todo está prohibido a menos que se permita explícitamente.
- ✓ Todo está permitido a menos que se prohíba explícitamente.

Cabe mencionar algunas estrategias de Seguridad, entre ellas:

- ✓ **Asignar a cada usuario el mínimo de privilegios que necesite**. El objetivo es minimizar los daños en caso de que la cuenta de un usuario sea invadida. En caso de que un usuario quiera realizar actividades diferentes tiene que solicitar que se le asignen los privilegios correspondientes.

- ✓ **Defensa en profundidad:** Consiste en usar tantos mecanismos de seguridad como sea posible, colocándolos uno tras otro. Puede hacer muy compleja la utilización del sistema.

- ✓ **Check Point:** Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto. Puede disminuir el rendimiento.

- ✓ **Falla en posición segura:** Los sistemas deben estar diseñados para que en caso de falla queden en un estado seguro. Por ejemplo en redes, en caso de falla se debe suspender el acceso a Internet.

- ✓ **Seguridad por Obscuridad:** La estrategia es mantener un bajo perfil y tratar de pasar desapercibido, de modo que los atacantes no lo detecten.

- ✓ **Simplicidad:** Los sistemas muy complejos tienden a tener fallas y huecos de seguridad. La idea es mantener los sistemas tan simples como sea posible, eliminando funcionalidad innecesaria. Sistemas simples que tienen mucho tiempo, han sido tan depurados que prácticamente no tienen huecos de seguridad.

- ✓ **Seguridad basada en hosts:** Los mecanismos de seguridad están en los hosts. Puede ser diferente en cada host, lo cual hace difícil su Instalación y mantenimiento. Si un host es atacado con éxito, peligra la seguridad de la red (muchos usuarios tienen el mismo login y password en todos los hosts a los que tienen acceso).

- ✓ **Seguridad basada en la red:** La seguridad se basa en controlar los accesos a los hosts desde la red. El método más común es la implementación de firewalls[16].

Una forma útil de clasificar los ataques a la seguridad es en términos de ataques pasivos y ataques activos.

- **Un ataque pasivo** intenta averiguar o hacer uso de la información del sistema, pero sin afectar a los recursos del mismo.

- **Un ataque activo** intenta alterar los recursos del sistema o influir en su funcionamiento.

[16] **Firewalls**. Es un mecanismo para proteger las redes, implementando un control de acceso hacia y desde Internet.

2.2.3 Seguridad en Internet

Intentar comunicar un secreto en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece.

La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que se lee, las páginas visitadas, las cosas que se compran y la gente a la que se habla representan información que a la mayoría de las personas no les gusta dar a conocer.

Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.

La seguridad en Internet y las leyes que la protegen, están basadas principalmente en los sistemas de encriptación. Esos sistemas son los que permiten que las informaciones que circulan por Internet sean indescifrables, ininteligibles, para cualquier persona que no sea aquella a la que va destinada.

2.2.3.1 Características de Seguridad de Internet

- **Gestión de claves** (incluyendo negociación de claves y su almacenamiento): Antes de que el tráfico sea enviado/recibido, cada router /cortafuegos /servidor (elemento activo de la red) debe ser capaz de verificar la identidad de su interlocutor.

- **Confidencialidad:** La información debe ser manipulada de tal forma que ningún atacante pueda leerla. Este servicio es generalmente prestado gracias al cifrado de la información mediante claves conocidas sólo por los interlocutores.

- **Imposibilidad de repudio:** Ésta es una forma de garantizar que el emisor de un mensaje no podrá posteriormente negar haberlo enviado, mientras que el receptor no podrá negar haberlo recibido.

- **Integridad:** La autenticación valida la integridad del flujo de información garantizando que no ha sido modificado en el tránsito emisor-receptor.

- **Autenticación:** Confirma el origen/destino de la información -corrobora que los interlocutores son quienes dicen ser.

- **Autorización:** La autorización se da normalmente en un contexto de autenticación previa. Se trata un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

CAPITULO III: LA ARQUITECTURA DE PROTOCOLOS TCP/IP

3.1 Historia

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPANET) que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. World Wide Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés).

3.2 Arquitectura TCP/IP

TCP/IP es un conjunto de protocolos. La sigla TCP/IP significa "**Protocolo de control de transmisión/Protocolo de Internet**" y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos.

Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- Dividir mensajes en paquetes.
- Usar un sistema de direcciones.

- Enrutar datos por la red.
- Detectar errores en las transmisiones de datos.

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

3.3 Las capas de TCP/IP

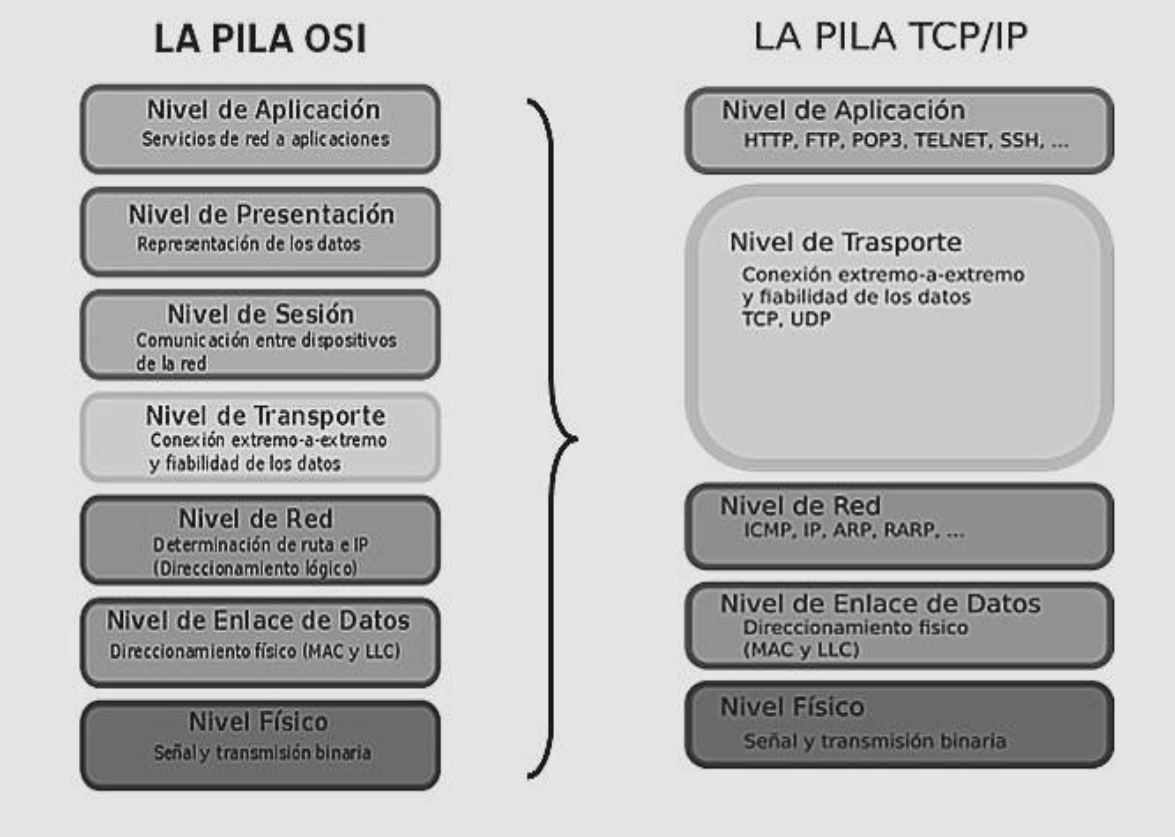


Figura 3.1: Comparación de la Pila OSI con la Pila TCP/IP

La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- **Capa de Aplicación:** Se corresponde con los niveles OSI de aplicación, presentación y sesión. Es la capa más alta de la pila; contiene toda la lógica necesaria para posibilitar las distintas aplicaciones de usuario. Los programas de aplicación escogen entre diferentes protocolos de transporte dependiendo del tipo de servicio de transporte que requieran. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP[17]), transferencia de ficheros (FTP[18]), conexión remota (TELNET[19]) y otros más recientes como el protocolo HTTP[20].

- **Capa de Transporte:** Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos. su principal tarea es proveer comunicación punto a punto entre las aplicaciones. Los protocolos de transporte (TCP y UDP) usan el servicio de entrega de paquetes que provee la capa de Internet.

---

[17] **El Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol).** Es un protocolo de servicio de correo electrónico, listas de correo, etc. y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP.

[18] **El Protocolo de Transferencia de Archivos (FTP, File Transfer Protocol)** se permite transmitir archivos tanto de texto como en binario. Además, el protocolo controla el acceso de los usuarios. Permite el envío y recepción de ficheros de cualquier tipo hacia un usuario

[19] **TELNET.** Es un protocolo para que dos computadores lejanos se puedan conectar y trabajar uno en el otro como si estuviera conectado directamente. Uno de ellos es el usuario y el otro el servidor. TCP se encarga del intercambio de información.

[20] **HTTP** es permitir la transferencia de archivos (principalmente, en formato HTML). entre un navegador (el cliente) y un servidor web mediante una cadena de caracteres denominada dirección URL.

- **Capa de Internet:** Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

- **Capa Física:** Análogo al nivel físico del OSI. En esta capa está definida la interfaz entre el dispositivo de transmisión de datos (por ejemplo: la estación de trabajo o el computador) y el medio de transmisión o red. Esta capa se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos y cuestiones afines.

- **Capa de Acceso a la Red:** Esta capa es la responsable del intercambio de datos entre el sistema final (servidor, estación de trabajo, etc.) y la red a la cual está conectada. El emisor debe proporcionar a la red la dirección del destino, de tal manera que esta pueda encaminar los datos hasta el destino apropiado.

3.4 El Protocolo TCP

TCP es un protocolo de transporte orientado a conexión enormemente extendido en Internet. Las aplicaciones de red más populares (ftp, telnet, acceso Web…) lo utilizan en sus comunicaciones.

La función principal del nivel de transporte dentro de la arquitectura de protocolos TCP/IP es la de permitir la comunicación extremo a extremo entre dos aplicaciones de forma económica y fiable.

La unidad básica de transferencia se denomina segmento, de tamaño máximo el denominado MSS[21].

Existe otro protocolo de transporte en la arquitectura TCP/IP muy diferente, UDP. Éste es mucho más sencillo que TCP. Se limita a enviar paquetes de datos, denominados datagramas, de un terminal a otro sin garantizar que éstos sean recibidos correctamente.

Si la aplicación requiere fiabilidad en la comunicación, deberá ser ella misma la que se la proporcione o bien se tendrá que recurrir al TCP.

3.4.1 Características Generales de TCP

TCP es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP).

TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión. Las principales características del protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.
- TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.

[21] **MSS (Maximum Segment Size**) expresado en octetos. que se negocia por los extremos de la comunicación en el establecimiento de la misma.

- TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

3.4.2 El objetivo de TCP

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores.

Esto significa que los routers[22] (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente[23], y la máquina receptora se llama servidor[24].

Por eso es que decimos que estamos en un entorno Cliente-Servidor.[25] Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

[22] **Router** es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.

[23] El **cliente** es una aplicación informática o un computador que accede a un servicio remoto en otro computador, conocido como servidor, normalmente a través de una red de telecomunicaciones.

[24] Un **servidor** es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman **segmentos**.

3.4.3 El formato de los datos en TCP

Un segmento TCP está formado de la siguiente manera:

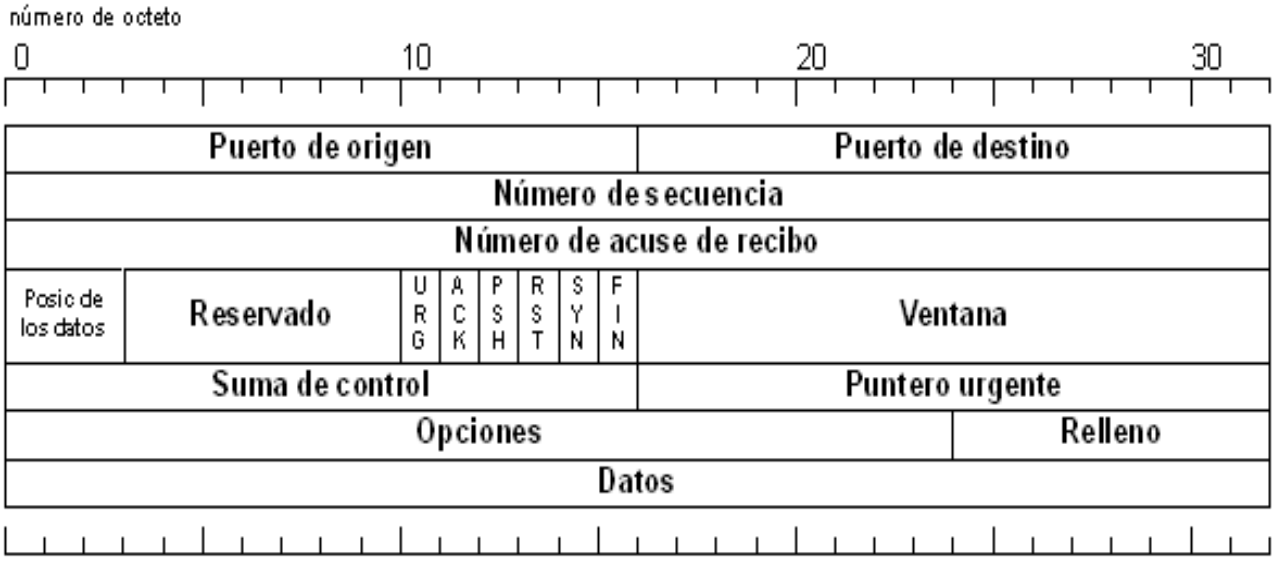


Figura 3.2 - Formato de la cabecera de TCP

Significado de los diferentes campos:

- **Puerto de origen** (16 bits): Puerto relacionado con la aplicación en curso en la máquina origen.

[25] La **arquitectura cliente-servidor** consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.

- **Puerto de destino** (16 bits): Puerto relacionado con la aplicación en curso en la máquina destino.

- **Número de secuencia** (32 bits): Cuando el indicador SYN está fijado en 0, el número de secuencia es el de la primera palabra del segmento actual. Cuando SYN está fijado en 1, el número de secuencia es igual al número de secuencia inicial utilizado para sincronizar los números de secuencia (ISN).

- **Número de acuse de recibo** (32 bits): El número de acuse de recibo, también llamado número de descargo se relaciona con el número (secuencia) del último segmento esperado y no el número del último segmento recibido.

- **Margen de datos** (4 bits): Esto permite ubicar el inicio de los datos en el paquete. Aquí, el margen es fundamental porque el campo opción es de tamaño variable.

- **Reservado** (6 bits): Un campo que actualmente no está en uso pero se proporciona para el uso futuro.

- **Indicadores** (6x1 bit): Los indicadores representan información adicional:
  - ✓ **URG**: Si este indicador está fijado en 1, el paquete se debe procesar en forma urgente.
  - ✓ **ACK**: Si este indicador está fijado en 1, el paquete es un acuse de recibo.
  - ✓ **PSH** (PUSH): Si este indicador está fijado en 1, el paquete opera de acuerdo con el método PUSH.
  - ✓ **RST**: Si este indicador está fijado en 1, se restablece la conexión.
  - ✓ **SYN**: El indicador SYN de TCP indica un pedido para establecer una conexión.
  - ✓ **FIN**: Si este indicador está fijado en 1, se interrumpe la conexión.

- **Ventana** (16 bits): Campo que permite saber la cantidad de bytes que el receptor desea recibir sin acuse de recibo.
- **Suma de control** (CRC): La suma de control se realiza tomando la suma del campo de datos del encabezado para poder verificar la integridad del encabezado.
- **Puntero urgente** (16 bits): Indica el número de secuencia después del cual la información se torna urgente.
- **Opciones** (tamaño variable): Diversas opciones
- **Relleno**: Espacio restante después de que las opciones se rellenan con ceros para tener una longitud que sea múltiplo de 32 bits.

3.5 El protocolo UDP

El protocolo UDP (Protocolo de datagrama de usuario) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión). Por lo tanto, el encabezado del segmento UDP es muy simple:

puerto de origen (16 bits);	**puerto de destino (16 bits);**
longitud total (16 bits);	**suma de comprobación del encabezado (16 bits);**
Datos (longitud variable).	

Figura 3.3: Encabezado del Segmento UDP

Significado de los diferentes campos

- **Puerto de origen**: es el número de puerto[26] relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario. Por lo tanto, este campo es opcional. Esto significa que si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).

- **Puerto de destino**: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

- **Longitud**: este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de 4 x 16 bits (que es 8 x 8 bits), por lo tanto la longitud del campo es necesariamente superior o igual a 8 bytes.

- **Suma de comprobación**: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento.

3.5.1 Funciones de UDP

Entre las funciones que realiza el UDP están:

- **Acceso a puertos:** UDP provee la capacidad de acceder a los puertos, a diferencia de TCP, con servicios Sin-Conexión y No-Confiables. Muchas aplicaciones necesitan direccionar a IP y el acceso a puertos de TCP, pero manejando ellas mismas la verificación de los datos, por lo que UDP es la solución ideal.

[26] **Puerto** es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir.

- **Envió de paquetes:** También es usado por aplicaciones que solamente envían mensajes cortos y pueden enviar de nuevo los mensajes si la respuesta no llega en corto tiempo.

3.5.2 Modo de Conexión

El concepto de conexión es muy importante porque le permite a un puerto local dar servicio a muchos puertos remotos concurrentemente. Esta es la base del modelo de aplicación cliente-servidor que es usado en redes.

Una aplicación envía un mensaje independiente a otra aplicación mediante el Protocolo de Datagramas de Usuario (UDP). UDP añade una cabecera creando una unidad denominada datagrama de UDP o mensaje de UDP. UDP traslada los mensajes de UDP salientes a IP. UDP acepta mensajes de UDP entrantes de IP y determina la aplicación de destino. UDP es un servicio de comunicaciones no orientado a conexión que suele usarse en aplicaciones de búsquedas simples en bases de datos.

3.6 El protocolo IP

El protocolo de Internet (IP) es llamado la base tecnológica de TCP/IP. El protocolo IP y sus protocolos de encaminamiento asociados son posiblemente la parte más significativa del conjunto TCP/IP.

IP es sin conexión. Está basado en la idea de los datagramas interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el host de origen hasta el host destino, quizás recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en datagramas, de hasta 64K octetos cada uno. Cada datagrama se transmite a través de la red interred, posiblemente fragmentándose

en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un datagrama IP consta de una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable. En la **figura 3. 4** se muestra el formato de la cabecera.

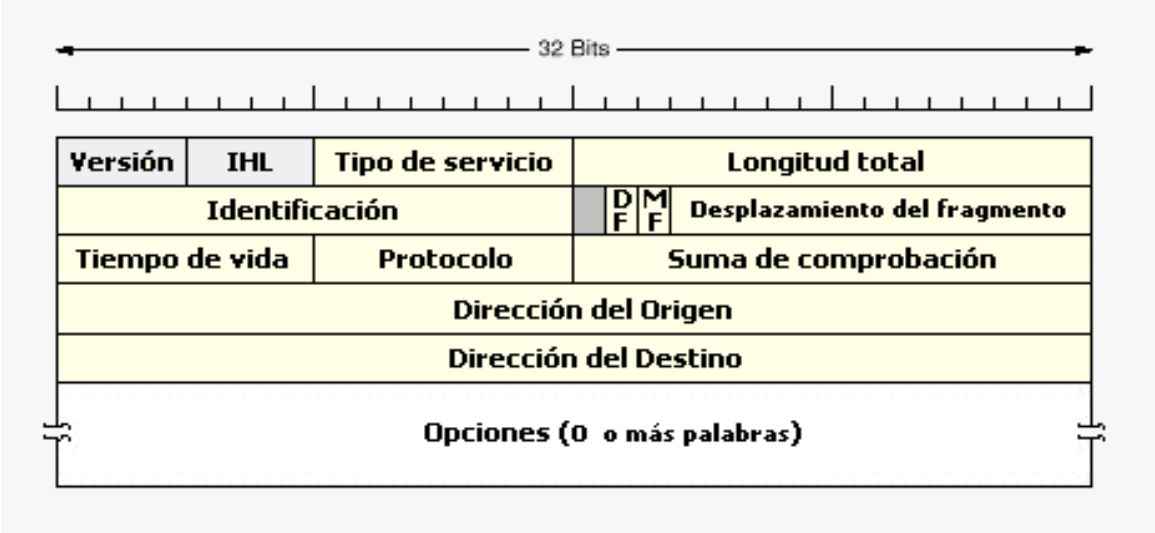


Figura 3.4: Formato de la cabecera IP

Los campos de la cabecera IP son:

- El campo **Versión** indica a qué versión del protocolo pertenece cada uno de los datagramas. Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.
- La **longitud de la cabecera** no es constante, un campo de la cabecera, **IHL**, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. Tamaño 4 bit.

- El campo **Tipo de servicio** le permite al host indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Tamaño 8 bit.

- La **Longitud total** incluye todo lo que se encuentra en el datagrama, tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos (bytes). Tamaño 16 bit.

- El campo **Identificación** se necesita para permitir que el hostal destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación. Tamaño 16 bits.

- Enseguida viene un bit que no se utiliza después dos campos de 1 bit. Las letras **DF** quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente. Si el datagrama no puede pasarse a través de una red, se deberá encaminar sobre otra red, o bien, desecharse. Las letras **MF** significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificación doble contra el campo de **Longitud total,** con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

- El **desplazamiento de fragmento** indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo **Longitud total.** Tamaño 16 bits.

- El campo **Tiempo de vida** es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits. Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo *Protocolo* indica, a qué proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más.

- **Protocolo:** El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.

- El **código de redundancia de la cabecera** es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del **código de redundancia** de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. Tamaño: 16 bit.

- **La Dirección de origen** contiene la dirección del *host* que envía el paquete. Tamaño: 32 bit.

- **La Dirección de destino:** Esta dirección es la del *host* que recibirá la información. Los routers o gateways[27] intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bit.

[27] **Una pasarela o puerta de enlace** es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

- El campo **Opciones** se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Esto, básicamente, proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar, la asignación de bits de cabecera a información que muy rara vez se necesita.

3.6.1 La dirección de Internet

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

- **Clase A**: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que

tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPANET es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

- **Clase B:** Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del *host* permitiendo, por consiguiente, un número máximo de 64516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de ordenadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

- **Clase C:** En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 ordenadores en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Clase	Primer byte	Identificación de red	Identificación de hosts	Número de redes	Número de hosts
A	1 ... 126	1 byte	3 byte	126	16.387.064
B	128 ... 191	2 byte	2 byte	16.256	64.516
C	192 ... 223	3 byte	1 byte	2.064.512	254

Tabla 3.1: Tabla de direcciones IP de Internet.

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos.

El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran conectadas, en la identificación de host para máquinas que aún no conocen su número de *host* dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast[28]:

[28] **Broadcast**, **difusión** en español, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

- ✓ El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de sistemas, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno.
- ✓ Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un ordenador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

El broadcast es una característica que se encuentra implementada de formas diferentes dependiendo del medio utilizado, y por lo tanto, no siempre se encuentra disponible.

3.6.2 La nueva versión de IP

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (Internet Protocol Next Generation). El número de versión de este protocolo es el 6 (que es utilizada en forma mínima) frente a la antigua versión utilizada en forma mayoritaria. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.).

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

3.6.2.1 Formato de la cabecera.

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión. El formato completo de la cabecera sin las extensiones es el siguiente:

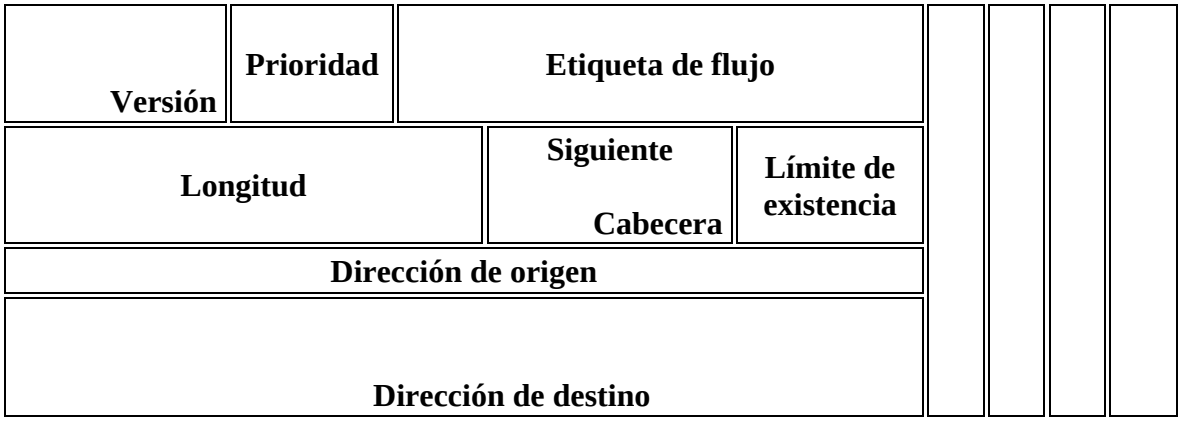


Figura 3.5: Organización de la cabecera IPv6.

- **Versión:** Número de versión del protocolo IP, que en este caso contendrá el valor 6. Tamaño: 4 bit.

- **Prioridad:** Contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 4 bit.

- **Etiqueta de flujo:** Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los routers que lo soporten. Tamaño: 24 bit.

- **Longitud:** Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 bit.

- **Siguiente cabecera:** Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 bit.

- **Límite de existencia:** Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño: 8 bit.

- **Dirección de origen:** El número de dirección del host que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 bit.

- **Dirección de destino:** Número de dirección de destino, aunque puede no coincidir con la dirección del host final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. Tamaño: 128 bit.

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento.

Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para routing extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

3.6.2.2 Direcciones en la versión 6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bit (cuatro veces mayor). Estas nuevas direcciones identifican a un interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos a través de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme. Teóricamente serían 2^{128} direcciones posibles, siempre que no apliquemos algún formato u organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 **trillones** de direcciones distintas por cada **metro cuadrado** de la superficie del planeta Tierra.

Según diversas fuentes consultadas, estos números una vez organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564

direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a un interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso.

Estos tres tipos de direcciones son:

- **Direcciones unicast:** Son las direcciones dirigidas a un único interfaz de la red. Las direcciones unicast que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.

- **Direcciones anycast:** Identifican a un conjunto de interfaces de la red. El paquete se enviará a un interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones *unicast* que se encuentran asignadas a varios interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones unicast.

- **Direcciones multicast:** Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente.

Las direcciones de broadcast no están implementadas en esta versión del protocolo, debido a que esta misma función puede realizarse ahora mediante el uso de las direcciones multicast.

CAPITULO IV: PROTOCOLO DE TRANSFERENCIAS DE ARCHIVOS

4.1 Historia

En 1969, nació ARPANET como una pequeña red de pocos ordenadores que transmitían información de unos a otros mediante paquetes conmutados, y tres años más tarde un grupo de investigadores del MIT presentó la propuesta del primer "Protocolo para la transmisión de archivos en Internet".

Era un protocolo muy sencillo basado en el sistema de correo electrónico pero sentó las bases para el futuro protocolo de transmisión de archivos (FTP).

En 1985, quince años después de la primera propuesta, se termina el desarrollo del aún vigente protocolo para la transmisión de archivos en Internet (FTP), basado en la filosofía de cliente-servidor.

El gran boom de Internet se produce en 1995. Este año puede ser considerado como el nacimiento de la Internet comercial. Desde ese momento su crecimiento ha superado todas las expectativas. En este año la World Wide Web supera a FTP transformándose en el servicio preferido de la red, después de que el año anterior superase en popularidad a Telnet.

Con la llegada del World Wide Web, y de los navegadores, ya no es necesario conocer los complejos comandos de FTP, este protocolo se puede utilizar escribiendo la URL del servidor al que queramos conectar en el navegador web, indicando con **ftp: //** que vamos a contactar con un servidor ftp y no con un servidor web (que sería **http://**).

La versión original del FTP fue publicado como RFC 114 el 16 de abril de 1971, y más adelante reemplazado por el RFC 765 (junio de 1980) y el RFC 959 (octubre de 1985), la versión que se usa actualmente. Muchos han propuesto alternativas a la versión de 1985, como por ejemplo el RFC 2228 (junio de 1997)

que propone extensiones de seguridad y la RFC 2428 (septiembre de1998) que añade soporte para IPv6 y define un nuevo tipo de modo pasivo.

4.2 Función del FTP

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP.

El objetivo del protocolo FTP es:

- Permitir que equipos remotos puedan compartir archivos.
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor.
- Permitir una transferencia de datos eficaz.

4.3 El Modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control)
- Un canal de datos

Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- **DTP** (Proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado

del servidor se denomina Servidor de DTP y el DTP del lado del cliente se denomina Usuario de DTP.

- **PI** (Intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:
  - ✓ El Servidor PI es responsable de escuchar los comandos que provienen de un Usuario PI a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del Usuario PI a través de éste, de responderles y de ejecutar el Servidor DTP.

  - ✓ El Usuario PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del Servidor PI y de controlar al Usuario de DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor.

Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro.

Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la

transferencia de información entre dos procesos del servidor conectados en el puerto correcto.

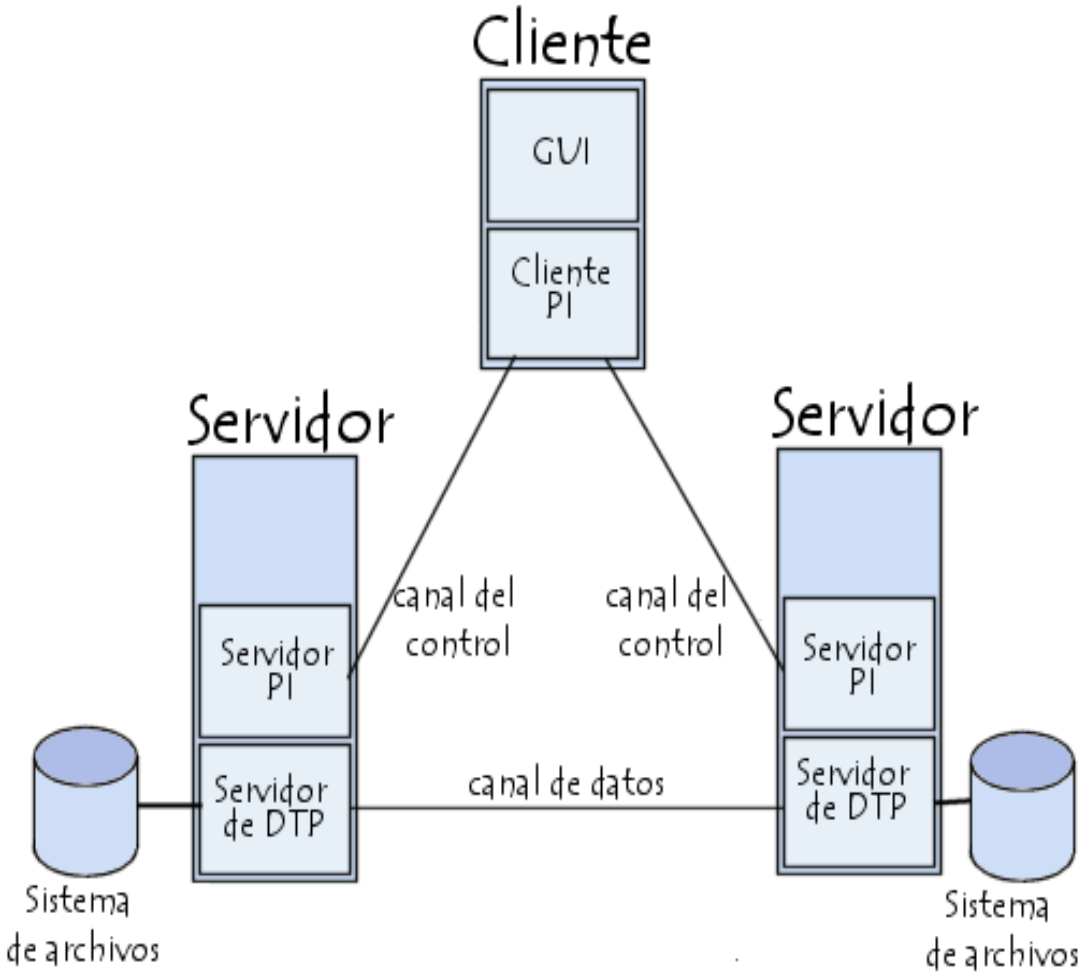


Figura 4.1: Diagrama de un servicio FTP

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

4.4 Tipos de transferencia de archivos en FTP

Es importante conocer cómo debemos transportar un archivo a lo largo de la red. Si no utilizamos las opciones adecuadas podemos destruir la información del archivo. Por eso, al ejecutar la aplicación FTP, debemos acordarnos de utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica):

- **Tipo ASCII:** Adecuado para transferir archivos que sólo contengan caracteres imprimibles (archivos ASCII, no archivos resultantes de un procesador de texto), por ejemplo páginas HTML, pero no las imágenes que puedan contener.

- **Tipo binario:** Este tipo es usado cuando se trata de archivos comprimidos, ejecutables para PC, imágenes, archivos de audio, etc.

CAPITULO V: SEGURIDAD IP

La comunidad de internet ha desarrollado mecanismos de seguridad para aplicaciones específicas en una serie de áreas como, por ejemplo, correo electrónico (S/MIME[29], PGP[30]), cliente/servidor (Kerberos[31]), acceso a la Web (SSL[32]), entre otras. Sin embargo, los usuarios tienen preocupaciones relativas a la seguridad que rebasan las capas de protocolos.

La seguridad IP abarca tres áreas fundamentales: autentificación, confidencialidad y gestión de claves.

- El mecanismo de autentificación garantiza que un paquete recibido, de hecho, fue transmitido por la parte identificada como fuente u origen en la cabecera del paquete. Además, este mecanismo asegura que el paquete no ha sido alterado durante la transmisión.
- La herramienta de confidencialidad permite que los nodos que se comunican cifren los mensajes para prevenir escuchas de terceras partes.
- La herramienta de gestión de claves se ocupa del intercambio seguro de claves.

---

[29] **S/MIME (Secure / Multipurpose Internet Mail Extensions, del inglés, Extensiones de Correo de Internet de Propósitos Múltiples / Seguro):** es un estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME.

[30] **Pretty Good Privacy o PGP (privacidad bastante buena):** es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública.

[31] **Kerberos**: es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

[32] **SSL (Secure Sockets Layer):** Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

5.1 Introducción a la seguridad IP

En 1994, el Comité de Arquitectura de Internet (IAB: Internet Architecture Board) publicó un informe titulado Seguridad en la Arquitectura de Internet (RFC 1636).

El informe manifestaba el consenso general sobre la necesidad de una mayor y mejor seguridad en Internet, e identificaba la necesidad de proteger la infraestructura de la red de la observación y el control no autorizado del trafico de red, así como la necesidad de asegurar el trafico entre usuarios finales utilizando mecanismos de autenticación y cifrado.

Estas preocupaciones están del todo justificadas. Como prueba, el informe anual del 2001 del Equipo de respuestas a Emergencia en Computadores o CERT (Computer Emergency Response Team) informaba sobre más de 52000 incidentes de seguridad.

Los tipos de ataque más graves incluían los falsos IP, en los que los intrusos crean paquetes con direcciones IP falsas y explotan las aplicaciones que usan autenticación basadas en IP; y distintas formas de escucha y captura de paquetes, donde los atacantes leen la información transmitida, incluida la de conexión al sistema y la de los contenidos de bases de datos.

En respuestas a estas cuestiones, la IAB incluyo la autenticación y el cifrado como características necesarias de seguridad en el IP de nueva generación, que se conoce como IPv6. Afortunadamente, estas capacidades de seguridad se diseñaron para que fueran empleadas con el actual IPv4 y el futuro IPv6.

Esto significa que los fabricantes ya pueden empezar a ofrecer estas características, y ya muchos de ellos han incorporado algunas capacidades de IPSec a sus productos.

5.1.1 Aplicaciones de IPSec

IPSec proporciona la capacidad de asegurar las comunicaciones a través de una LAN, de una WAN privada y pública y de Internet. Los siguientes son algunos ejemplos de su uso:

- **Conexión segura entre oficinas sucursales a través de Internet:** una compañía puede construir una red virtual privada y segura a través de Internet o de una WAN pública. Esto permite que una empresa se apoye fuertemente en Internet y reduzca su necesidad de redes privadas, disminuyendo gastos y coste en la gestión de red.
- **Acceso remoto seguro a través de Internet:** un usuario final cuyo sistema este dotado de protocolo de seguridad IP puede hacer una llamada local a su proveedor de servicios de Internet y acceder de forma segura a la red de una compañía. Estos reduce los gastos de los empleados que se tienen que desplazar y de los empleados a distancias.
- **Establecimiento de conexión extranet e intranet con socios***:* IPSec se puede usar para hacer que las comunicaciones con otras organizaciones sea seguras, garantizando la autenticación y la confidencialidad y proporcionando un mecanismo de intercambio de claves.
- **Mejora de la seguridad en el comercio electrónico:** aunque algunas aplicaciones web y de comercio electrónico tienen incorporado protocolos de seguridad, el uso de IPSec mejora la seguridad.

La característica principal de IPSec que permite dar soporte a esta variedad de aplicaciones es que puede cifrar y/o autentificar todo el tráfico en el nivel IP. Por lo tanto, pueden asegurarse todas las aplicaciones distribuidas, incluyendo conexión remota, cliente/servidor, correo electrónico, transferencia de ficheros, acceso a la web, etc.

La figura 5.1. Representa un uso común del uso de IPSec. Una organización tiene algunas LAN en lugares dispersos. En cada LAN hay trafico IP que no es seguro. Los protocolos IPSec se utilizan para el tráfico exterior, a través de una WAN privada o publico. Estos protocolos operan en dispositivos de red, como por ejemplo un router o un cortafuego, que conecta cada LAN al mundo exterior. El dispositivo de red IPSec cifrara y comprimirá todo el tráfico que entre en la WAN, descifrara y descomprimirá todo el tráfico que provenga de ella; estas operaciones son transparentes a las estaciones de trabajo y a los servidores en la LAN. También es posible la transmisión segura con usuarios individualmente que se conecta a la WAN. Dichas estaciones de trabajo de usuarios deben implementar los protocolos IPSec para proporcionar seguridad.

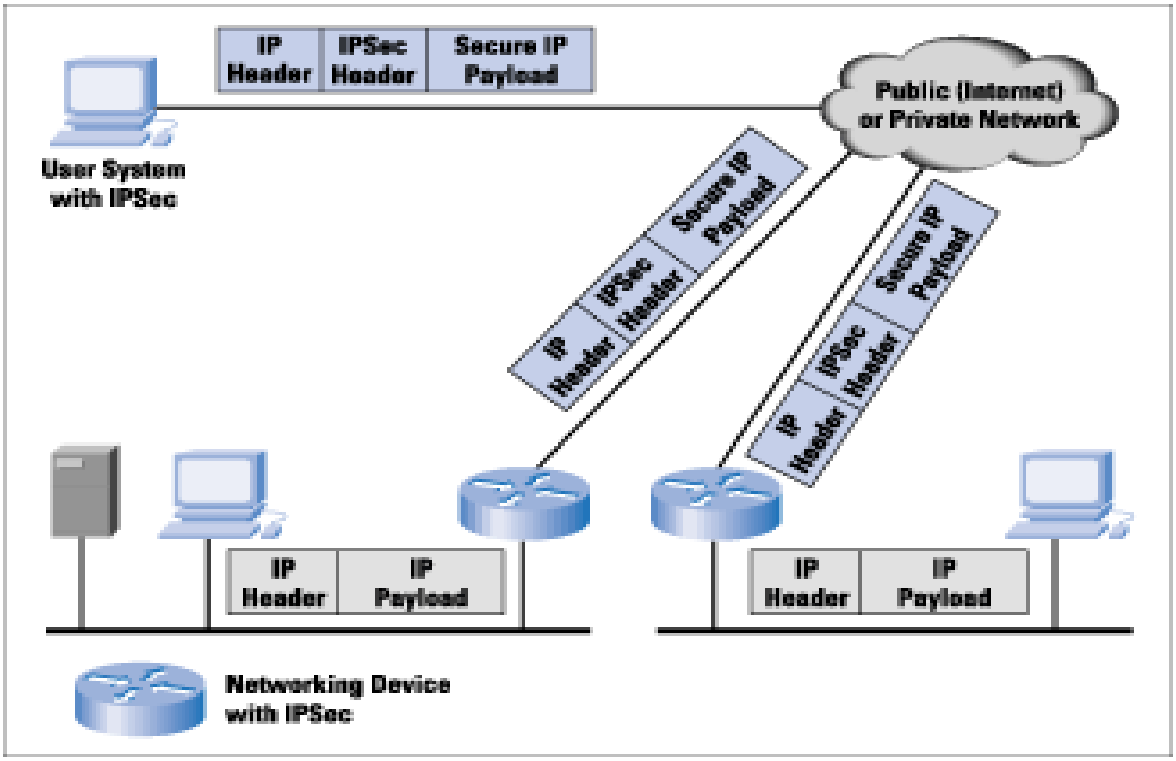


Figura 5.1. Entorno de Seguridad IP

5.1.2 Beneficios de IPSec

Se implementan los siguientes beneficios de IPSec:

- Cuando IPSec se implementa en un cortafuego o un router: proporciona una gran seguridad que se puede aplicar a todo el tráfico que lo cruza. El trafico en una compañía o grupo de trabajo no provoca costes adicionales de procesamiento relativo a la seguridad.

- IPSec es seguro en un cortafuego si se obliga a que todo el tráfico que proviene del exterior use IP, y el cortafuego es el único medio de entrada desde Internet a la organización.

- IPSec está por debajo de la capa de transporte (TCP, UDP) y, por ello, es transparente a las aplicaciones. No es necesario cambiar el software en el sistema de un usuario o de un servidor cuando IPSec se implementa en el cortafuego o el router. Incluso si IPSec se implementa en sistemas finales, el software de nivel superior, incluyendo aplicaciones, no se ve afectado.

- IPSec puede ser transparente a usuarios finales. No es necesario entrenar a los usuarios para la utilización de mecanismos de seguridad, ni suministrar material relativo al uso de claves para cada usuario, ni inhabilitar dicho material cuando los usuarios abandonan la organización.

- IPSec puede proporcionar seguridad a usuarios individuales si es necesario, lo cual es útil para trabajadores externos y para establecer una subred virtual segura en una organización para las aplicaciones confidenciales.

5.1.3 Aplicaciones de enrutamiento

Además de dar soporte a usuarios finales y proteger los sistemas y las redes de las instalaciones de la organización, IPSec puede desempeñar un papel fundamental en la arquitectura de enrutamiento necesaria para la comunicación de redes. IPSec puede garantizar que:

- Un anuncio de router (un nuevo router anuncia su presencia) procede de un router autorizado.
- Un anuncio de un router vecino (un router intenta establecer o mantener una relación con un router en otro dominio de enrutamiento) viene de un router autorizado.
- Un mensaje redirigido proviene del router al que se envió el paquete inicial.
- Una actualización de enrutamiento no se falsifica.

Sin estas medidas de seguridad, un oponente puede interrumpir las comunicaciones o desviar el tráfico. Los protocolos de enrutamiento como OSPF[33] deberían ejecutarse por encima de las asociaciones de seguridad entre routers que están definidos por IPSec.

5.2 Arquitectura de seguridad IP

La especificación IPSec se ha hecho muy compleja. Para entender la arquitectura general, en primer lugar, conviene observar los documentos que definen IPSec. Luego se trata los servicios de IPSec y se introducen el concepto de asociación de seguridad.

[33] **Open Shortest Path First (frecuentemente abreviado OSPF)** es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible.

5.2.1 Documentos de IPSec

La especificación de IPSec se compone de numerosos documentos. Los más importantes de ellos, publicados en Noviembre de 1998, son los RFC 2401, 2402, 2406 y 2408:

- RFC 2401: descripción general de una arquitectura de seguridad.
- RFC 2402: descripción de la extensión de autentificación de un paquete a IPv4 e IPv6.
- RFC 2406: descripción de la extensión de cifrado de un paquete a IPv4 e IPv6.
- RFC 2408: especificación de las capacidades de gestión de claves.

Permitir estas características es obligatorias para IPv6 y opcional para IPv4. En ambos casos, las características de seguridad se implementan como cabeceras de extensión que siguen a la cabecera IP principal.

La cabecera de extensión para la autentificación se conoce como cabecera de autentificación (AH. Authentication Header); y para el cifrado se conoce como cabecera de encapsulado de carga útil de seguridad (ESP. Encapsulating Security Payload Header).

Además de estos cuatros RFC, el grupo de trabajo (Security Protocol Working Group), creado por la IETF, ha publicado una serie de borradores adicionales.

Los documentos se dividen en siete grupos, como se muestra en la figura 5.2.

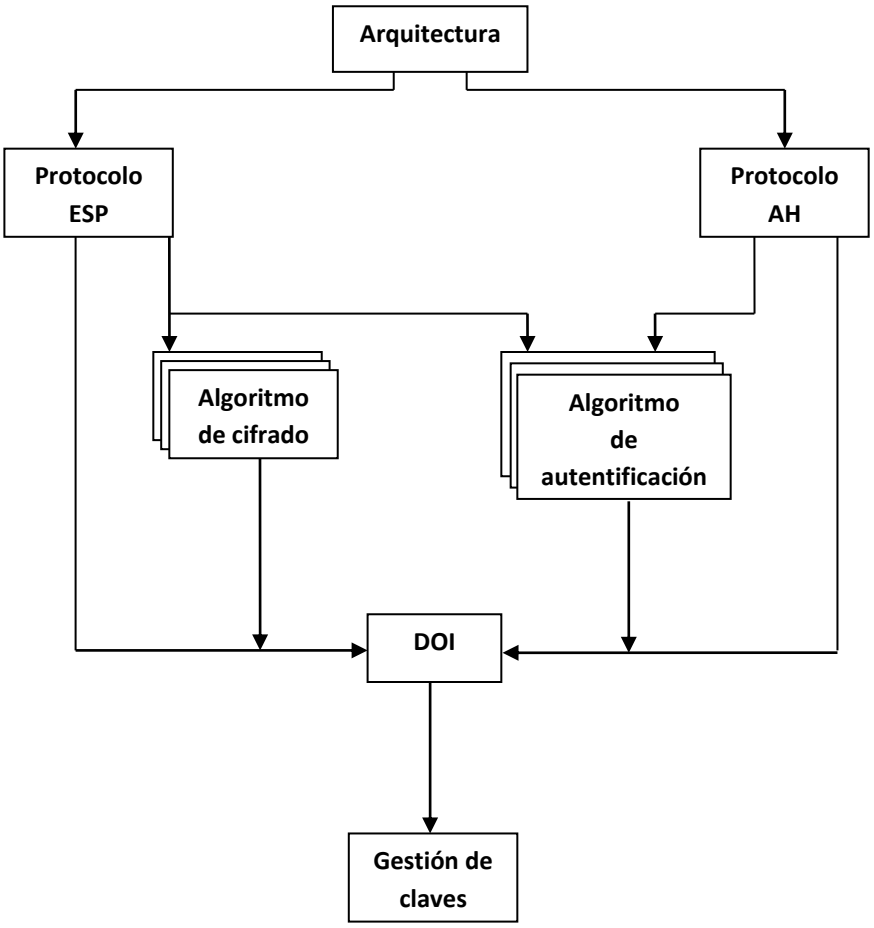


Figura 5.2: Esquema general de documento IPSec

- **Arquitectura***:* cubre los conceptos generales, los requisitos de seguridad, las definiciones y los mecanismos que definen la tecnología IPSec.

- **Encapsulado de carga útil de seguridad (ESP):** cubre el formato del paquete y los aspectos generales relacionados con el uso de ESP para el cifrado de paquetes y, de manera opcional, para las autentificación.

- **Cabecera de autentificación (AH):** cubre el formato del paquete y los aspectos relacionados con el uso de AH para la autentificación de paquetes.

- **Algoritmos de cifrado:** un conjunto de documentos que describen cómo se utilizan distintos algoritmos de cifrado para ESP.

- **Algoritmos de autentificación:** un conjunto de documentos que describen, cómo se utilizan distintos algoritmos de autentificación para AH y para la opción de autentificación de ESP.

- **Gestión de claves:** documentos que describen los esquemas de gestión de claves.

- **Dominio de interpretación (DOI: Domain of Interpretation):** contiene los valores necesarios para que los demás documentos se relacionen entre sí. Estos incluyen identificadores para algoritmos aprobados de cifrado y de autentificación así como parámetros operativos como el tiempo de vida de las claves.

5.2.2 Servicios IPSec

IPSec proporciona servicios de seguridad en la capa IP permitiendo que un sistema elija los protocolos de seguridad necesarios, determine los algoritmos que va a usar para el servicio o servicios y ubique las claves criptográficas necesarias para proporcionar los servicios solicitados.

Se usan dos protocolos para proporcionar seguridad: un protocolo de autentificación designado por la cabecera del protocolo, AH, y un protocolo

combinado de cifrado/autentificación designado por el formato del paquete para ese protocolo, ESP.

Los servicios son los siguientes:

- Control de acceso.
- Integridad sin conexión.
- Autentificación del origen de datos.
- Rechazo de paquetes reenviados.
- Confidencialidad (cifrado).
- Confidencialidad limitada del flujo de tráfico.

	AH	ESP(solo cifrado)	ESP (cifrado y autentificación)
Control de acceso	X	x	X
Integridad sin conexión	X		X
Autentificación del origen de datos	X		X
Rechazo de paquetes reenviados	x	X	X
Confidencialidad		X	X
Confidencialidad limitada del flujo de tráfico		X	x

Tabla 5.1: Servicios de IPSec

La tabla 5.1 muestra que servicios proporcionan los protocolos AH y ESP. Para ESP, existen dos casos: con y sin opción de autentificación.

Tanto AH como ESP son vehículos para el control de acceso, basado en la distribución de claves criptográficas y la gestión de flujos de tráfico referente a estos protocolos de seguridad.

5.2.3 Asociaciones de seguridad

Un concepto fundamental que aparece en los mecanismos de autentificación y confidencialidad en IP es el de Asociación de Seguridad (SA, Security Association).

Una asociación es una relación unidireccional entre un emisor y un receptor que ofrece servicios de seguridad al tráfico que se transporta. Si se necesita una relación que haga posible un intercambio bidireccional seguro, entonces se requiere dos asociaciones de seguridad. Los servicios de seguridad se suministran a una SA para que use AH o ESP, pero no los dos.

Una asociación de seguridad se identifica unívocamente por tres parámetros:

- **Índice de parámetros de seguridad (SPI, Security Parameters Index):** una ristra de bit asignada es esta SA y que tiene solo significado local. El SPI se transporta en cabecera AH y ESP para permitir que el sistema receptor elija la SA con la cual se procesara un paquete recibido.

- **Dirección IP de destino:** actualmente solo se permiten direcciones de un único destino (unicast); ésta es la dirección del destino final de la SA, que puede ser un sistema de un usuario final o un sistema de red, como por ejemplo un cortafuego o un router.

- **Identificador del protocolo de seguridad:** indica si la asociación es una asociación de seguridad AH o ESP.

Por consiguiente, en cualquier paquete IP, la asociación de seguridad se identifica unívocamente por la dirección de destino en la cabecera IPv4 o IPv6 y el SPI en la cabecera de extensión adjunta (AH o ESP).

5.2.3.1 Parámetros de SA

En cada implementación de IPSec hay una base de datos nominal de asociaciones de seguridad que define los parámetros asociados con cada SA. Una asociación de seguridad se define, normalmente por los siguientes parámetros:

- **Contador de número de secuencias:** un valor de 32 bit que se utiliza para generar el campo número de secuencia en la cabeceras AH o ESP.

- **Desbordamiento del contador de secuencias***:* un indicador que señala si el desbordamiento del contador de número de secuencia debería generar una acción de auditoría y evitar la transmisión de más paquetes en esta SA (se requiere para todas las implementaciones).

- **Ventana contra repeticiones:** se usa para determinar si un paquete AH o ESP que llega es una repetición.

- **Información AH***:* algoritmos de autentificación, claves, tiempos de vida de las claves y parámetros relacionados que se usan con AH.

- **Información ESP:** algoritmos de cifrado y autentificación, claves, valores de inicialización, tiempo de vidas de las claves y parámetros relacionados que se usan con ESP.

- **Tiempo de vida de la asociación de seguridad:** un intervalo de tiempo o contador de bytes después del cual una SA se debe reemplazar con una nueva SA (y un nuevo SPI) o se debe finalizar, junto con una indicación de cuáles de estas acciones deberían ocurrir.

- **Modo de protocolo IPSec:** túnel, transporte o modo comodín.

- **MTU (maximum transmission unit) del camino:** cualquier unidad de transferencia máxima que se observe en el camino (tamaño máximo de un paquete que se puede transmitir sin fragmentación) y variables de caducidad.

El mecanismo de gestión de claves que se emplean para que éstas se distribuyan está ligado a los mecanismos de autentificación y privacidad solo mediante el índice de parámetros de seguridad. Por ello, la autentificación y privacidad se han especificado independientemente de cualquier mecanismo específico de gestión de claves.

5.2.3.2 Selectores de SA

IPSec proporciona al usuario una gran flexibilidad en la forma en que los servicios de IPSec se aplican al tráfico IP. Como se verá más adelante, las SA se pueden combinar de distintas maneras para producir la configuración de usuario deseada. Además IPSec proporciona un alto grado de segmentación al discriminar entre trafico al que se aplica protección de IPSec y trafico que tiene permiso para evitar o pasar por alto a IPSec, refiriéndose al primer caso al tráfico de IP a SA especificas.

El medio por el que el trafico IP se relaciona con SA especificas (o a ninguna SA en el caso del trafico al que no se aplica IPSec) es **la base de datos de políticas de seguridad** (SPD, Security Policy Database). En su forma más simple, una SPD contiene entradas, cada una de las cuales define un subconjunto de trafico IP y señala una SA para ese tráfico. En entornos más complejos, puede haber múltiples entradas que se relacionan potencialmente con una sola SA o con varias SA asociadas con una única entrada a la SPD. Con el fin de tratar este aspecto más detalladamente, se hace referencia a la documentación relevante sobre IPSec.

Cada entrada de la SPD se define por un conjunto de valores de campos del protocolo IP y de protocolo de capas superiores, llamados selectores. En efecto, estos selectores se usan para filtrar tráfico saliente y establecer la correspondencia con una SA en particular.

El procesamiento de tráfico saliente obedece a la siguiente secuencia general para cada paquete IP:

1. Comparar los valores de los campos adecuados del paquete (los campos de selector) con la SPD para encontrar una entrada coincidente de la SPD, que señalara cero o más SA.
2. Determinar la SA, si la hubiese, para este paquete y su SPI asociado.
3. Llevar a cabo el procesamiento IPSec necesario (por ejemplo, procesamiento AH o ESP).

Los siguientes selectores determinan una entrada de la SPD:

- **Dirección IP de destino:** puede ser una única dirección IP, una lista o rango de direcciones o una dirección comodín (mascara). Las dos últimas son necesarias para permitir que más de un sistema de destino comparta la misma SA (por ejemplo, detrás de un cortafuego).

- **Dirección IP fuente:** puede ser una única dirección IP, una lista o rango de direcciones o una dirección comodín (mascara). Las dos últimas son necesarias para permitir que más de un sistema fuente comparta las misma SA (por ejemplo, detrás de un cortafuego).

- **ID de usuario:** un identificador de usuario obtenido del sistema operativo. No es un campo de las cabeceras IP ni de capas superiores, sino que está disponible si IPSec se ejecuta en el mismo sistema operativo que el usuario.

- **Nivel de confidencialidad de los datos:** se usan para los sistemas que proporcionan seguridad en el flujo de información (por ejemplo, secreta o no clasificada).

- **Protocolo de la capa de transporte:** se obtiene del protocolo IPv4 o del campo siguiente cabecera de IPv6. Puede ser un número de protocolo individual, una lista de número de protocolo o un rango de números de protocolos.

- **Protocolo IPSec (AH o ESP 0 AH/ESP):** si está presente, éste se obtiene del protocolo IPv4 o del campo siguiente cabecera de IPv6.

- **Puertos fuentes y destino:** pueden ser valores individuales de puertos TCP o UDP, una listas enumerada de puertos o puerto comodín.

- **Clase IPv6:** se obtiene de la cabecera de IPv6. Puede ser un valor específico de clase IPv6 o un valor comodín.

- **Etiqueta de flujo IPv6:** se obtiene de la cabecera IPv6. Puede ser un valor específico de la etiqueta de flujo IPv6 o un valor comodín.

- **Tipo de servicio IPv4 (TOS, Type of Service):** se obtiene de la cabecera IPv4. Puede ser un valor específico del tipo de servicio de IPv4 o un valor comodín.

5.2.4 Modo de transporte y túnel

Tanto AH como ESP permiten dos modos: modo transporte y modo túnel. La operación de estos dos modos se entiende más fácilmente a partir de la descripción de AH y ESP.

5.2.4.1 Modo transporte

El modo transporte proporciona protección principalmente a los protocolos de capas superiores. Es decir, la protección del modo transporte se extiende a la carga útil de un paquete IP.

Algunos ejemplos incluyen un segmento TCP o UDP o un paquete ICMP, que operan directamente encima de IP en la pila de protocolo de un host. Normalmente, el modo transporte se usa para la comunicación extremo a extremo entre host (por ejemplo, un cliente y un servidor o dos estaciones de trabajo). Cuando un host se ejecuta AH o ESP sobre IPv4, la carga útil consiste en los datos que habitualmente siguen a la cabecera IP. Para IPv6, la carga útil consiste en los datos que normalmente siguen a la cabecera IP y a cualquier cabecera de extensión de IPv6 que esté presente, con la posible excepción de la cabecera de opciones de destino, que se puede incluir en la protección.

ESP en modo transporte cifra y, de manara opcional, autentifica la carga útil de IP, pero no la cabecera IP. AH en modo transporte autentifica la carga útil de IP y partes seleccionadas de la cabecera IP.

5.2.4.2 Modo túnel

El modo túnel proporciona protección al paquete IP completo. Para conseguirlo, después de que se ha añadido los campos AH y ESP al paquete IP, el paquete completo mas los campos de seguridad se tratan como carga útil de un paquete IP “exterior” nuevo con una nueva cabecera IP exterior. El paquete original entero, o interior, viaja a través de un “túnel” desde un punto de la red IP a otro; ningún router a lo largo del camino puede examinar la cabecera IP exterior. Como el paquete original esta encapsulado, el nuevo paquete, que es mayor, puede tener direcciones de origen y destino totalmente diferente, lo cual añade seguridad.

El modo túnel se usa cuando uno o los dos extremos de una SA es una pasarela de seguridad, como podría ser un cortafuego o un router que implementa IPSec. Con el modo túnel, una serie de hosts en redes, detrás de cortafuegos pueden estar implicados en comunicaciones seguras sin implementar IPSec. Los paquetes no protegidos generados por dichos hosts se transmiten por un túnel a través de redes externas por medios de asociaciones de seguridad en modo túnel, establecidas por el software IPSec en el cortafuegos o el router seguro en los límites de la red local.

	SA en modo transporte	SA en modo túnel
AH	Autentifica la carga útil de IP y las partes seleccionadas de la cabecera de extensión de IPv6.	Autentifica todo el paquete IP interno (cabecera interior más carga útil de IP) más las partes seleccionadas de la cabecera IP exterior y la cabeceras externas de extensión de IPv6
ESP	Cifra la carga útil de IP y cualquier cabecera de extensión de IPv6 que siga a la cabecera ESP.	Cifra el paquete IP interior
ESP con autentificación	Cifra la carga útil de IP y cualquier cabecera de extensión de IPv6 que siga a la cabecera ESP. Autentifica la carga útil de IP, pero no la cabecera IP.	Cifra el paquete IP interior Autentifica el paquete IP interior.

Tabla 5.2 Funcionalidad del modo túnel y del modo transporte

ESP en modo túnel cifra y, de manera opcional, autentifica el paquete IP interior completo, incluyendo la cabecera IP interior. AH en modo túnel autentifica el paquete IP interior completo y las partes seleccionada de la cabecera IP exterior.

5.3 Cabecera de autenticación

La cabecera de autentificación proporciona soporte para la integridad de los datos y la autentificación de paquetes IP. La característica de integridad de los datos garantiza que no es posible que se produzca modificación no detectada en el contenido de un paquete durante la transmisión.

Las características de autentificación permiten que un sistema final o dispositivo de red autentifique al usuario o aplicación y filtre al tráfico adecuadamente; también evita los ataques de suplantación de dirección que observan hoy en día en Internet, además protege contra los ataque de repetición y se basa en el uso de un código de autentificación de mensaje (MAC, Massage Authentication Code).

La cabecera de autentificación se compone de los siguientes campos (figura 5.3):

- **Cabecera siguiente (ocho bits):** identifica el tipo de cabecera que esta inmediatamente después de esta.

- **Longitud de carga útil (ocho bit):** longitud de cabecera de autentificación en palabra de 32 bit, menos 2. Por ejemplo, la longitud predetermina del campo de datos de autentificación es de 96 bit, o tres palabras de 32 bit. Con una cabecera fija de tres palabras hay un total de seis palabras en la cabecera, y el campo longitud de carga útil tiene un valor de 4.

- **Reservado (16 bit):** para uso posteriores.

- **Índice de parámetros de seguridad (32 bit):** identifica una asociación de seguridad.

- **Número de secuencias (32 bit):** un valor de un contador que se incrementa mono tónicamente, que se trata más tarde.

- **Datos de autentificación (variable):** un campo de longitud variable (debe ser un numero entero de palabras de 32 bit), que contiene el valor de comprobación de integridad (ICV, Integrity Check Value), o el MAC para este paquete, que se discutirá más tarde.

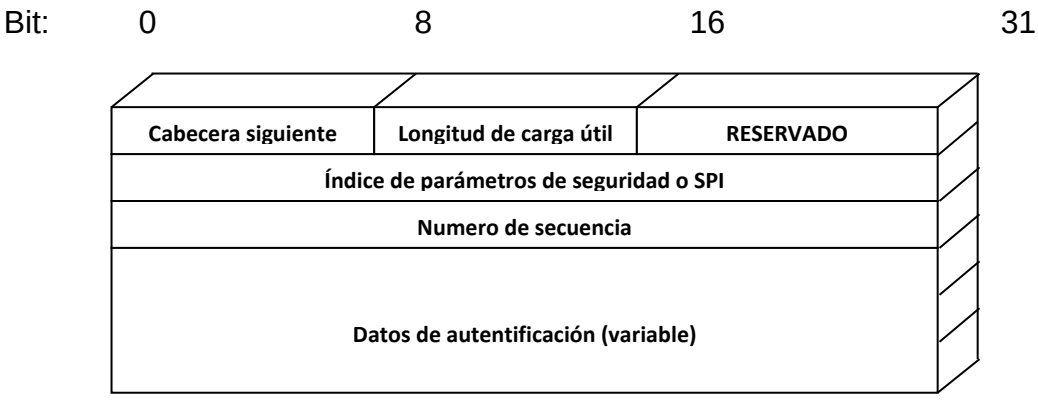


Figura 5.3 Cabecera de autentificación IPSec

5.3.1 Servicios contra repeticiones

Un ataque de repetición es aquel en que un atacante obtiene una copia de un paquete autentificado y lo transmite más tarde al destino previsto inicialmente.

El recibo de paquete IP autentificado duplicados puede interrumpir de algún modo un servicio o tener otras consecuencias negativas.

El campo numero de secuencia sirve para impedir tales ataques. En primer lugar, analizaremos la generación de números de secuencias por parte del emisor, y luego observaremos como se procesa el receptor.

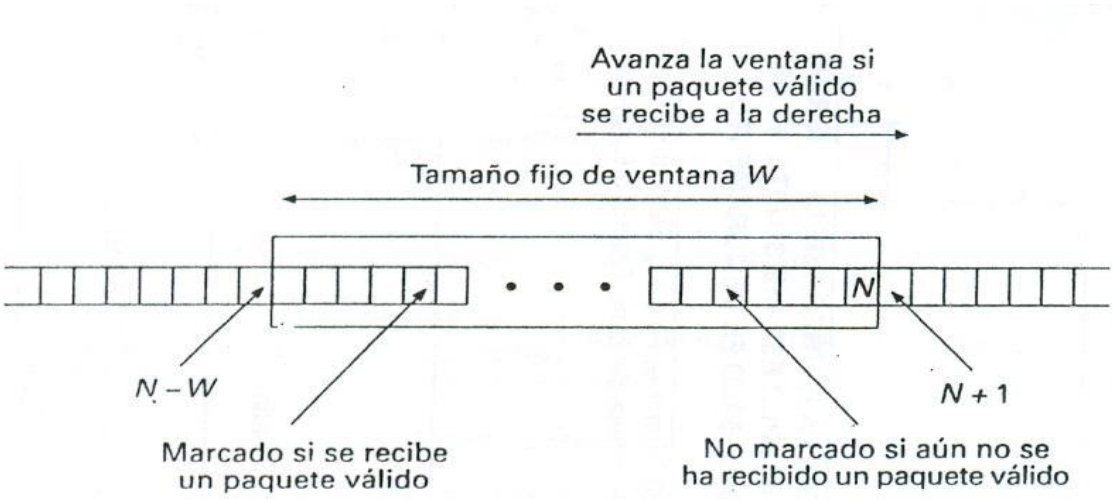
5.3.2 Valor de comprobación de integridad

El campo datos de autentificación contiene un valor conocido como **valor de comprobación de la integridad** *o*, como ya se ha indicado, ICV. EL ICV es un código de autentificación de mensajes o una versión truncada de un código producido por un algoritmo MAC.

La especificación actual dicta que una implementación adecuada debe permitir:

- HMAC-MD5-96
- HMAC-SHA-1-96

Los dos usan el algoritmo HMAC, el primero de ellos con el código hash MD5 y el segundo con el código hash SHA – 1. En ambos casos, el valor HMAC total se calcula, pero luego se trunca usando los primeros 96 bit, que es la longitud



predeterminada para el campo datos de autentificación.

Figura 5.4 Mecanismo contra repeticiones

El MAC se calcula sobre:

- Los campos de cabeceras IP que no cambian durante la transfusión (invariables) o que son predecibles en valor en la llegada en el punto final para la SA de AH. Los campos que pueden cambiar durante la transmisión y cuyo valor a la llagada es impredecible se fijan a cero para el cálculo tanto en el origen como en el destino.
- La cabecera AH, a excepción del campo dato de autentificación. Este campo se fija a cero para el cálculo tanto en el origen como en el destino.
- Los datos completos de los protocolos de nivel superior, que se suponen invariable durante la transmisión (por ejemplo, un segmento TCP o un paquete IP interior en modo túnel).

Para IPv4, los ejemplos de campos variables son la longitud de cabeceras de Internet y la dirección del origen. Un ejemplo de un campo variable pero predecible es la dirección de destino (con enrutado de origen flexible o estricto).

Ejemplos de campos variables que se fijan a cero antes del cálculo del ICV son los campos tiempo de vida y checksum de cabecera. Obsérvese que los campos de dirección de origen y destino están protegidos para prevenir la suplantación de dirección.

Para IPv6, los ejemplos en la cabecera base son versión (invariable), dirección de destino (variable pero predecible) y etiquetas de flujo (variable y fijada a cero para el cálculo).

5.3.3 Modos transporte y túnel

La figura 5.5 muestra las dos formas en que se puede usar el servicio de autentificación IPSec. En un caso, se proporciona autentificación directamente entre el servidor y las estaciones de trabajo clientes; la estación de trabajo puede estar en la misma red que el servidor o en una red exterior.

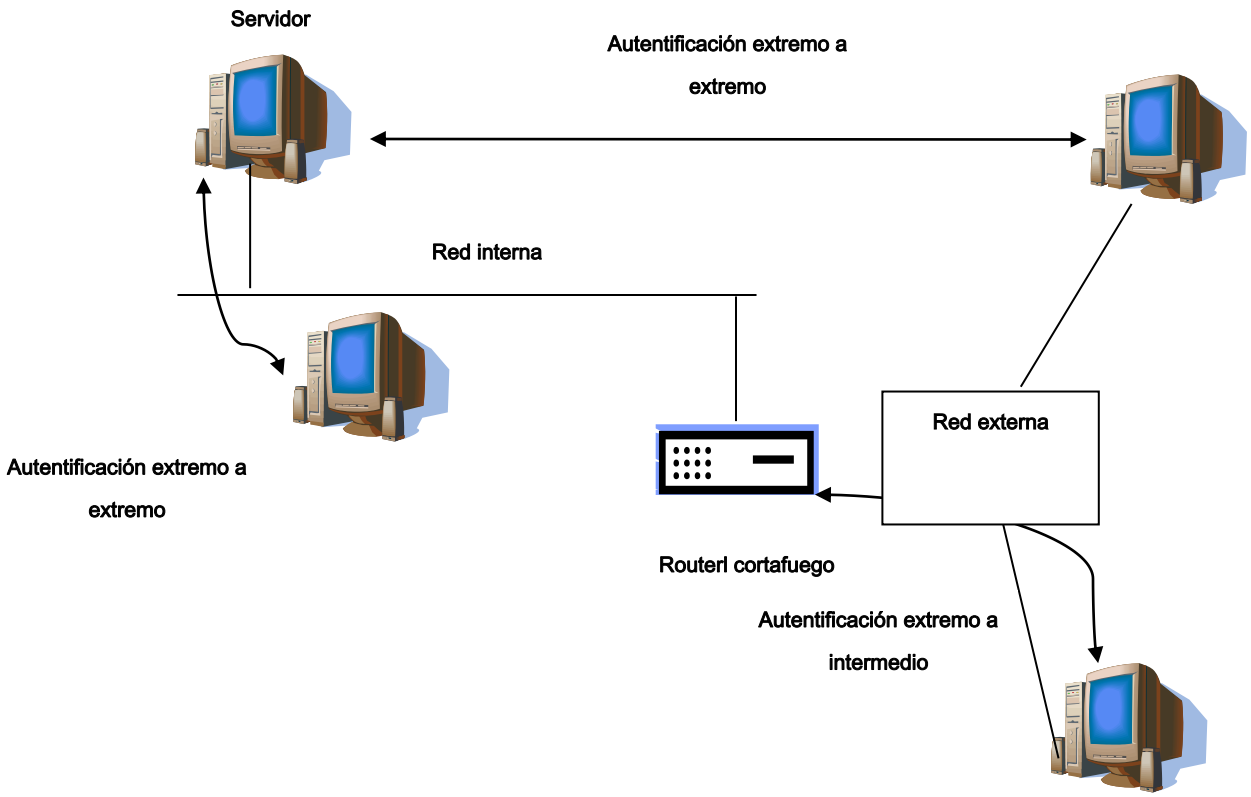


Figura 5.5 Autentificación extremo a extremo frente a extremo a intermediario

Mientras la estación de trabajo y el servidor compartan una clave secreta protegida, el proceso de autentificación es seguro. Este caso utiliza una SA en modo transporte. En el otro caso, una estación de trabajo remota se autentifica a si misma ante el cortafuego colectivo, ya sea para el acceso a toda la red interna o porque el servidor solicitado no permite la características de autentificación. Este caso utiliza una SA en modo túnel.

Si se observa el ámbito de autentificación que proporciona AH y la localización de la cabecera de autentificación para los dos modos, las consideraciones son, en cierto modo, diferentes para IPv4 e IPv6. La figura 5.6a muestra paquete típicos IPv4 e IPv6. En este caso la carga útil IP es un segmento

TCP; también podría ser una unidad de datos para cualquier otro protocolo que use IP, como UDP o ICMP.

Para AH en modo transporte usando IPv4, la AH se inserta después de la cabecera IP original y ante de la carga útil de IP (por ejemplo, un segmento TPC); esto se ilustra en la parte superior de la figura 5.6b. La autentificación cubre el paquete completo, excluyendo campos variables de la cabecera IPv4 que estén fijados a cero para el cálculo de MAC.

En el contexto de IPv6, AH se considera una carga útil de extremo a extremo; es decir, no la examinan ni la procesan routers intermedios. Por lo tanto, la AH aparece después de la cabecera base IPv6 y la cabecera de extensión salto en salto (hop by hop), enrutamiento y fragmento.

Las cabeceras de extensión de opciones de destino podrían aparecer antes o después de la cabecera AH, dependiendo de la semántica deseada. Nuevamente, la autentificación cubre el paquete completo, excluyendo campos variables que se fijan a cero para el cálculo del MAC.

Para AH en modo túnel, se autentifica el paquete IP original completo y la AH se inserta entre la cabecera IP original y la nueva cabecera IP externa (figura 5.6c). La cabecera IP interna contiene las direcciones finales de origen y destino, mientras que una cabecera IP externa puede contener diferentes direcciones IP (por ejemplo, direcciones de cortafuegos u otras pasarelas de seguridad).

Con el modo túnel, AH protege el paquete completo, incluyendo la cabecera IP interior completa. La cabecera IP exterior para el caso de IPv6, las cabeceras de extensión IP externa), se protege a excepción campos variable impredecibles.

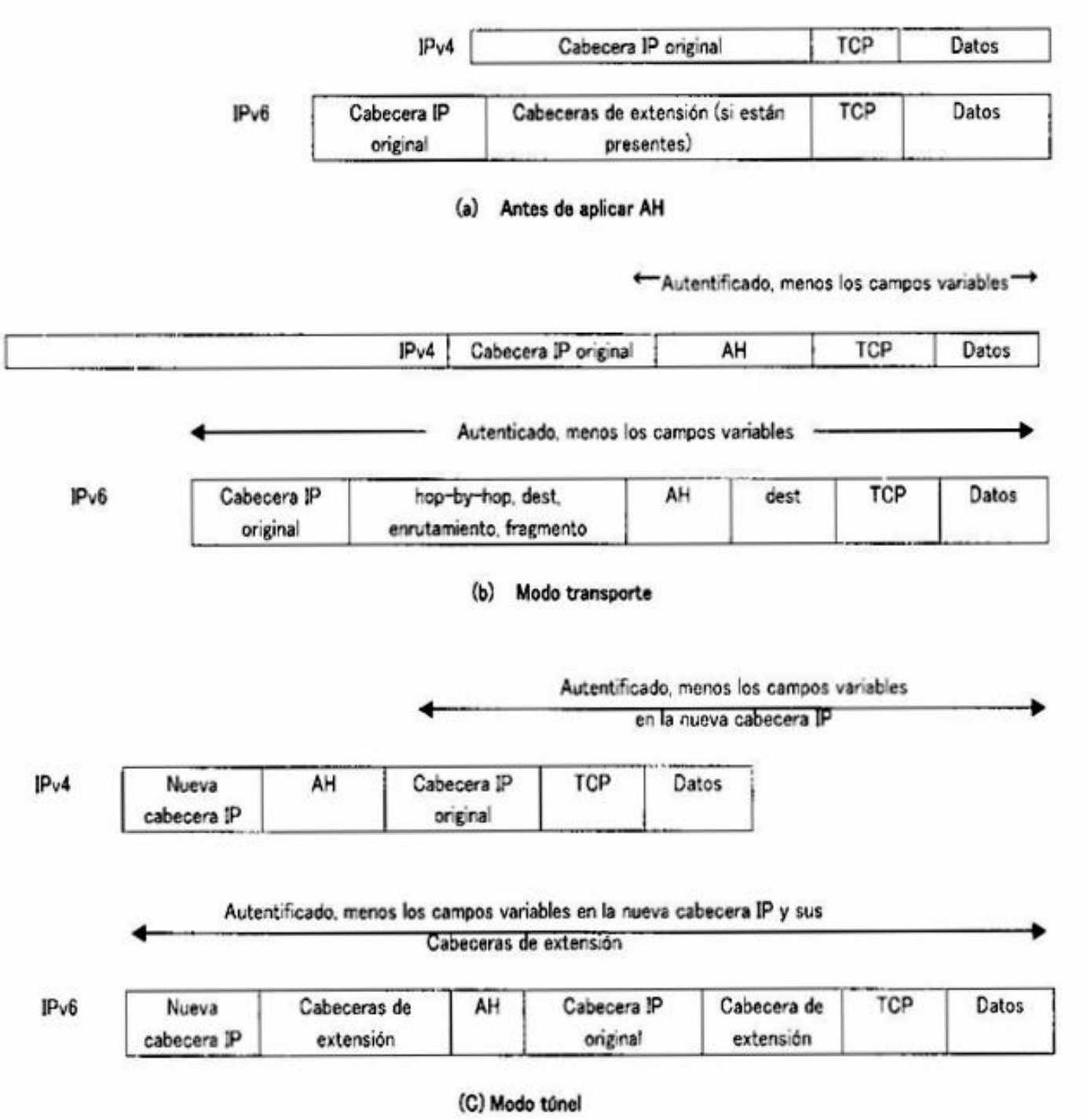


Figura 5.6 Ámbito de autentificación AH

5.4 Encapsulamiento de la carga útil de seguridad

El encapsulamiento de la carga útil de seguridad proporciona servicios de confidencialidad, incluyendo confidencialidad del contenido de los mensajes y confidencialidad limitada del flujo de tráfico. Como característica opcional, ESP también puede ofrecer los mismos servicios de autentificación que AH.

5.4.1 El formato ESP

El formato de un paquete ESP. Contiene los siguientes campos:

- **Índice de parámetros de seguridad (32 bits):** identifica una asociación de seguridad.
- **Numero de secuencias (32 bits):** el valor de un contador que se incrementa monótonamente; proporciona la función anti repetición, como se explicó para AH.
- **Datos de carga útil (variable):** es un segmento de la capa de transporte (modo de transporte) o un paquete IP (modo túnel) protegido mediante cifrado.
- **Relleno (0-255 bytes):** la finalidad de este campo se trata más tarde.
- **Longitud de relleno (ocho bits):** indica números de bytes de relleno en el campo inmediatamente anterior.
- **Cabecera siguiente (ocho bits):** identifica el tipo de datos que contiene el campo de datos de carga útil identificando la primera cabecera en esa carga útil (por ejemplo, una cabecera de extensión en IPv6 o un protocolo de la capa superior como TCP).
- **Datos de autentificación (variables):** un campo de longitud variable (debe ser un numero entero de palabra de 32 bits) que contiene el valor de comprobación de integridad calculado sobre el paquete ESP menos el campo de datos de autentificación.

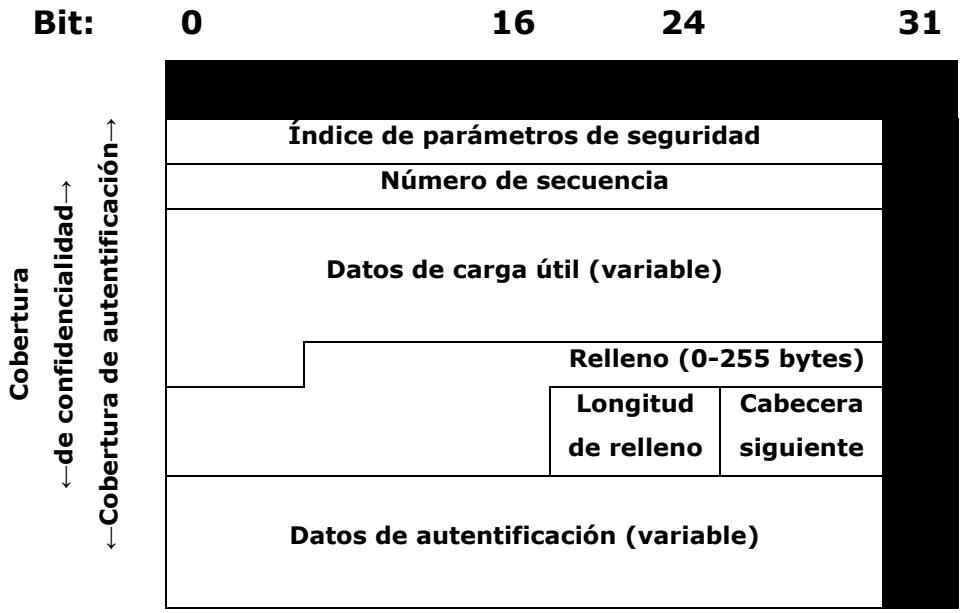


Figura 5.7 formato ESP de IPSec

5.4.2 Algoritmos de cifrado y autentificación

Los campos datos de carga útil, relleno, longitud de relleno y cabecera siguiente se cifran mediante el servicio ESP.

Si el algoritmo utilizado para cifrar la carga útil requiere datos de sincronización criptográfica, como puede ser un servidor de sincronización (IV. Initialization Vector), entonces estos datos pueden aparecer explícitamente el principio del campo datos de carga útil. Si se incluye, un IV no se cifra normalmente, aunque con frecuencia se considera que es parte del texto cifrado.

La especificación actual dicta que una implementación adecuada debe permitir DES en modo CBC. A otros algoritmos se les ha asignado identificadores en el documento DOI y podrían, por los tanto, usarse fácilmente para el cifrado.

Estos incluyen:

- Triple DES de tres claves
- RC5
- IDEA
- Triple IDEA de tres claves
- CAST
- Blowfish

Como con AH, ESP permite el uso de un MAC con una longitud predeterminada de 96 bits. También como con AH, la especificación dicta que una implementación adecuada debe permitir HMAC-MD5-96 y HMAC-SHA-1-96.

5.4.3 Relleno

El campo de relleno sirve para los siguientes propósitos:

- Si un algoritmo de cifrado requiere que el texto claro sea un múltiplo de un numero d bytes (por ejemplo, el múltiplo de un solo bloque para un cifrador de bloque), el campo de relleno se usa para expandir el texto claro (que consiste en los campos datos de carga útil, relleno, longitud de relleno y cabecera siguiente para alcanzar la longitud necesaria.

- El formato ESP requiere que los campos longitud de relleno y cabecera siguiente estén correctamente alineados en una palabra de 32 bits. El campo relleno se usa para garantizar esta alineación.

- Se puede añadir relleno adicional para proporcionar confidencialidad parcial de flujo de tráfico, disimulando lo longitud real de la carga útil.

5.4.4 Modo transporte y túnel

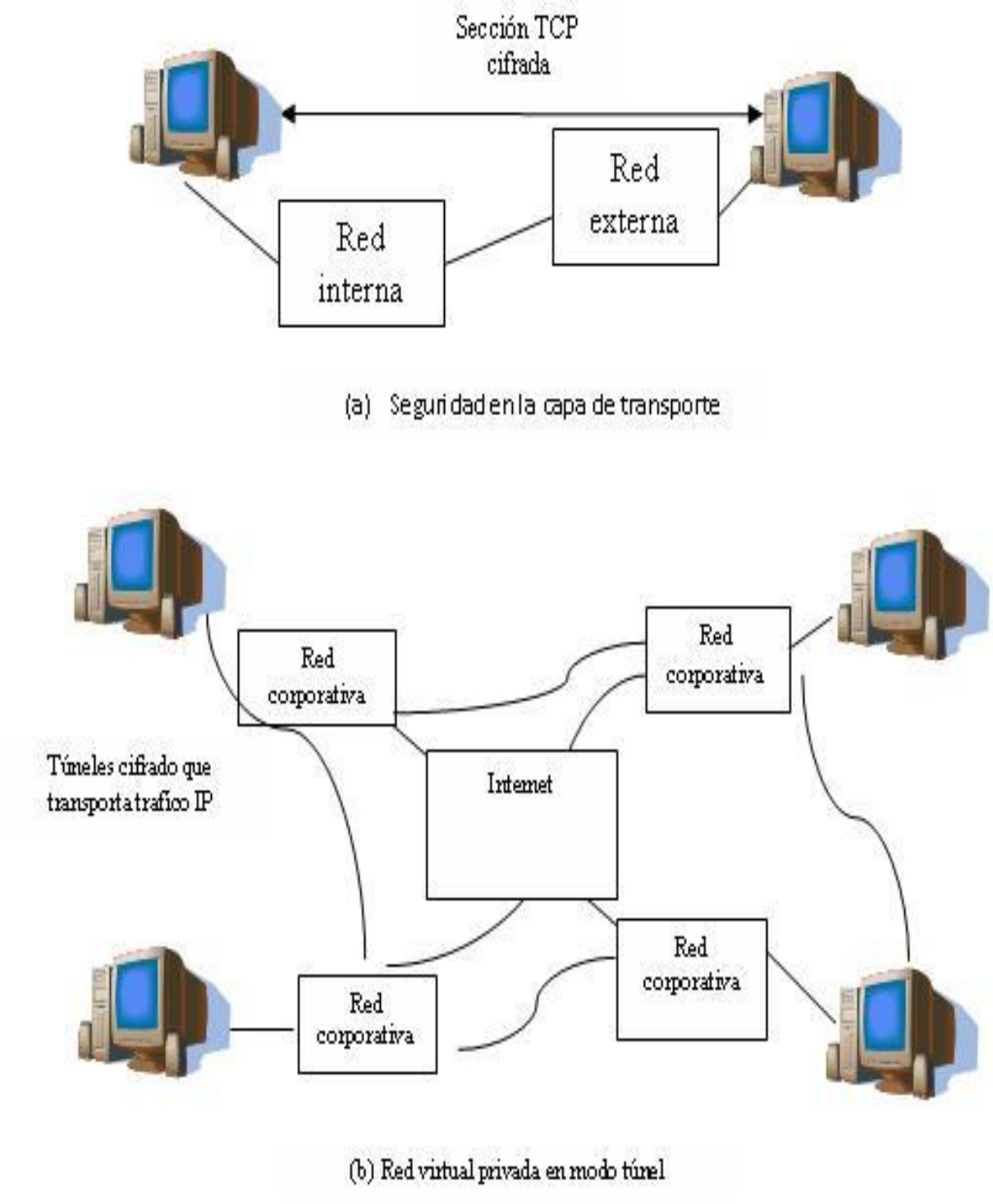


FIGURA 5.8. Cifrado en modo transporte frente a cifrado en modo túnel

La figura 5.8 muestra dos formas de utilización del servicio ESP de IPSec. En la parte superior de la figura, el cifrado (y de manera opcional, la autentificación) se proporciona directamente entre dos host.

En este ejemplo una organización tiene cuatro redes privadas conectadas entre sí a Internet. Los host de las redes internas usan Internet para el transporte de datos pero no interactúan con otros hosts basados en Internet.

Finalizados los túneles en la pasarela de seguridad para cada red interna, la configuración permite que los hosts eviten la implementación de la capacidad de seguridad.

La primera técnica usa una SA en modo transporte, mientras que la segunda se vale de una SA en modo túnel.

5.4.4.1 ESP en modo de transporte

ESP en modo de transporte se usa para cifrar y, de manera opcional, para autentificar los datos transportados por IP (por ejemplo, un segmento TCP).

Para este modo, usando IPv4, la cabecera ESP se inserta en el paquete IP inmediatamente antes de la cabecera de la capa de transporte (por ejemplo, TCP, UDP, ICMP) y después del paquete IP se coloca una terminación ESP (los campos relleno, longitud de relleno y cabecera siguiente); si se elige autentificación se añade el campo datos de autentificación ESP después de la terminación ESP.

La autentificación cubre todo el texto cifrado más la cabecera ESP.

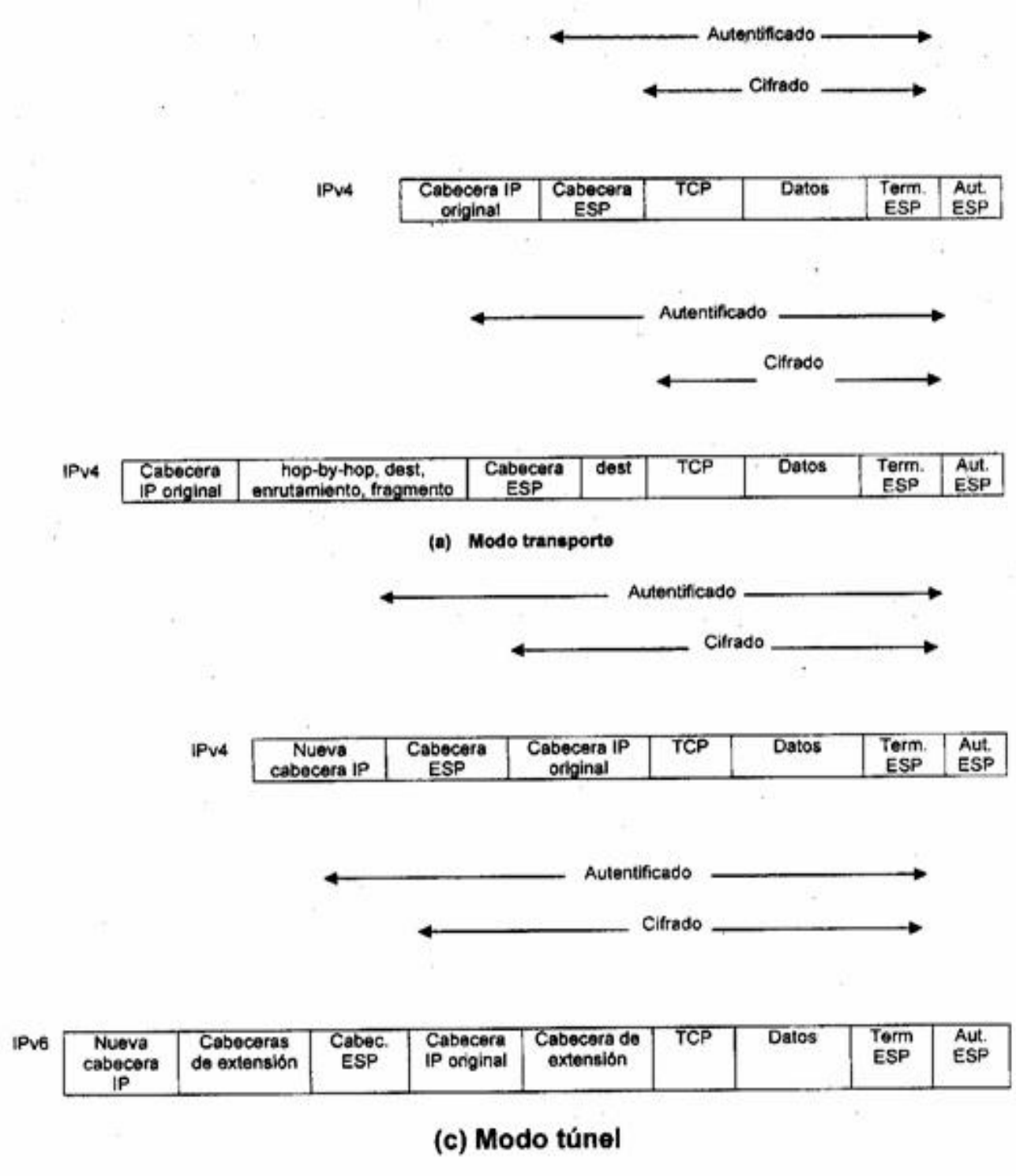


Figura 5.9 Ámbito de cifrado y autentificación de ESP

En el contexto de IPv6, ESP se considera una carga útil de extremo a extremo; es decir, no se examina ni se procesa por routers intermedios. Por lo tanto, la cabecera ESP aparece después de la cabecera base IPv6 y las cabeceras de extensión hop-by-hop, enrutamiento y fragmento.

La cabecera de extensión de opciones de destino podría aparecer ante o después de la cabecera ESP, dependiendo de la semántica deseada.

Para IPv6, el cifrado cubre el segmento completo del nivel de transporte más la terminación ESP más la cabecera de extensión de opciones de destino si ocurre después de la cabecera ESP. Nuevamente, la autentificación cubre el texto cifrado y la cabecera ESP.

La operación del modo transporte se puede resumir de la siguiente manera:

1. En el origen, el bloque de dato formado por la terminación ESP y el segmento completo de la capa de transporte se cifra y el texto claro de este bloque se sustituye por su texto cifrado para formar el paquete IP para la transmisión. La autentificación se añade si se elige esta opción.

2. Luego, el paquete se encamina al destino. Cada routers intermedio necesita examinar y procesar la cabecera IP y cualquier cabecera de extensión IP de texto claro, pero no necesita examinar el texto cifrado.

3. En nodo de destino examinar y procesa la cabecera IP mas cualquier cabecera de extensión IP de texto claro. Luego, basándonos en el SPI en la cabecera ESP, el nodo de destino descifra el resto del paquete para recuperar el segmento de texto clara de la capa de transporte.

La operación del modo de transporte proporciona confidencialidad para cualquier aplicación que lo use, evitando, de esta forma la necesidad de implementar confidencialidad en cada aplicación individualidad.

Este modo de operación también es razonablemente eficaz, añadiendo una parte pequeña a la longitud total del paquete IP.

Una desventaja de este modo no es posible analizar el tráfico en los paquetes transmitidos.

5.4.4.2 ESP en modo túnel

ESP en modo túnel se utiliza para cifrar un paquete IP entero (figura 5.9b). Para este modo la cabecera ESP se antepone al paquete y luego se cifra el paquete y la terminación ESP. Este método se puede usar para contrarrestar el análisis del tráfico.

Como la cabecera IP contiene la dirección de destino y, posiblemente, información sobre la directiva de enrutamiento de origen y la opción salto en salto, no es posible simplemente transmitir el paquete IP cifrado precedido de la cabecera ESP.

Los routers intermedios no podrían procesar un paquete así. Por consiguiente es necesario encapsular el bloque completo (cabecera SP mas texto cifrado más datos de autentificación, en caso de estar presente) con una nueva cabecera de dirección IP que contenga suficiente información también para el enrutamiento pero no para el análisis de tráfico.

Mientras el modo transporte es adecuado para proteger conexiones entre hosts que permite la características ESP, el modo túnel es útil un una configuración que incluye cortafuego u otro tipo de pasarela de seguridad que protege una red fiable frente a redes externas.

En este último caso el cifrado se produce entre un host externo y la pasarela de seguridad o entre dos pasarelas de seguridad. Este libera a los hosts de la red interna de la carga de procesamiento del cifrado y simplifica la distribución de claves deduciendo el número de clave necesaria. Además, dificulta el análisis del tráfico basado en el destino final.

Consideremos el caso en el que un host externo desea comunicarse con un hosts en una red interna protegida por un cortafuego, y en el que ESP se implementa en el host externos y los cortafuegos.

Para la transferencia de un segmento de la capa de transporte de host externo al interno se lleva a cabo los siguientes pasos:

1. El origen prepara un paquete IP interno con una dirección de destino de host interno de destino. Este paquete esta precedido de una cabecera ESP; luego, el paquete y la terminación ESP se cifra y se puede añadir los datos de autentificación. El bloque resultante se encapsula con una nueva cabecera IP (cabecera base mas extensiones opcionales como las opciones del enrutamiento y salto en salto para IPv6) cuya dirección de destino es el cortafuego; esto conforma el paquete externo IP.
2. El paquete externo se encamina al cortafuego destino. Cada routers intermedio necesita examinar y procesar la cabecera IP externa más cualquier cabecera externa de extensión IP. Pero no necesita examinar el texto cifrado.
3. El cortafuego destino examina y procesa la cabecera IP externa y cualquier cabecera de extensión IP externa. Luego, basándose en el SPI de la cabecera ESP, el nodo de destino descifra el resto del paquete para recuperar el paquete IP interior en texto claro.
   Este paquete, se transmite a la red interna.
4. El paquete interno se encamina a través de cero o más routers en la red interna hacia el host de destino.

5.5 Combinación de asociaciones de seguridad

Una SA individual puede implementar el protocolo AH o el ESP pero no los dos. A veces, un flujo de tráfico particular pedirá los servicios proporcionados por AH y ESP. Además, un flujo de tráfico particular puede requerir servicios IPSec

entre hosts y, para ese mismo flujo, servicios separados entre pasarelas de seguridad, como, por ejemplo, cortafuegos.

En todos estos casos, se deben emplear varias SA para el mismo flujo de tráfico con el objetivo de conseguir los servicios IPSec deseados.

El termino **grupo de asociaciones de seguridad** se refiere a una secuencia de asociaciones de seguridad a través de las cuales se debe procesar el trafico para proporcionar un conjunto de servicios IPSec. Las SA en un grupo pueden finalizar en distintos extremos o los mismos.

Las asociaciones de seguridad se pueden combinar de dos formas:

- **Transporte adyacente:** se refiere a la aplicación de más de un protocolo de seguridad al mismo paquete IP, sin invocar al modo túnel. Este enfoque para la combinación de AH y ESP permite un solo nivel de combinación; un mayor grado de anidamiento no produce beneficios adicionales ya que el procedimiento se realiza en una instancia IPSec: el destino (final).

- **Anidamiento de túneles:** se refiere a la aplicación de varias capas de protocolos de seguridad mediante modo túnel IP.
  Este enfoque permite múltiples niveles de anidamiento, ya que cada túnel puede originarse o terminar en un sitio IPSec diferente a lo largo del recorrido.

Los dos enfoques se pueden combinar, por ejemplo, haciendo que una SA de transporte entre hosts viaje parte del camino a través de una SA túnel entre pasarelas de seguridad. Un aspecto interesante que surge al considerar los grupos de SA es el orden en el que se puede aplicar la autentificación y el cifrando entre un par dado de extremo finales y las formas de hacerlo.

5.5.1 Autentificación más confidencialidad

El cifrado y la autentificación se pueden combinar para transmitir un paquete IP con confidencialidad y autentificación entre hosts. Analizaremos varios enfoques.

5.5.1.1 Opción ESP con autentificación

Existen dos casos:

- **ESP en modo transporte:** la autentificación y el cifrado se aplican a la carga útil[34] de IP enviada al host, pero la cabecera IP no está protegida.

- **ESP en modo túnel:** la autentificación se aplica al paquete IP completo enviado a la dirección IP externa de destino (por ejemplo, un cortafuego), y la autentificación se realiza en ese destino.
  El paquete IP interno completo está protegido por un mecanismo de privacidad, para su envío al destino IP interno. Para los dos casos, la autentificación se aplica al texto cifrado, en vez de al texto claro.

5.5.1.2 Transporte adyacente

Otra forma de aplicar autentificación después del cifrado es usar dos SA de transportes agrupados, donde la interna es una SA de ESP y la externa una SA de AH. En este caso, ESP se usa sin su opción de autentificación.

Debido a que la SA interna es una SA de trasporte, el cifrado se aplica a la carga útil IP. El paquete resultante está formado por una cabecera IP (y posiblemente extensiones de cabecera IPv6) seguido de un ESP. Luego, se aplica a AH en modo transporte, para que la autentificación cubra el ESP más la cabecera IP original (y extensiones) excepto los campos variables.

[34] C**arga útil** es el conjunto de datos, como los campos de datos de un formulario web, que representa la información del usuario e información de usuario, y no la información de sistema.

La ventaja de este enfoque con respecto a usar simplemente una sola SA de ESP con la opción de autentificación ESP reside en que la autentificación abarca más campos, incluyendo las direcciones IP de origen y de destino. La desventaja se halla en el uso de dos SA en vez de una.

5.5.1.3 Grupo túnel/transporte

El uso de autentificación ante del cifrado podría ser preferible por varios motivos.

En primer lugar, como los datos de autentificación están protegidos mediante cifrado, es imposible que nadie intercepte el mansaje y altere los datos de autentificación sin ser detectado.

Segundo se puede desear almacenar información de autentificación con el mensaje en el destino para una referencia posterior. Es más conveniente hacer esto si la información de autentificación se aplica al mensaje sin cifrar; de otro modo, el mensaje tendría que volver a cifrarse para verificar la información de autentificación.

Un enfoque para la aplicación de autentificación antes del cifrado entre dos host es usar un grupo formado por una SA de transporte AH interna y una SA túnel ESP externa. En este caso, la autentificación se aplica a la carga útil IP mas la cabecera IP (y extensiones) a excepción de los campos variables. El paquete IP resultante luego se procesa de modo túnel por ESP; el resultado es que todo el paquete interno autentificado se cifra y se añade una nueva cabecera IP externa (y extensiones).

5.5.2 Combinaciones básicas de asociaciones de seguridad

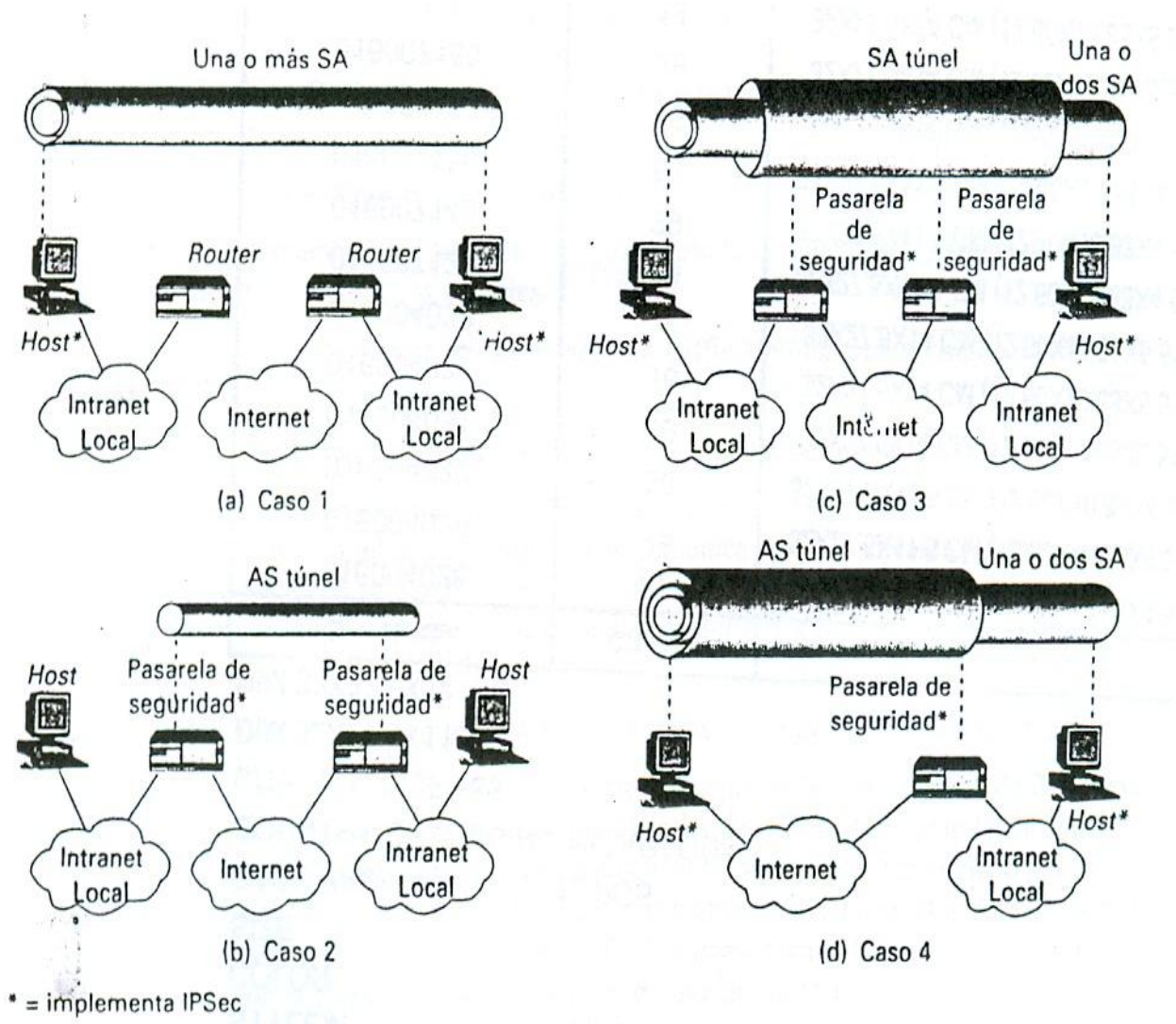


Figura 5.10 Combinación básica de asociaciones de seguridad

El documento de arquitectura IPSec presenta cuatro ejemplos de combinaciones de SA que deben ser soportadas por hosts IPSec adecuados (por ejemplo, estación de trabajo, servidor) o pasarela de seguridad (por ejemplo, cortafuegos, routers). Cada SA puede ser tanto AH o ESP. Para asociaciones de

seguridad host a host, el modo puede ser transporto o túnel; si no, debe ser modo túnel.

En el caso 1, toda la seguridad se proporciona entre sistemas finales que implementa IPSec. Para que los dos sistemas finales se comuniquen mediante una SA, deben compartir las claves secretas apropiadas.

Las siguientes son algunas de las posibles combinaciones:

a. AH en modo transporte.
b. ESP en modo túnel
c. AH seguida de ESP en modo transporte (una SA ESP dentro de una SA AH)
d. Cualquiera de a, b o c dentro de una AH o ESP en modo túnel.

Para el caso 2, la seguridad se proporciona solo entre pasarela (routers, cortafuegos, etc.) y ningún host implementa IPSec. Este ilustra el modo túnel en una red virtual privada. El documento de la arquitectura de seguridad especifica que solo se necesita una SA túnel para este caso.

El túnel podría permitir AH, ESP o ESP con la opción de autentificación. No se requieren túneles anidados porque los servicios IPSec se aplican al paquete interno completo.

El caso 3 se construye sobre el caso 2 añadiendo seguridad de extremo a extremo. Se permite las mismas combinaciones discutidas para los casos 1 y 2. El túnel de pasarela a pasarela proporciona autentificación o confidencialidad del tráfico entre sistemas finales.

Cuando el túnel de pasarela a pasarela es ESP, también proporciona una forma limitada de confidencialidad del tráfico. Los host individuales pueden implementar cualquier servicio IPSec adicional requerido para ciertas aplicaciones

o para ciertos usuarios por medio de asociaciones de seguridad de extremo a extremo.

El caso 4 proporciona soporte para un host remoto que usa internet para llegar al cortafuego de una organización y luego acceder a algún servidor o estación de trabajo detrás del cortafuego. Solo se requiere el modo túnel entre host remoto y el cortafuego. Como en el caso 1, se pueden usar una o dos SA entre el host remoto y el host local.

5.6 Gestión de claves

La parte de gestión de claves de IPSec implica la determinación y distribución de claves secretas. Un requisito habitual es el de cuatro claves para la comunicación entre dos aplicaciones: parejas de transición y recepción tanto para AH como para ESP.

El documento de la arquitectura de IPSec asigna soporte para dos tipos de gestión de claves:

- **Manual:** un administrador de sistema configura manualmente cada sistema con sus propias claves y con las claves de otros sistemas que se comunican. Esto es práctico para entornos pequeños relativamente estáticos.

- **Automática:** un sistema automático permite la creación bajo demanda de claves para asociaciones de seguridad y facilita el uso de claves en un sistema distribuido grande con una configuración cambiante.

El protocolo de gestión de claves automático predeterminado para IPSec se conoce como ISAKMP/Oakley y se compone de los siguientes elementos:

- **Protocolo de determinación de claves Oakley:** Oakley es un protocolo de intercambio de claves que se basa en el algoritmo Diffie-Hellman[35] pero que proporciona seguridad adicional. Oakley es genérico en el sentido de que no dicta formatos específicos.

- **Asociación de seguridad y Protocolo de gestión de claves (ISAKMP, Internet Security Association and Key Management Protocol):** ISAKMP proporciona un marco de trabajo para la gestión de claves en Internet y el soporte del protocolo específico, incluyendo formatos, para la negociación de los atributos de seguridad.

ISAKMP por sí mismo no impone un algoritmo específico de intercambio de claves, consiste en un conjunto de tipos de mensaje que permiten el uso de una variedad de algoritmos de intercambio de claves. Oakley es el algoritmo específico de intercambio de claves de uso obligado con la versión inicial de ISAKMP.

5.6.1 Protocolo de determinación de claves Oakley

Oakley es una mejora del algoritmo de intercambio de claves Diffie-Hellman.

Recordemos que Diffie-Hellman implica la siguiente iteración entre los usuarios A y B. Hay un acuerdo previo sobre dos parámetros globales: q, un número primo grande; y α, una raíz primitiva de q. A elige un entero aleatorio X_A como su clave privada, y transmite a B su clave publica $Y_A = \alpha^{X_A} \bmod q$. De la misma forma, B elige un entero aleatorio X_B como su clave privada, y transmite a A su clave publica $Y_B = \alpha^{X_B} \bmod q$. Ahora, cada parte puede calcular la clave secreta de sesión:

[35] **Diffie-Hellman**[1] (debido a Whitfield Diffie y Martin Hellman) permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada).

$$K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q = \alpha^{X_A X_B} \bmod q$$

El algoritmo Diffie-Hellman tiene dos características interesantes:

- Las claves secretas se crean solo cuando es necesario. Ni hay que almacenar claves secretas durante un periodo largo de tiempo exponiéndolas a vulnerabilidad.
- El intercambio no requiere una infraestructura preexistente, sino un acuerdo sobre los parámetros globales.

Hay una serie de debilidades en Diffie-Hellman:

- No proporciona información sobre las identidades de las partes.
- Está expuesto al ataque por interceptación (man-in-the-middle), en el que una tercera parte C suplanta a B mientras se comunica con A y suplanta a A mientras se comunica con B. tanto A como B acaba en la negociación de una clave con C, que puede observar el tráfico y conducirlo entre A y B. el ataque por interceptación se produce como sigue:
  1. B envía su clave Y_B en un mensaje dirigido a A (ver figura 5.8).

  2. El enemigo (E) intercepta este mensaje, guarda la clave publica de B y envía un mensaje a A, que tiene el identificador de usuario de B, pero la clave publica de E es Y_E. este mensaje se envía de forma que parezca enviado por el sistema de B. A recibe el mensaje de E y almacena la clave publica de E con el identificador de usuario de B. de la mismo forma, E envía un mensaje a B con la clave publica de E, fingiendo que proviene de A.

  3. B calcula una clave secreta K_1 basada en la clave privada de B y en Y_E. A calcula una clave secreta K_2 basada en la clave privada de A

y en Y_E. E calcula K_1 usando la clave secreta de EX_E e Y_B y calcula K_2 usando X_E e Y_A.

4. De ahora en adelante, E puede retransmitir mensajes de A a B y de B a A, cambiando de forma adecuada sus cifrado en ruta de forma que ni A ni B sabrán que están compartiendo su combinación con E.

5. Requiere un elevado número de cálculo como resultado, es vulnerable al ataque de obstrucción, en el que un componente solicita un gran número de claves. La víctima gasta recursos considerables de computación haciendo exponenciación[36] modular inútil, en vez de trabajo real.

Oakley está diseñado para tener las ventajas de Diffie-Hellman y contrarrestar sus puntos débiles.

5.6.1.1 Características de Oakley

El algoritmo Oakley se caracteriza por cinco aspectos importantes:

1. Emplea un algoritmo conocido como cookies para impedir los ataques de obstrucción.
2. Permite que las dos partes negocien un grupo: este, básicamente, especifica los parámetros globales del intercambio de claves de Diffie-Hellman.

[36] **La exponenciación** es una operación definible en un álgebra sobre un cuerpo normada completa o álgebra de Banach (espacio vectorial normado completo que además es un anillo) que generaliza la función exponencial de los números reales.

3. Usa valores aleatorios (nonce[37]) para proteger de ataques de repetición.
4. Permite el intercambio de valores de clave pública de Diffie-Hellman.
5. Autentifica el intercambio Diffie-Hellman para evitar ataques de intercepción.

Consideremos el problema de los ataques de obstrucción. En este ataque, un oponente falsifica la dirección origen de usuario legítimo y envía una clave pública Diffie-Hellman a la víctima. Luego, la victimas realiza una exponenciación modular para calcular la clave secreta. Mensaje repetido de este tipo puede obstruir el sistema de la víctima con trabajos inútil.

El intercambio de cookies requiere que cada parte envíe un número pseudoaleatorio, la cookies en el mensaje inicial, que la otra parte reconoce. Este reconocimiento debe repetirse en el primer mensaje del intercambio de la clave Diffie-Hellman. Si la dirección fue falsificada, el oponente no obtiene respuesta. Así un oponente puede forzar a un usuario a generar reconocimiento y no a realizar el cálculo Diffie-Hellman.

ISAKMP obliga a que la generación de cookies satisfaga tres requisitos básicos:

1. La cookies debe depender de las partes específicas. Esto evita que un atacante obtenga una cookies usando una dirección IP y un puerto UDP reales y usándola luego para inundar a la victimas con solicitudes de direcciones IP o puertos elegidos de forma aleatorias.

2. No debe ser posible que alguien que no sea la entidad emisora genere cookies que sean aceptadas por esa entidad; esto implica que la entidad

[37] N**once es una abreviatura de (**number used once,). Es a menudo un número aleatorio en un protocolo de autentificación para evitar que viejas comunicaciones no puedan ser rechazadas.

emisora usara información secreta local en la generación y posterior verificación de una cookies. No debe ser posible deducir esta información secreta a partir de una cookies particular. La importancia de este requisito se halla en que la entidad emisora no necesita guardar copias de su cookies, en cuyo caso sería más vulnerable, pero puede verificar el reconocimiento de una cookies entrante cuando sea necesario.

3. Los métodos de generación y verificación de cookies deben ser rápidos para evitar ataques que intenten sabotear los recursos del procesador.

El método recomendado para crear cookies es realizar un hash rápido (por ejemplo, MDS) sobre las direcciones IP de origen y de destino, los puertos UDP fuente y destino y un valor secreto generado localmente.

Oakley permite el uso de diferentes grupos para el intercambio de claves Diffie-Hellman. Cada grupo incluye la definición de los dos parámetros globales y la identidad del algoritmo. La especificación incluye los siguientes grupos:

- Exponenciación modular con módulo de 768 bits
  $q = 2^{768} – 2^{704} – 1+ 2^{64} \times (12^{638} \times \pi! + 149686)$
  $\alpha = 2$

- Exponenciación modular con módulo de 1024 bits
  $q = 2^{1024} – 2^{960} – 1+ 2^{64} \times (12^{894} \times \pi! + 129093)$
  $\alpha = 2$

- Exponenciación modular con modulo de 1536 bits
  - Parámetros que deben determinarse

- Grupo de curvas elípticas sobre 2^{155}

- Generador (hexadecimal): X = 7B, Y = IC8
- Parámetros de curva elíptica (hexadecimal): A = 0, Y = 7338F

- Grupo de curva elíptica sobre 2^{185}
  - Generador (hexadecimal): X = 18, Y = D
  - Parámetros de curva elíptica (hexadecimal): A = 0, Y = IEE9

Los primeros tres grupos son el algoritmo clásico de Diffie-Hellman usando exponenciación modular. Los últimos dos grupos usan la curva elíptica análoga a la de Diffie-Hellman.

Oakley usa valores aleatorios (nonces) para proteger de los ataques de repetición. Cada **nonce** es un número pseudoaleatorio generado localmente. Los nonces aparecen en respuestas y se cifran durante ciertas partes del intercambio para asegurar su uso.

Se pueden usar tres métodos de autentificación con Oakley:

- **Firmas digitales:** el intercambio se autentifica firmando un hash obtenible mutuamente; cada parte cifra el hash con su clave privada. El hash se genera usando parámetros importantes como identificadores de usuario y nonces.
- **Cifrado de clave pública:** el intercambio se autentifica cifrando parámetros como identificadores y nonces con la clave privada del emisor.
- **Cifrado de clave simétrica**: se puede usar una clave procedente de algún mecanismo fuera de banda para autentificar el intercambio mediante el cifrado simétrico de los parámetros de intercambio.

5.6.1.2 Ejemplo de intercambio Oakley

La especificación Oakley incluye una serie de ejemplos de intercambios que están permitidos por el protocolo. Para dar una idea de Oakley, presentamos un

ejemplo, llamado intercambio agresivo de clave en la especificación, porque solo se intercambian tres mensajes.

La figura 5.11 muestra el protocolo de intercambio agresivo de claves. En el primer paso, el iniciador (I) transmite una cooky, el grupo que se va a usar, y la clave pública.

I → R: CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, S_{KI}[ID_I || ID_R || N_I || GRP || g^x || EHAO]

R→ I: CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, , ID_I N_R, N_I, S_{KR}[ID_R || ID_I || N_R || N_I || GRP || g^y || g^x || EHAS]

I→ R: CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, S_{KI}[ID_I || ID_R || N_I || N_R || GRP || g^x || g^y || EHAS]

Figura 5.11 Ejemplo de intercambio agresivo de claves Oakley

Notación:

I = Iniciador

R = Replicante

CKY_I, CKY_R = Cookies de iniciador y replicante

OK_KEYX = Tipo de mensaje de intercambio de claves

GRP = Nombre del grupo Diffie-Hellman para este intercambio

g^x, g^y = Clave pública del iniciador y del replicante; g^{xy} = clave de sesión de este intercambio

EHAO, EHAS = Funciones de cifrado, hash y de autentificación ofrecidas y seleccionadas

NIDP = Indica que no se usa cifrado para el resto del mensaje

ID_I, ID_R = Identificador del iniciador y del replicante

N_I, N_R = Nonce aleatorio suministrado por el iniciador o el replicante para este intercambio

$S_{KI}[X]$, $S_{KR}[X]$ = Indica la firma sobre X usando la clave privada (clave de firma) del iniciador, o del replicante

Diffie-Hellman de I para este intercambio. También indica los algoritmos ofrecidos de cifrado de clave pública, hash y de autentificación que se van a usar en este intercambio. Además, se incluyen en el mensaje los identificadores de I y del replicante (R) y el nonce de I para este intercambio. Por último, I añade una firma usando la clave privada de I que firma los dos identificadores, el nonce, el grupo, la clave publica Diffie-Hellman y los algoritmos ofrecidos.

Cuando R recibe el mensaje el mensaje, verifica la firma usando la clave pública de firma de I. R reconoce el mensaje devolviendo la cookies de I, el identificador y el nonce, así como el grupo. R también incluye una cookie en el mensaje, la clave pública Diffie-Hellman de R, los algoritmos seleccionados (que deben estar entre los algoritmos ofrecidos), el identificador de R y el nonce de R que firma los dos identificadores, los dos nonces, el grupo, las dos claves publicas Diffie-Hellman y los algoritmos seleccionados.

Cuando I recibe el segundo mensaje, verifica la firma usando la clave publica de R. los valores nonce en el mensaje aseguran que no es la repetición de un mensaje antiguo. Para completar el intercambio, I debe enviar un mensaje de vuelta a R para verificar que I ha recibido la clave pública de R.

5.6.2 ISAKMP

ISAKMP define los procedimientos y los formatos de los paquetes para establecer, negociar, modificar y eliminar asociaciones de seguridad.

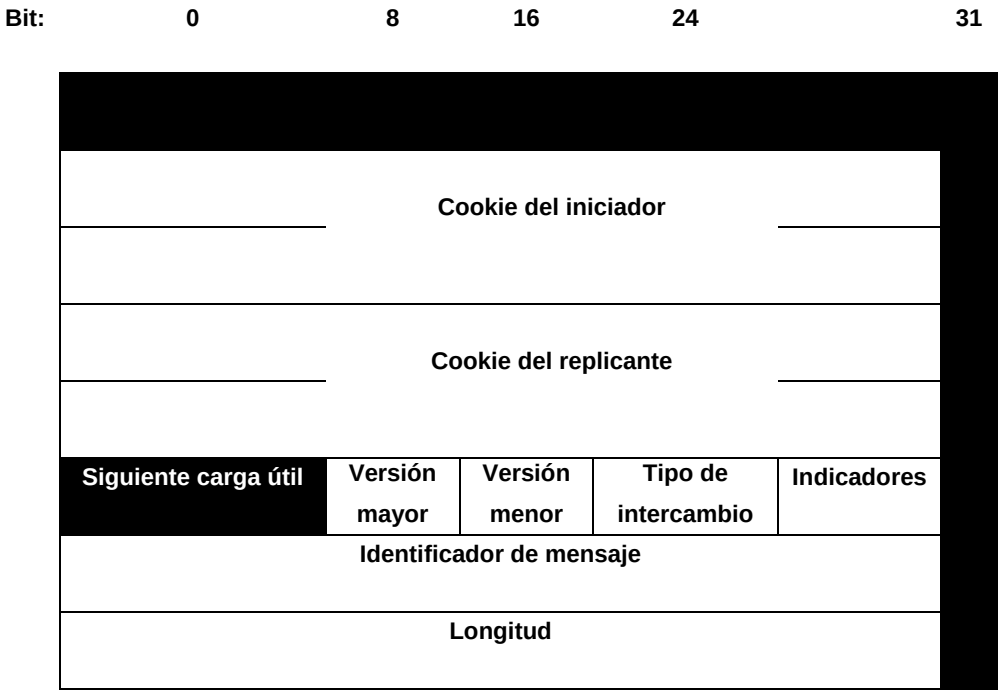
Como parte del establecimiento de la SA, ISAKMP define las cargas útiles para intercambiar la generación de claves y los datos de autentificación. Los formatos de las cargas útiles proporcionan un marco de trabajo consistente independiente del protocolo específico del intercambio de claves, del algoritmo de cifrado y del mecanismo de autentificación.

5.6.2.1 Formato de la cabecera ISAKMP

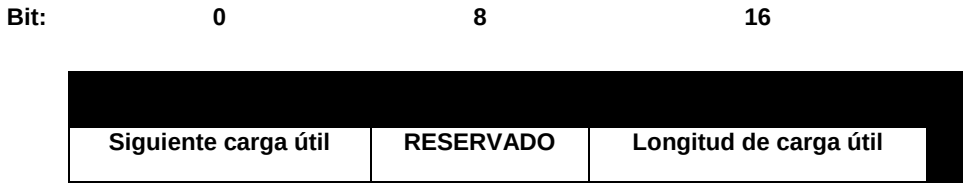
Un mensaje ISAMKMP se compone de una cabecera ISAKMP seguida de una o más cargas útiles. Todo esto se transfiere en un producto de transporte. La especificación obliga a que las implementaciones permitan el uso de UDP para el protocolo de transporte.

Consta de los siguientes campos:

- **Cookie del iniciador (64 bits):** cookies de la entidad que inicio el establecimiento de la SA, notificación de SA o eliminación de la misma.
- **Cookie de los replicantes (64 bits**): cookie de la entidad que responde; nula en el primer mensaje del iniciador.
- **Siguiente carga útil (ocho bits):** indica el tipo de la primera carga útil del mensaje; las cargas útiles se discuten en el siguiente sub-apartado.
- **Versión mayor (cuatro bits):** indica la versión mayor que se usa del ISAKMP.
- **Versión menor (cuatro bits):** indica la versión menor en uso.
- **Tipo de intercambio (ocho bits):** indica el tipo de intercambio; se discute más adelante en esta sección.
- **Indicadores (ocho bits**): indica las opciones específicas fijada para este intercambio ISAKMP. Dos bits definidos hasta ahora: el bit de cifrado (encryption bit) se fija si todas las cargas útiles que siguen a la cabecera se cifran usando el algoritmo de cifrado para esta SA. El bit de garantía (commit bit) se usa para asegurar que el material cifrado no se recibe antes de terminar el establecimiento de la SA.
- **Indicador de mensaje (32 bits):** identificador único para este mensaje.
- **Longitud (32 bits):** longitud del mansaje total (cabecera y todas las cargas útiles) en octetos.



(a) Cabecera ISAKMP



(b) Cabecera genérica de carga útil

Figura 5.12 Formatos ISAKMP

5.6.2.2 Tipos de carga útil ISAKMP

Todas las cargas útiles ISAKMP comienzan con la misma cabecera genérica de carga útil que muestra la figura 5.12b. El campo siguiente carga útil tiene un valor O si es la ultima carga útil del mensaje; sino su valor es el tipo de la carga útil siguiente. El campo longitud de carga útil indica la longitud en octetos de esa carga útil, incluyendo la cabecera genérica de carga útil.

Tipo	Parámetros	Descripción
Asociación de seguridad (SA).	Dominio de interpretación, situación.	Se usa para negociar atributos de seguridad e indicar el DOI y la situación en la que tiene lugar la negociación.
Propuesta (P)	Numero de propuestas, identificador de protocolo, tamaño de SPI, nº de transformaciones, SPI.	Se usa durante la negociación de SA; indica el protocolo que ha de usarse y un número de transformaciones.
Transformación (T)	Numero de transformaciones, identificación de transformaciones, atributos de la SA.	Se usa durante la negociación de la SA; indica los atributos de transformaciones y los relacionados con las SA.
Intercambio de clave (KE)	Datos de intercambio de claves	Permite una variedad de técnica de intercambio de claves.
Identificación (ID)	Tipo de identificador, datos de identificadores.	Se usa para intercambiar información de identificación
Certificado (CERT)	Codificación de certificados, datos de identificadores.	Se usa para transportar certificados y otra información relacionada.
Solicitud de certificado (CR)	Numero de tipos de certificado, tipos de certificados, numero de autentificaciones de certificado, autoridades de certificación.	Se usa para solicitar certificados; indica los tipos de certificados solicitados y las autoridades de certificación aceptables.
Hash (HASH)	Datos de hash	Contiene datos generados por una función hash.
Firma (SIG)	Datos de la firma	Contiene datos generados por una función de firma digital.
Nonce (NONCE)	Datos del nonce.	Contiene un nonce.
Notificación (N)	DOI, identificación de protocolo, tamaño de SPI, notificar tipo de mensaje, SPI, datos de notificación	Se usa para transmitir datos de notificación, como condición de error.
Eliminar (D)	DOI, identificación de protocolo, tamaño de SPI, nº de SPI, SPI (uno o más).	Indica una SA que ya no es válida.

Tabla 5.3 Tipos de carga útil ISAKMP

La tabla 5.3 resume los tipos de carga útiles definidos para ISAKMP, y presenta los campos o parámetros que son parte de cada carga útil. La carga útil de SA se usa para empezar el establecimiento de una SA. En esta carga útil, el parámetro dominio de interpretación identifica el DOI en el que se está llevando a cabo la negociación. En DOI IPSec es un ejemplo, pero ISAKMP puede usarse en otros contextos. El parámetro situación defina la política de seguridad para esta negociación; básicamente, se especifican los niveles de seguridad requerido para el cifrado y la confidencialidad (por ejemplo, nivel de confidencialidad, compartimento de seguridad).

La carga útil de propuesta contiene información usada durante la negociación de la SA. La carga útil indica el protocolo para esta SA (ESP o AH) para la cual se están negociando servicios y mecanismo. La carga útil también incluye el SPI de la entidad emisora y el número de transformaciones. Cada transformación está contenida en una carga útil de transformaciones. El uso de varilla cargas útiles de transformaciones permite que el iniciador ofrezca varias posibilidades, de las cuales el replicante debe elegir una o rechazar la oferta.

La carga útil de la transformación define una transformación de seguridad que se debe usar para asegurar el canal de comunicaciones para el protocolo designado. El parámetro números de transformaciones sirve para identificar esta carga útil concreta con el objetivo de que el replicante pueda usarlo para indicar la aceptación de esta transformación. Los campos identificación de transformación y atributos identifica una transformación especifica (por ejemplo, 3 DES, HMAC-SHA-1-96 para AH) con sus atributos asociados (por ejemplo, longitud de hash).

La carga útil del intercambio de claves se puede usar para una variedad de técnicas de intercambio de claves, incluyendo Oakley, Diffie-Hellman y el intercambio de claves basado en RSA que usa PGP. El campo de clave de intercambio de claves contiene los datos necesarios para generar una clave de sesión y depende del algoritmo de intercambio de claves que se ha utilizado.

La carga de identificación se usa para determinar la identidad de las entidades que se comunican y se puede usar para determinar la autenticidad de la información. Normalmente, el campo datos de identificación contiene una dirección IPv4 o IPv6.

La carga útil del certificado transfiere un certificado de clave pública. El campo codificación del certificado indica el tipo de certificado o la información referente al este, que puede incluir la siguiente:

- Certificado X.509-PKCS#7
- Certificado PGP
- Clave firmada DNS
- Certificado X.509 – firma
- Certificado X.509 – intercambio de claves
- Tokens de Kerberos
- Lista de revocación de certificados (CRL)
- Lista de revocación de autoridades (ARL)
- Certificado SPKI

En cualquier momento del intercambio ISAKMP, el emisor puede incluir una carga útil de solicitud de certificado para solicitar el certificado de las otras entidades comunicantes. La carga útil puede presentar más de un tipo de certificado aceptable y más de una autoridad de certificación aceptable.

La carga útil hash contiene datos generados por una función hash sobre alguna parte del mensaje y/o estado ISAKMP. Esta carga útil puede usarse para verificar la integridad de los datos en un mensaje y para autentificar a las entidades negociadoras.

La carga útil de firma contiene datos generados por una función de firma digital sobre alguna parte del mensaje y/o estado ISAKMP. Esta carga útil se usa

para verificar la integridad de los datos en un mensaje y puede usarse para servicios de no repudio.

La carga útil nonce contiene datos aleatorios que se usan para garantizar la validez temporal durante un intercambio y proteger de ataques de repetición. La carga útil de notificación contiene la información de error o la información de estado asociada con esta SA o esta negociación de SA. Se ha definido los siguientes mensajes de error ISAKMP:

Tipos de carga útil invalido	Identificador de protocolo invalido	Codificación de certificado invalidad
DOI no permitido	SPI invalido	Certificado invalido
Situación no permitida	Identificador de transformación invalido	Mala sintaxis de solicitud de certificado
Cookie invalidad	Atributos no permitidos	Autoridad de certificación invalida
Versión mayor invalidada	Ninguna propuesta elegida	Información hash invalidada
Versión menor invalidada	Mala sintaxis de propuesta	Fallo de autentificación
Tipo de intercambio invalido	Carga útil mal formada	Firma invalida
Indicadores inválidos	Información de clave invalida	Notificación de dirección
Identificadores de mensaje invalida		

Tabla 5.4. Notificaciones de error o negociación de SA

El único mensaje de estado ISAKMP definido hasta ahora es Conectado. Además de estas notificaciones ISAKMP, se usan las notificaciones especificas DOI.

Para IPSec, se definen los siguientes mensajes adicionales de estado:

- **Tiempo de vida del replicante:** comunica el tiempo de vida de la SA elegido por el replicante.

- **Estado de repetición:** se usa para la confirmación positiva de la elección del replicante en cuanto a si el replicante realizara detección anti repeticiones o no.

- **Contacto inicial:** informa a la otra parte que esta es la primera SA establecida con el sistema remoto. Entonces el receptor de esta notificación podría eliminar cualquier SA existente que tenga para el sistema emisor basándose en que el sistema emisor ha reiniciado y ya no son válidas.

La carga útil de eliminación indica una o más SA que el emisor ha eliminado de su base de datos y que, por lo tanto, ya no son válidas.

5.6.2.3 Intercambios ISAKMP

ISAKMP proporciona un marco de trabajo para el intercambio de mensajes, donde los tipos de carga útil sirven como pilares de construcción.

La especificación identifica cinco tipos predeterminados de intercambio que deberían permitirse; estos se resumen en la Tabla 5.5. En la tabla, SA se refiere a la carga útil de una SA con cargas útiles asociadas de Protocolos y Autentificación.

a) El **intercambio base** permite que el material de intercambio de claves y autentificación se transmita junto. Esto minimiza el número de intercambios a costa de no proporcionar protección de identidad.

   Los dos primeros mensajes proporcionan cookies y establecen una SA con el protocolo y las transformaciones acordadas; ambas partes usan un nonce para evitar ataques de repetición. Los dos últimos mensajes intercambias el material de clave y los identificadores de usuarios, con la carga útil AUTH que se usa para autentificar claves, identidades y los nonces de los dos primeros mensajes.

b) El **intercambio de protección de identidad** expande el intercambio base para proteger las identidades de los usuarios.

   Los dos primeros mensajes establecen la SA. Los dos siguientes mensajes realizan el intercambio de claves, con nonces para la protección contra repeticiones. Una vez que la clave de sesión ha sido calculada, las partes intercambian mensajes cifrados, que contienen información de autentificación, como firmas digitales y, opcionalmente, certificados que validan las claves públicas.

c) El **intercambio de solo autentificación** se usa para realizar autentificación mutua sin intercambio de claves.

   Los dos primeros mensajes establecen la SA. Además el replicante usa el segundo mensaje para transportar su identificador y utiliza la autentificación para proteger el mensaje. El iniciador envía el tercer mensaje para transmitir su identificador autentificado.

d) El **intercambio agresivo** reduce el número de intercambio a costa de no proporcionar protección de identidad.

   En el primer mensaje el iniciador propone una SA con opciones ofrecidas de protocolo y transformación asociadas. El iniciador

también empieza el intercambio de claves y proporciona su identificador.

En el segundo mensaje, el replicante indica su aceptación de la SA con un protocolo y una transformación particular es, completa el intercambio de claves y autentifica la información transmitida. En el tercer mensaje, el iniciador transmite un resultado de autentificación que cubre la información previa, cifrada usando la clave de sesión secreta compartida.

e) El **intercambio informativo** se usa para la transmisión unidireccional de información para la gestión de SA.

Intercambio	**Nota**
(a) Intercambio base	
(1) I→R: SA; NONCE	**Empieza la negociación SA ISAKMP**
(2) R→I:SA; NONCE	**Acuerdo sobre la SA básica**
(3) I→R: KE; ID_I; AUTH	**Clave generada; identidad del iniciador verificada por el replicante**
(4) R→I: KE; ID_R: AUTH	**Identidad del replicante verificada por el iniciador; clave generada; SA establecida**
(b) Intercambio de protección de identidad	
(1) I→R: SA	**Empieza la negociación SA-ISAKMP**
(2) R→I:SA	**Acuerdo sobre la SA básica**
(3) I→R: KE; NONCE	**Clave generada**
(4) R→I: KE; NONCE	**Clave generada**
(5) I→R: ID_I; AUTH	**Identidad del iniciador verificada por el replicante**
(6) * R→I: ID_R; AUTH	**Identidad del replicante verificada por el iniciador; SA establecida**

(c) Intercambio solo de autenticación	
(1) I→R: SA; NONCE	**Empieza la negociación SA-ISAKMP**
(2) R→I:SA; NONCE; ID_R: AUTH	**Acuerdo sobre la SA básica; identidad del replicante verificada por el iniciador; SA establecida**
(3) I→R: ID_I; AUTH	**Identidad del iniciador verificada por el replicante; SA establecida**
(d) Intercambio agresivo	
(1) I→R: SA; KE; NONCE;	**Empieza la negociación SA-ISAKMP y el intercambio de**
(2) R→I:SA; KE; NONCE; ID_R: AUTH	**Identidad del iniciador verificada por el replicante; clave generad; acuerdo sobre la clave SA básica.**
(3) I→R: AUTH	**Identidad del replicante verificada por el iniciador; SA establecida**
(e) Intercambio informativo	
(1) * I→R: /D	**Notificación o eliminación de error o estado**

Tabla 5.5 Tipos de intercambios ISAKMP

Notación:
I = iniciador
R = replicante
(*) = significa cifrado de carga útil después de la cabecera ISAKMP

CAPITULO VI: Diseño Metodológico

6.1 Tipo de estudio

El presente trabajo es de carácter exploratorio y descriptivo, ya que presenta las siguientes características:

- Existe poca investigación relacionada con nuestro tema especifico, en la Unan – Managua.
- Se presenta un trabajo con pocos antecedentes bibliográficos. Las fuentes principales de información son páginas de sitios web y libros.

6.2 Método de investigación

En este trabajo se utilizan como métodos de investigación, una combinación de los métodos de análisis y de síntesis, de acuerdo al problema planteado, se organizó, clasificó, estudió y conservó mucha de la información recolectada y se comparó con lo existente a fin de encontrar una solución, referente al tema planteado.

6.3 Técnicas de colección de la información

En el desarrollo de este trabajo se combinaron dos métodos de investigación para llegar a obtener resultados satisfactorios:

i. Fuentes Primarias:

- Bibliotecas: consultas de libros relacionados con nuestro tema general y todo lo referente para llegar a relacionar nuestro tema especifico, además tesis monográficas y de seminario de graduación donde comparamos conceptos, definiciones, etc.
- También se utilizó información encontrada en Internet, siendo esta una de las principales fuentes de información obtenida de los diferentes capítulos conformada en nuestra tesis, además de temas relacionados

con el proceso de encriptamiento con el fin de conocer más a fondo el desarrollo de nuestro proyecto.

ii. Fuentes secundarias:

- Utilizamos manuales relacionados a la plataforma de programación de Visual.net.
- Se analizaron manuales de seguridad.
- Se utilizó una guía para escribir la tesis.
- Se requirió de algunos folletos relacionados con la metodología de investigación.
- Se tomo como muestra el diseño de un software que simula el proceso de encriptar y desencriptar archivos.

6.4 Procedimiento

En esta investigación documental se aplicó el método de análisis y síntesis para la recopilación de la información. Una vez asignado el tema específico se procedió a la recopilación de información, luego se seleccionó lo más importante.

Para obtener dicha información se acudió al Departamento de Computación y la Biblioteca Central de la Unan - Managua, así mismo de visitas a sitios de internet.

Después de recopilar la información para enunciar las teorías, se elaboró un marco conceptual para formar un cuerpo de ideas que sustentan el objetivo de estudio y ampliar los conocimientos, hubo una serie de presentaciones del tema, para valorar los avances de esta investigación, y de esa forma hacer mejoras en cada etapa del documento y así mismo en el desarrollo, diseño y análisis del proyecto.

Para la elaboración del proyecto se visitaron diferentes sitios web, con el objetivo de encontrar información sobre la encriptación y desencriptación de

archivos, y así proceder en la elaboración del sistema, primeramente se investigo en qué consistía cada algoritmo del proceso de encriptación, y luego seleccionar el que mejor funcionaba.

Cabe mencionar que el algoritmo seleccionado utiliza la misma clave para encriptar y desencriptar el archivo, pero en el proceso de mejoras del sistema se modificaron varios campos las cuales por orientaciones de nuestro tutor se agrego la casilla de confirmar contraseña y también la casilla simulando que se envía a una dirección IP de destino, de esta forma se hizo énfasis a uno de los mecanismos de la Seguridad IP.

Con la información recopilada, se hizo una aplicación para simular la transferencia de archivos utilizando el Protocolo de Seguridad IP, donde se aplicó algunos mecanismos de seguridad como la encriptación de archivos.

Terminado el desarrollo de esta aplicación se realizo un breve resumen, recomendaciones sobre el tema, la aplicación, y algunas conclusiones.

6.5 Descripción del instrumento

Dentro de la infraestructura informática debemos tomar en cuenta lo siguiente:

- Hardware con el cual cuenta para el funcionamiento de la red (Ruteadores, Hubs, etc.).
- Procesador Pentium III.
- Memoria RAM de 512 MB.
- Disco Duro de 60 GB.
- Windows XP.
- Antivirus debidamente actualizado.
- Microsoft Visual Studio 2008. Version 9.0.21022.8 RTM
- Microsoft Visual Basic .NET Framework. Version 3.5 SP1
- Installed Edition: Enterprise.

Se escogió Visual Basic.net por las siguientes razones:

1. Visual Basic.net es una herramienta productiva para la creación de aplicaciones que se ejecutan en el sistema operativo Microsoft Windows. La programación en Visual Basic se basa en un ambiente de desarrollo totalmente gráfico, que ofrece la creación de interfaces gráficas amigables, y en cierta medida, también la programación misma.

2. Visual.net cuenta con funciones de seguridad como por ejemplo: encriptar, que facilita la programación de esta aplicación si no existieran estas funciones sería un trabajo bien tedioso en otro lenguaje en donde se tendría que adecuar a ese lenguaje.

3. El editor de código y otros elementos del EID (**Entorno Integrado de Desarrollo)** poseen nuevas características y mejoras que facilitan la lectura y escritura de los procedimientos escritos en la aplicación. Este entorno incluye elementos tales como: barra de menús, barra de controles, barra de herramientas, ventana de propiedades, ventana de proyectos, depurador, formularios, etc.

6.6 Algoritmo de Cifrado y Descifrado de la aplicación

El espacio de nombres **System.Security.Cryptographic** de Microsoft .NET Framework proporciona diversas herramientas que ayudan al cifrado y el descifrado.

La clase **CryptoStream** es una de las numerosas clases que se proporcionan y está diseñada para cifrar o descifrar el contenido a medida que se transmite en secuencias a un archivo.

Se utilizaron las siguientes librerías o espacios de nombres:

System

System.Security

System.Security.Cryptography

System.Text

System.IO

El algoritmo utilizado para cifrar y descifrar es Rijndael que es un algoritmo del tipo AES (Estándar avanzado de encriptación), funciona de la siguiente manera:

1º. Se obtiene la clave para cifrar.

2º. Luego obtiene el archivo a cifrar a través de la clase CryptoStream utilizando el proveedor de cifrado para obtener un objeto de cifrado (**CreateEncryptor**) y el objeto de salida **FileStream**.

3º. Lee en el archivo de entrada y escribe en el archivo de salida que se está pasando al objeto **CryptoStream**, en el que se cifrará con la clave que proporcionó.

El proceso de descifrado es muy similar al proceso de cifrado, pero hay dos diferencias importantes entre los procedimientos **DecryptFile** y **EncryptFile**. En primer lugar, se utiliza **CreateDecryptor** en lugar de **CreateEncryptor** para la creación del objeto **CryptoStream**, especificando cómo se utilizará el objeto. En segundo lugar, al escribir el texto descifrado en el archivo de destino, el objeto **CryptoStream** es ahora el origen en vez de la secuencia de destino.

4º. Una vez que el archivo es encriptado, se realiza la simulación de la transferencia del archivo solicitando la dirección IP del destino al que se enviara el archivo.

El archivo encriptado no afecta el archivo original, si por error se olvida desencriptar o no recordamos la contraseña el archivo encriptado se pierde y no afecta el archivo original.

6.7 Descripción del algoritmo RIJNDAEL (Algoritmo Sim)

6.7.1 Buscar

Este algoritmo por defecto hace la búsqueda en la unidad C, opcional para el usuario buscar en cualquier directorio tales como: Mis documentos, USB, Escritorio, etc., y todo tipo de archivo.

```
Private Sub FiletoEncrypt_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles FiletoEncrypt.Click
    Dim FEcrypt As New OpenFileDialog
    limpiar()
    contar = contar + 1
    cer = 11
    FEcrypt.FileName = ""
    FEcrypt.Title = "ELIGA UN ARCHIVO PARA ENCRIPTAR"
    FEcrypt.InitialDirectory = "C:\"
    FEcrypt.Filter = "All Files (*.*) | *.*"
    If FEcrypt.ShowDialog = DialogResult.OK Then
       strFileToEncrypt = FEcrypt.FileName
       txtFiletoEncrypt.Text = strFileToEncrypt
       Dim iPosition As Integer = 0
       Dim i As Integer = 0
       While strFileToEncrypt.IndexOf("\"c, i) <> -1
          iPosition = strFileToEncrypt.IndexOf("\"c, i)
          i = iPosition + 1
       End While
       strOutputEncrypt = strFileToEncrypt.Substring(iPosition + 1)
       Dim S As String = strFileToEncrypt.Substring(0, iPosition + 1)
       strOutputEncrypt = strOutputEncrypt.Replace("."c, "_"c)
       txtdestinationEncrypt.Text = S + strOutputEncrypt + ".tmp"
       Encrypt.Enabled = True
```

```
        Encrypt.Focus()
    End If
End Sub
```

6.7.2 Encriptar

Este algoritmo consiste en una clave para poder encriptar el archivo seleccionado, cabe mencionar que este proceso se realiza internamente ya que hace llamada al procedimiento para ingresar la Contraseña:

```
Private Sub Encrypt_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Encrypt.Click
    Encrypt.Enabled = False
    txtPassEncrypt.Enabled = True
    FiletoEncrypt.Enabled = False
    txtPassEncrypt.Focus()
End Sub
```

1) **Algoritmo ingresar contraseña**

Consiste en teclear una clave secreta, como mínimo 8 caracteres, y como máximo 10 caracteres, luego que se ha ingresado la contraseña hace llamada al procedimiento Confirmar Contraseña.

```
Private Sub txtPassEncrypt_KeyPress(ByVal sender As Object, ByVal e As System.Windows.Forms.KeyPressEventArgs) Handles txtPassEncrypt.KeyPress
    If ChrW(Keys.Enter) = e.KeyChar Then
        If Len(txtPassEncrypt.Text) <> 8 Or txtPassEncrypt.Text <> "" Then
            If Len(txtPassEncrypt.Text) >= 8 Then
                txtPassEncrypt.Enabled = False
                contar = 1
                confirmar.Enabled = True
```

```
            confirmar.Focus()
        Else
            If txtPassEncrypt.Text = "" Then
                MsgBox(" DEBE ESCRIBIR SU CONTRASEÑA.",
MsgBoxStyle.Information, )
                txtPassEncrypt.Focus()
            Else
                MsgBox(" SU CONTRASEÑA DEBE SER DE 8 DIGITOS O MAS.",
MsgBoxStyle.Information, )
                txtPassEncrypt.Text = ""
                txtPassEncrypt.Focus()
            End If
            End If
        Else
            MsgBox(" DEBE INGRESAR UNA CONTRASEÑA.",
MsgBoxStyle.Information, )
            txtPassEncrypt.Text = ""
            txtPassEncrypt.Focus()
        End If
    End If
End Sub
```

2) Confirmar contraseña

Consiste en teclear la misma clave, su objetivo es que el usuario no olvide la contraseña al momento de desencriptar el archivo; una vez ingresado y confirmado la contraseña se envía el archivo simulando una dirección IP

```
Private Sub confirmar_KeyPress(ByVal sender As Object, ByVal e As
System.Windows.Forms.KeyPressEventArgs) Handles confirmar.KeyPress
    If ChrW(Keys.Enter) = e.KeyChar Then
```

```
        If Len(confirmar.Text) <> 8 Or confirmar.Text <> "" Then
            If Len(confirmar.Text) >= 8 Then
                If txtPassEncrypt.Text = confirmar.Text Then
                    confirmar.Enabled = False
                    contar = 1
                    Enviar.Enabled = True
                    Enviar.Focus()
                Else
                    MsgBox(" SU CONTRASEÑA NO COINCIDE CON LA
ANTERIOR.", MsgBoxStyle.Information, )
                    confirmar.Text = ""
                    confirmar.Focus()
                End If
            Else
                If (confirmar.Text) = "" Then
                    MsgBox(" DEBE ESCRIBIR UNA CONTRASEÑA.",
MsgBoxStyle.Information, )
                    confirmar.Focus()
                Else
                    MsgBox (" SU CONTRASEÑA DEBE SER DE 8 DIGITOS O MAS.",
MsgBoxStyle.Information,)
                    confirmar.Text = ""
                    confirmar.Focus ()
                End If
            End If
        Else
            MsgBox (" DEBE INGRESAR UNA CONTRASEÑA.",
MsgBoxStyle.Information,)
            confirmar.Text = ""
            confirmar.Focus()
        End If
```

```
    End If
End Sub
```

6.7.3 Enviar

Este algoritmo consiste en la simulación del envío del archivo, para esto se ingresa la dirección IP a la que se desea enviar el archivo.

```
Private Sub Enviar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Enviar.Click
  direccion.Show()
End Sub
```

1. Dirección IP

Consiste en el ingreso de la dirección IP, este algoritmo consta de 4 casillas donde el usuario digitará de acuerdo al rango y al tipo de dirección IP(A, B, C). Lo siguiente son los rangos que se debe de digitar para cada posición: 192...223 posición 1; 1...254 posición 2,3 y 4.

```
Imports System.Windows.Forms
Public Class direccion
   Sub limpiar()
   pos1.Text = ""
      pos2.Text = ""
pos3.Text = ""
pos4.Text = ""
pos1.Enabled = True
pos2.Enabled = False
pos3.Enabled = False
pos4.Enabled = False
```

```
End Sub
 Private Sub pos1_KeyPress(ByVal sender As Object, ByVal e As
System.Windows.Forms.KeyPressEventArgs) Handles pos1.KeyPress
      If Char.IsSymbol(e.KeyChar) Or Char.IsPunctuation(e.KeyChar) Or
Char.IsWhiteSpace(e.KeyChar) Then
         e.Handled = True
      End If
 If ChrW(Keys.Enter) = e.KeyChar Then
                If pos1.Text <> "" Then
        pos1.Enabled = False
        pos2.Enabled = True
       pos2.Focus()
  Else
     MsgBox("Este campo no puede ser nulo")
     pos1.Text = ""
     pos1.Focus()
  End If
Else
  If pos1.Text >= 192 And pos1.Text <= 223 Then
     pos1.Text = False
     pos2.Enabled = True
     pos2.Focus()
  End If
  End If
End Sub
```

6.7.4 Desencriptar

Al igual que el algoritmo de encriptar este consiste en una clave, cabe señalar que por ser simétrico depende de la misma clave con la que se encripto el archivo; una vez seleccionado esta opción inmediatamente se activa la opción Clave para Desencriptar.

```
Private Sub Dencrypt_Click(ByVal sender As System.Object, ByVal e As
    System.EventArgs) Handles Dencrypt.Click
    txtPassDecrypt.Enabled = True
    txtPassDecrypt.Focus()
End Sub
```

a) Clave para desencriptar

Al igual que el algoritmo password para encriptar el archivo, este consiste en teclear la misma clave secreta que se tecleo para encriptar el archivo.

```
    Private Sub txtPassDecrypt_KeyPress(ByVal sender As Object, ByVal e As
    System.Windows.Forms.KeyPressEventArgs) Handles
    txtPassDecrypt.KeyPress
  If ChrW(Keys.Enter) = e.KeyChar Then
    If Len(txtPassDecrypt.Text) <> 8 Or txtPassDecrypt.Text <> "" Then
      If Len(txtPassDecrypt.Text) >= 8 Then
        If txtPassDecrypt.Text = txtPassEncrypt.Text Then
          FileDesencrypt()
          clados()
          FiletoEncrypt.Enabled = True
          FiletoEncrypt.Focus()
          pbStatus.Visible = True
          MsgBox(" ARCHIVO DESENCRIPTADO CORRECTAMENTE",
MsgBoxStyle.Information, )
          contar = contar + 1
          Kill(txtdestinationEncrypt.Text)
          Kill(txtdestinationDecrypt.Text)
          Dencrypt.Enabled = False
          pbStatus.Visible = False
          Enviado2.Show()
```

```
                Enviado2.Ok.Enabled = True
                Enviado2.archivo.Text = txtFiletoEncrypt.Text  'strOutputEncrypt
                Enviado2.archivo.Enabled = False
                txtPassDecrypt.Enabled = False
                txtdestinationDecrypt.Visible = True
                txtdestinationDecrypt.Text = txtFiletoEncrypt.Text
            Else
                MsgBox(" ERROR:CONTRASEÑA NO RECONOCIDA, TECLEE CORRECTAMENTE SU CONTRASEÑA", MsgBoxStyle.Information, )
                txtPassDecrypt.Text = ""
                txtPassDecrypt.Focus()
            End If
        Else
            MsgBox(" SU CONTRASEÑA DEBE SER DE 8 DIGITOS O MAS.", MsgBoxStyle.Information, )
            txtPassDecrypt.Text = ""
            txtPassDecrypt.Focus()
        End If
    Else
        MsgBox(" ESCRIBA CORRECTAMENTE SU CONTRASEÑA.", MsgBoxStyle.Information, )
        txtPassDecrypt.Text = ""
        txtPassDecrypt.Focus()
    End If
  End If
End Sub
```

6.7.5 Cerrar (Pantalla de ENCRIPTAR_DESENCRIPTAR)

Solamente consiste en dar clic en la opción Cerrar, y podrá salir de la opción encriptar, desencriptar archivos, a la misma vez si al usuario se le olvido la

contraseña el archivo original no se verá afectado ya que elimina el archivo encriptado que es de extensión .tmp.

```
Private Sub close_Click(ByVal sender As System.Object, ByVal e As
    System.EventArgs) Handles cerrar.Click
        If txtdestinationDecrypt.Text = "" And txtdestinationEncrypt.Text <> ""
       And contar = 1 And cer <> 11 Then
        Kill(txtdestinationEncrypt.Text)
        End If
  Me.Close()
End Sub
```

6.7.6 Abrir (Archivo Encriptado y Desencriptado)

Su función es abrir el archivo, esta opción siempre se encuentra activa tanto para ver el archivo original como el archivo encriptado esto para que el usuario verifique que al momento de encriptar el archivo esta operación fue realizada exitosamente.

```
Private Sub Abrir_Click(ByVal sender As System.Object, ByVal e As
    System.EventArgs) Handles Abrir.Click
  Dim abr As New OpenFileDialog
  If contar = 1 Then
    abr.Filter = "ARCHIVOS TEMPORALES (*.tmp)|*.tmp"
    abr.InitialDirectory = "txtdestinationEncrypt.text"
    If abr.ShowDialog() = DialogResult.OK Then
      Process.Start(abr.FileName)
    End If
  Else
    abr.InitialDirectory = "txtdestinationEncrypt.text"
    If abr.ShowDialog() = DialogResult.OK Then
```

```
            Process.Start(abr.FileName)
        End If
    End If
End Sub
```

6.7.7 Salir (Pantalla principal)

Consiste solamente en salir de la aplicación.

```
Private Sub SalirToolStripMenuItem_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
SalirToolStripMenuItem.Click
 Dim resp As String
 resp = MessageBox.Show("ESTA SEGURO QUE DESEA SALIR
                                DEL SISTEMA.", _
 "AlgoritmoSim - Confirmar salida", MessageBoxButtons.YesNo,
MessageBoxIcon.Question)
        If resp = "6" Then
                Me.Close()
         End If
 End Sub
```

6.8 Discusión de los resultados

Al realizar la aplicación se obtuvieron los siguientes resultados:

- Se demostró que la implementación del algoritmo Rijndael funciona correctamente para la encriptación y desencriptación de cualquier tipo de archivo, bajo la plataforma Visual.net.

CONCLUSIONES

La realización de este trabajo nos ha permitido la obtención de una mayor comprensión de la seguridad existente en las redes IP. No sólo se ha profundizado en el estudio de los protocolos más importantes que permiten el funcionamiento de Internet (IP, UDP y TCP), sino que además se han podido observar globalmente, lo que nos ha permitido examinar sus características, relaciones y roles en el transporte de la Información por Internet.

El uso de herramientas de seguridad clásicas basadas en el filtrado simple de los datagramas que circulan por Internet (firewalls) se ha revelado insuficiente ante los ataques organizados. Así como el estudio de la seguridad informática, lo cual nos ayudó a comprender la importancia de aplicar seguridad a las redes analizando los peligros y amenazas más comunes que existen en Internet.

Con ayuda de los mecanismos de IPsec, a través de los algoritmos correspondientes, así como en los nuevos mecanismos de seguridad que pretenden darles solución a los problemas más comunes de la seguridad de redes, conociendo cómo funcionan, se diseñó una aplicación que simula la transferencia de archivos, a través de la plataforma Visual.Net, empleando los mecanismos de IPSec, dándole solución a uno de los problemas de seguridad más comunes como es la confidencialidad, cifrando la información que es enviada.

RECOMENDACIONES

Evaluar la viabilidad de esta aplicación, costos, condiciones legales, e infraestructura informática que sean las necesarias para que el proyecto se lleve a cabo y funcione correctamente.

Esta aplicación se puede mejorar para simular la transferencia de archivos desde un servidor FTP.

BIBLIOGRAFIA

LIBROS

1. Álvarez Marañón, Gonzalo. Pérez García, Pedro Pablo. “Seguridad Informática para empresas y particulares”. Editorial McGraw – Hill.
2. Carracedo Gallardo, Justo. “Seguridad en Redes Telemáticas”. Editorial McGraw – Hill.
3. Garfinkel, Simson y Stafford, Gene. “Seguridad Práctica en Unix e Internet”. McGraw-Hill.
4. Lockhart, Andrew. “Seguridad de redes: los mejores trucos”.
5. López Camacho, Vicente. “Linux, Guía de Instalación y administración”. Editorial Osborne Mac Graw- Hill. Interamericana de España, SAU.
6. Russel, Charlie. Crawford, Sharon.” Microsoft Windows NT Server 4.0”. McGraw-Hill.
7. Sánchez Allende, Jesús. López Lérida, Joaquín. Redes (iniciación y referencia). 1ª Edición. Editorial Mac Graw-Hill. Interamericana de España, SAU.
8. Stallings, William. “Comunicaciones y Redes de Computadores”. 7ª edición. Ed. Prentice-Hall. 2004.
9. Stallings, William. Fundamentos de Seguridad de Redes, aplicaciones y estándares. Tercera edición. Prentice Hall
10. Tanenbaum, Andrew S. “Redes de Computadoras”. 4ª Cuarta edición. Ed. Prentice-Hall. 2003

Webgrafia

http://es.wikipedia.org/wiki/Red_de_computadoras (02/03/2011)

http://www.monografias.com/trabajos24/redes-computadoras/redes-computadoras.shtml (02/03/2011)

http://es.wikipedia.org/wiki/Seguridad (05/04/2011)

http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica (05/04/2011)

http://es.wikipedia.org/wiki/Cracker (05/04/2011)

http://es.wikipedia.org/wiki/Script_Kiddie (05/04/2011)

http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf (10/04/2011)

http://gwolf.org/files/seg_en_redes.pdf(15/04/2011)

http://es.wikipedia.org/wiki/Seguridad_en_Internet (15/04/2011)

http://www.eumed.net/cursecon/ecoinet/seguridad/index.htm (16/04/2011)

http://usuarios.multimania.es/janjo/janjo1.html (15/05/2011)

http://www.frm.utn.edu.ar/comunicaciones/tcp_ip.html(15/05/2011)

http://www.monografias.com/trabajos15/arquitectura-tcp/arquitectura-tcp.shtml (20/05/2011)

http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet (20/05/2011)

http://es.wikipedia.org/wiki/Transmission_Control_Protocol (20/05/2011)

http://es.kioskea.net/contents/internet/tcp.php3(20/05/2011)

http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/tcp.html(20/05/2011)

http://es.kioskea.net/contents/internet/udp.php3 (22/05/2011)

http://es.wikipedia.org/wiki/User_Datagram_Protocol(22/05/2011)

http://es.kioskea.net/contents/internet/protip.php3(30/05/2011)

http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html(02/06/2011)

http://es.wikibooks.org/wiki/Redes_inform%C3%A1ticas/Protocolo_IP_en_el_nivel_de_red(02/06/2011)

http://es.wikipedia.org/wiki/Puerta_de_enlace(10/06/2011)

http://www.wikilearning.com/tutoriales/tcp_ip/tematica/845-1(20/06/2011)

http://es.wikipedia.org/wiki/Broadcast_(inform%C3%A1tica) (20/07/2011)

http://es.wikipedia.org/wiki/File_Transfer_Protocol(20/05/2011)

http://en.wikipedia.org/wiki/IPsec(20/08/2011)

ANEXOS

Manual de Usuario

Documento de ayuda al usuario para entender mejor el uso correcto del programa encriptar/desencriptar un archivo.

Elaborado por:

- Imelda Morales
- Juan Bosco Ramírez
- Mauren Somarriba

Información de Versión de la Plataforma:

Windows: 6.1.7600.0 (Win32NT)

Common Language Runtime: 2.0.50727.4952

Identidades

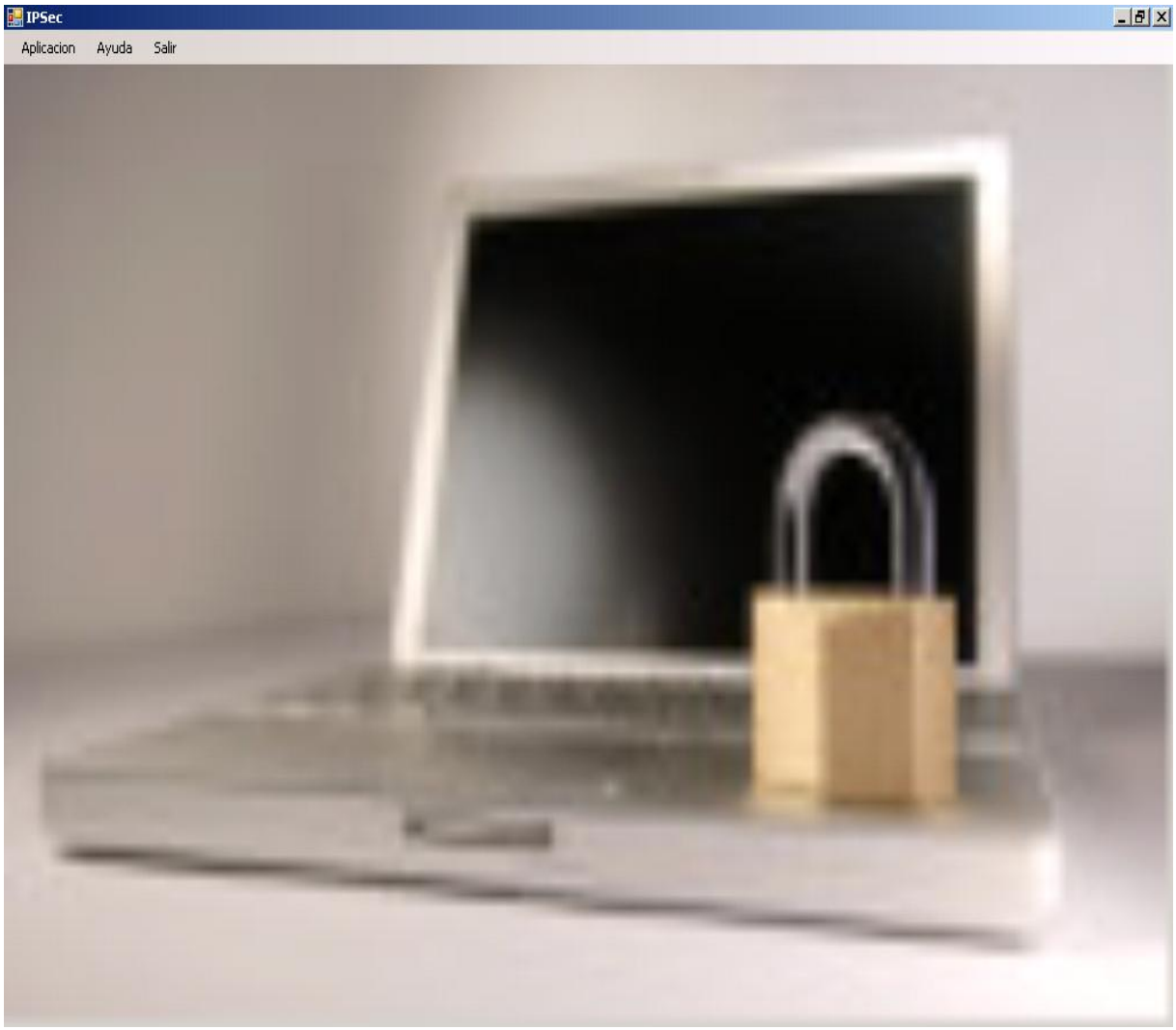
Identidad de la implementación: AlgoritmoSim.application, Versión=1.0.0.1

PROCEDIMIENTOS:

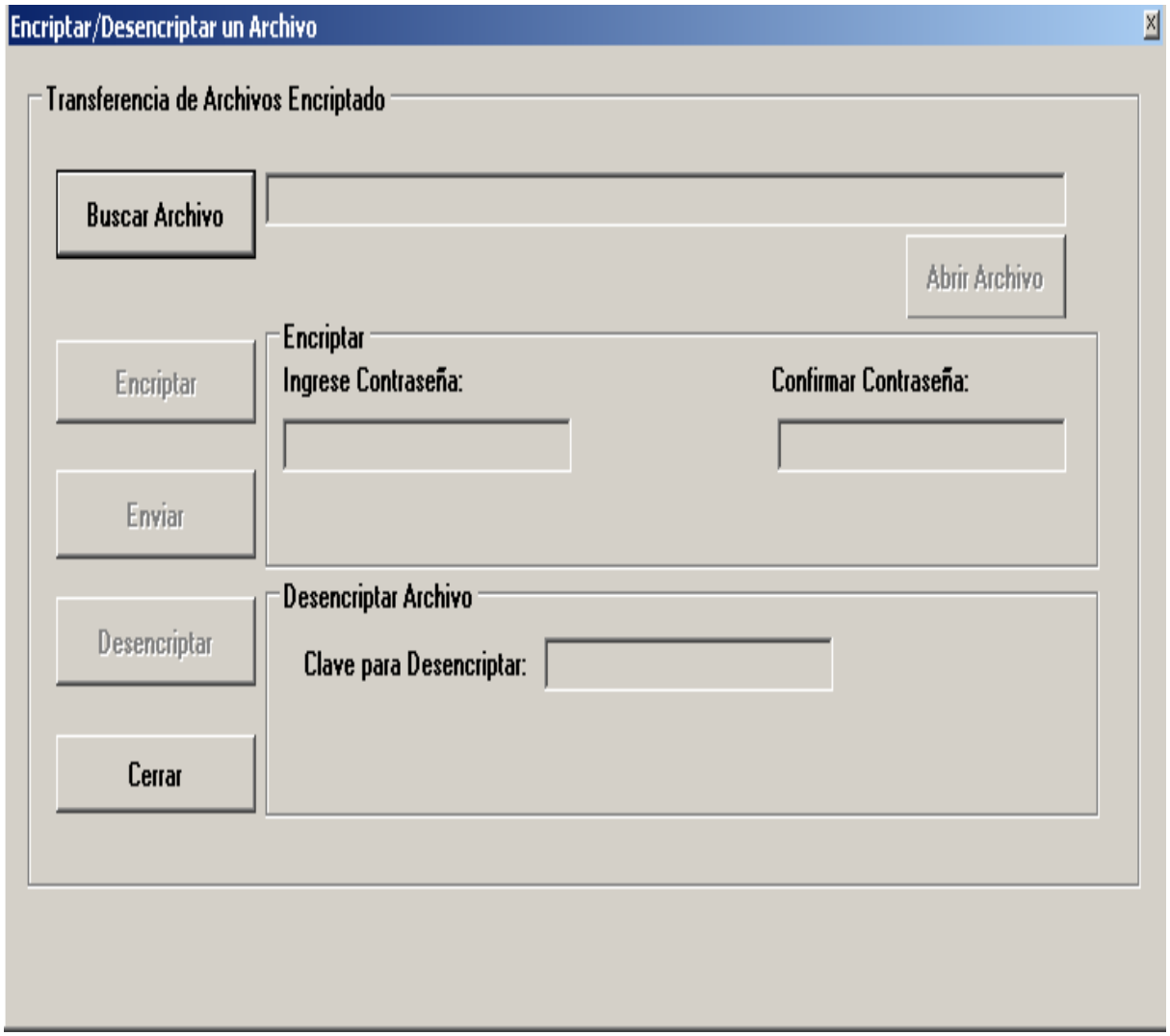
- **Buscar Archivo:** Buscar archivo de cualquier directorio.
- **Encriptar:** Se activa luego de seleccionar el archivo.
- **Ingresar Contraseña:** Se activa luego de activar Encriptar, en esta opción se debe ingresar como mínimo 8 caracteres.
- **Confirmar Contraseña:** Una vez que sea ingresado la contraseña se activa esta opción, su función es para que el usuario no olvide la Contraseña al momento de desencriptar el archivo.
- **Enviar:** Se activa luego de haber ingresado y confirmado la contraseña. Una vez seleccionado esta opción aparece una ventana pidiendo la dirección IP a la que se desea enviar el archivo. En esta opción se transfiere el archivo y al mismo tiempo lo Encripta (cuando se ha ingresado la dirección IP);
- **Desencriptar:** Se activa una vez transferido el archivo, luego de seleccionar esta opción se activa Clave para desencriptar el archivo.
- **Clave para Desencriptar:** Se activa luego de seleccionar Desencriptar, para esta opción se debe ingresar la misma clave con la que se encriptó el archivo.
- **Cerrar:** Salir de la opción Encriptar/Desencriptar Archivos.

VISUALIZACION (PANTALLAS)

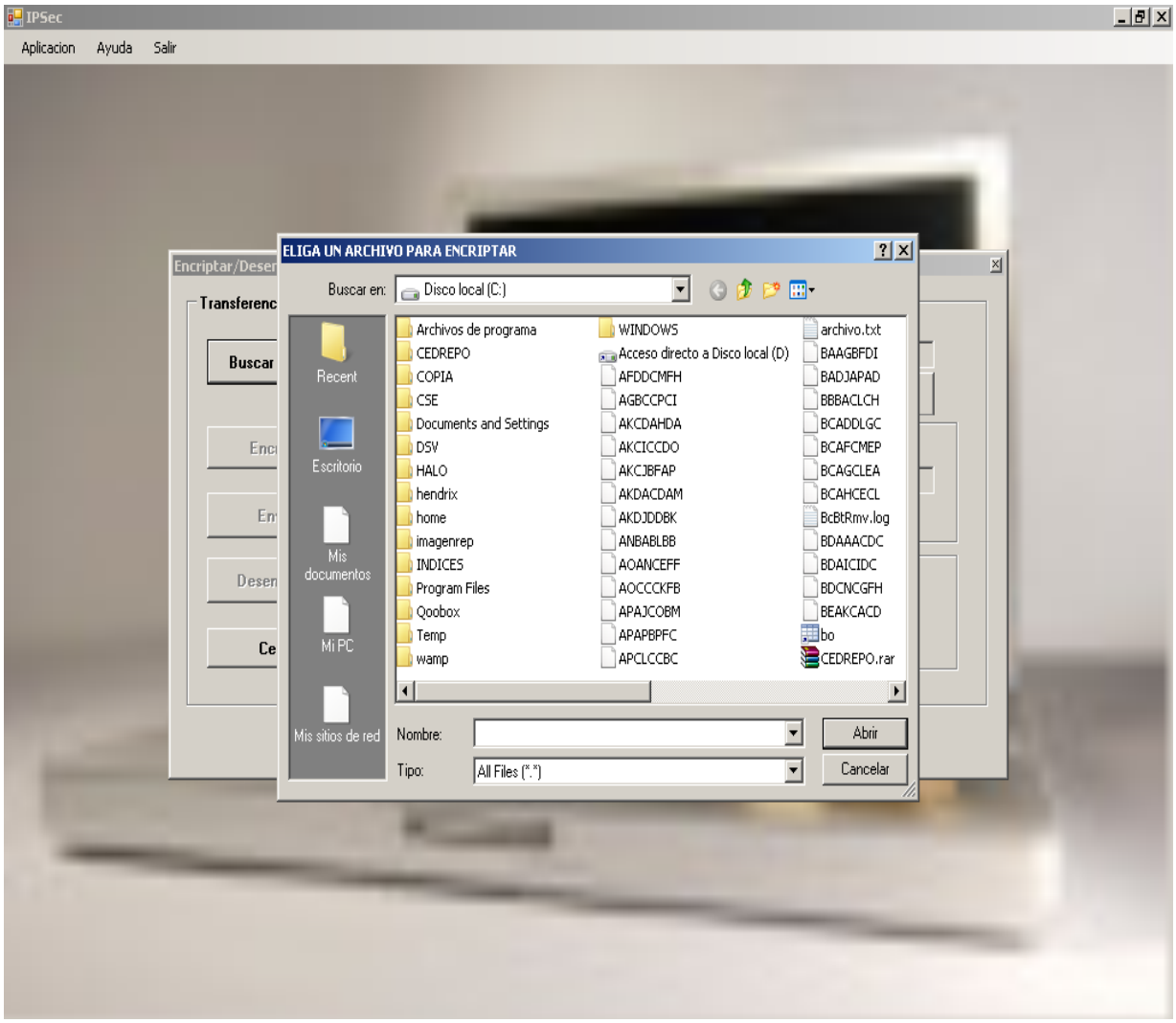
Paso 1: Pantalla de Inicio



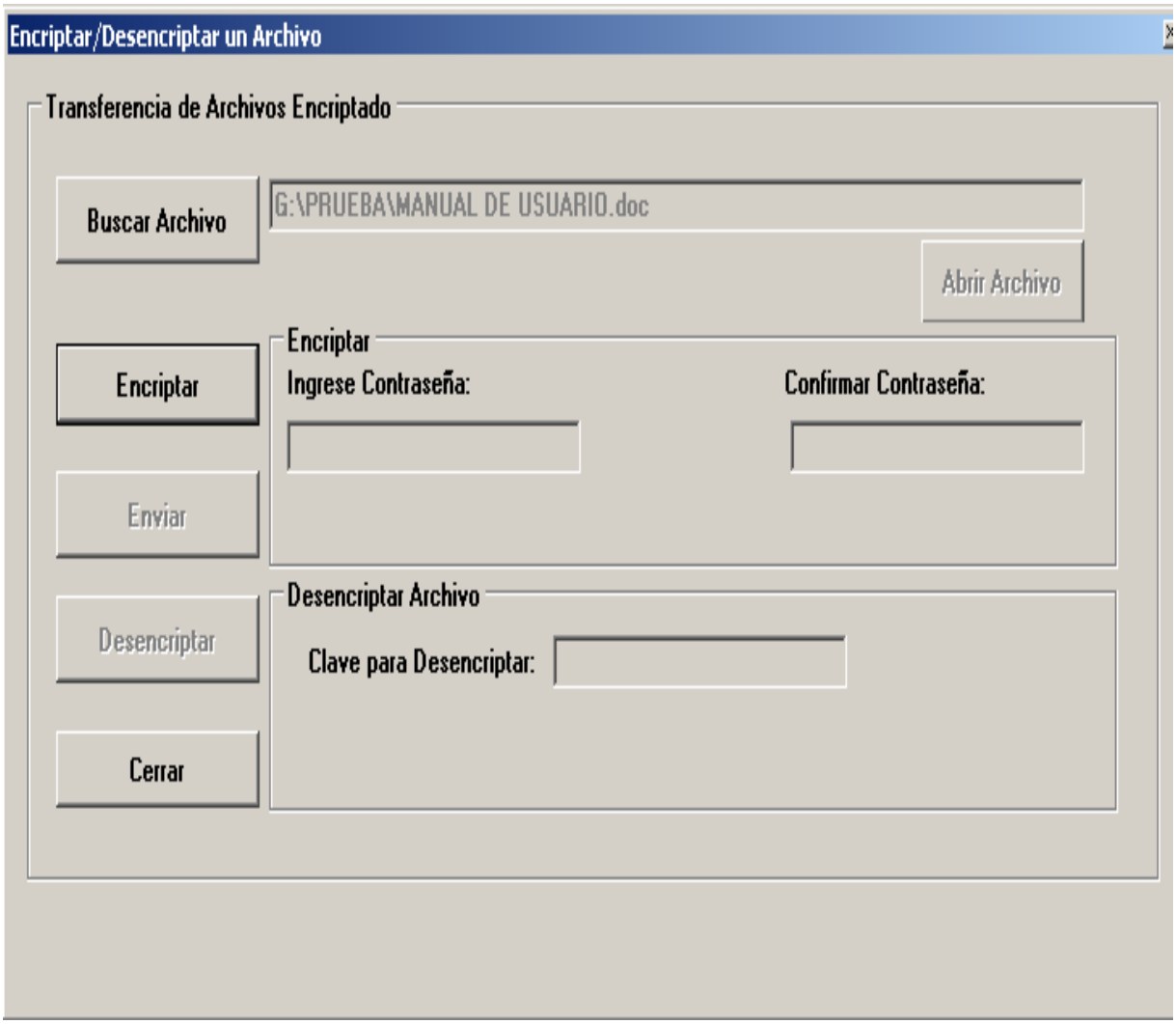
Paso 2: Buscar Archivo



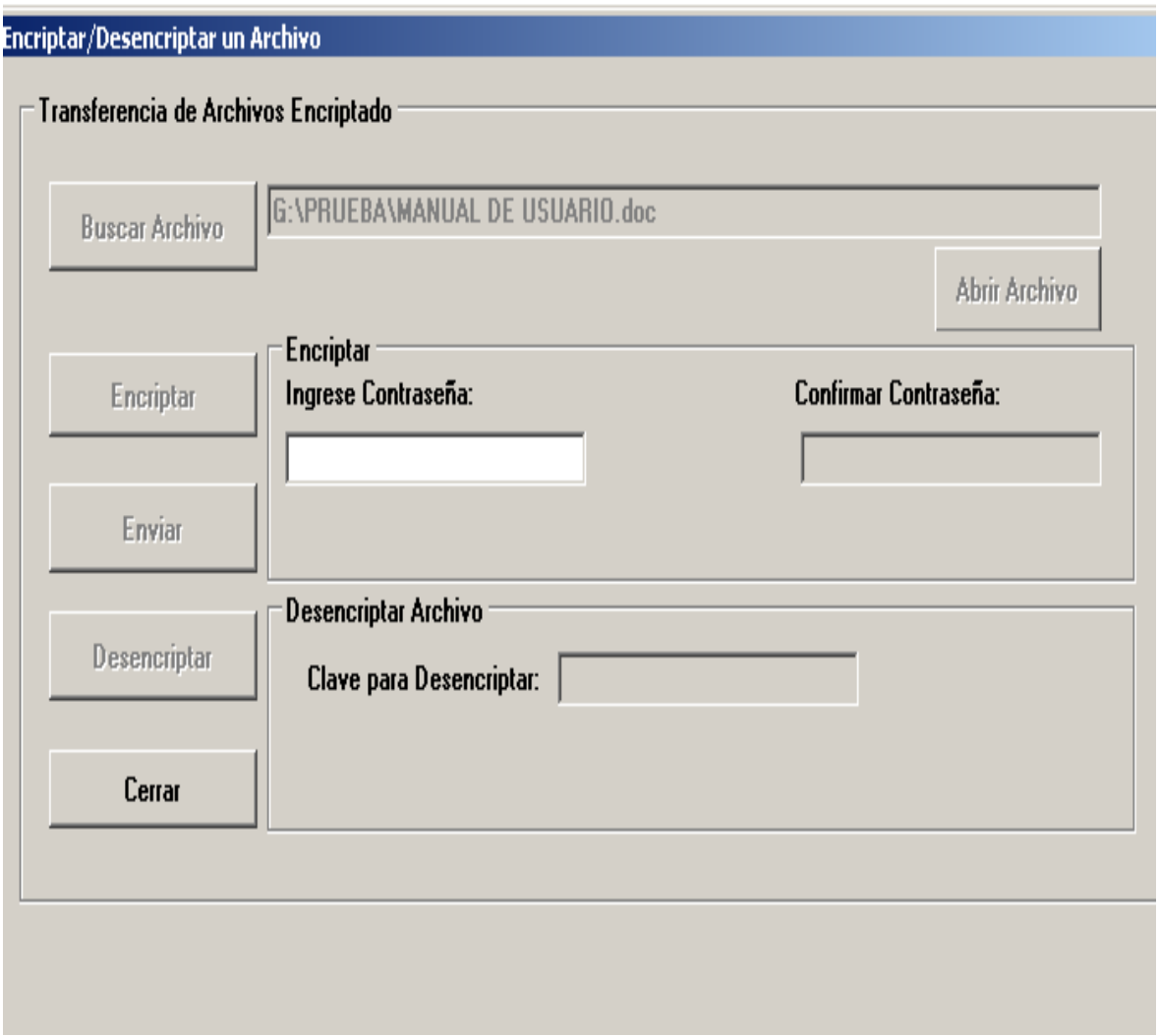
Paso 3: Escoger Archivo



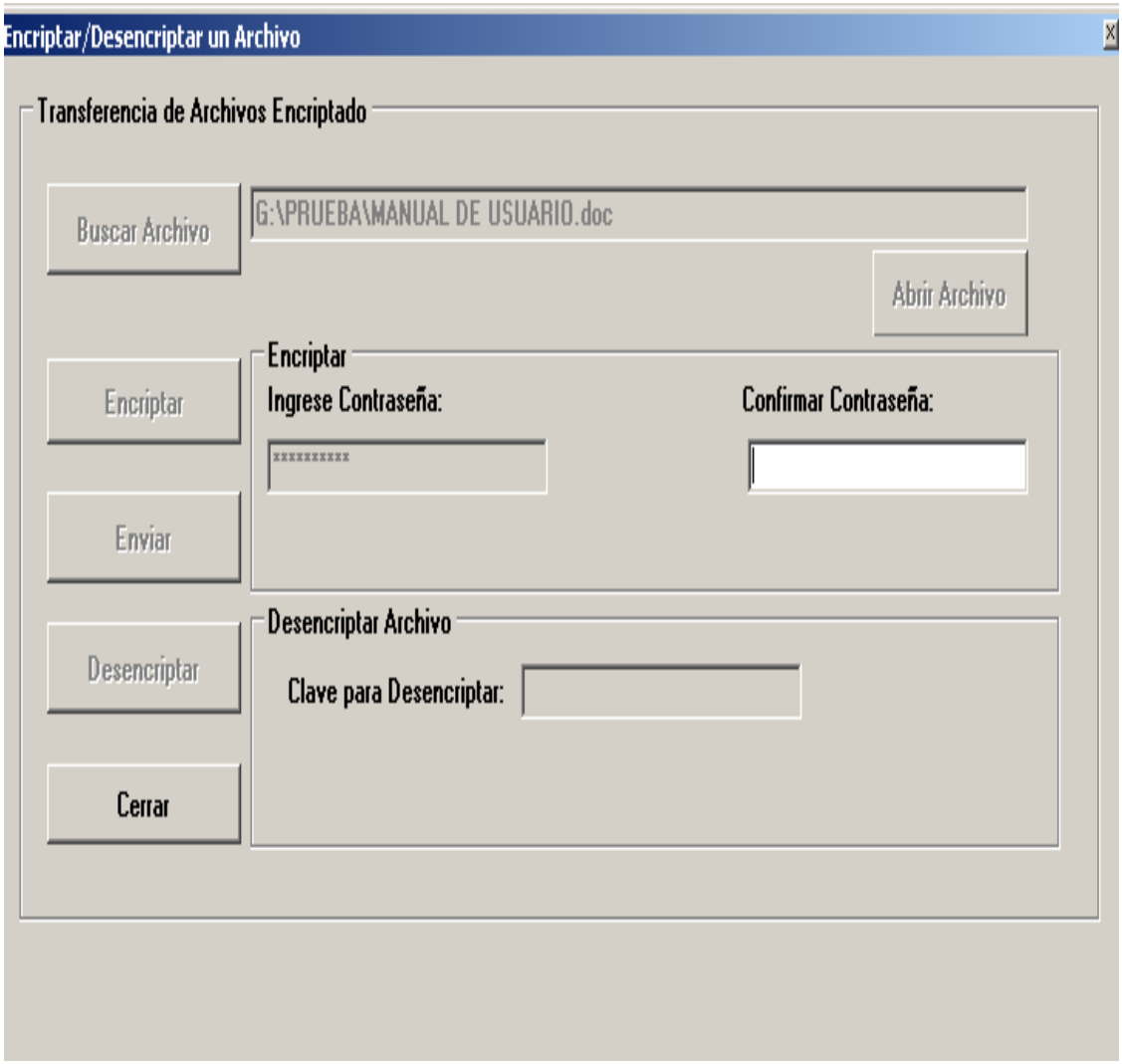
Paso 4: Encriptar Archivo



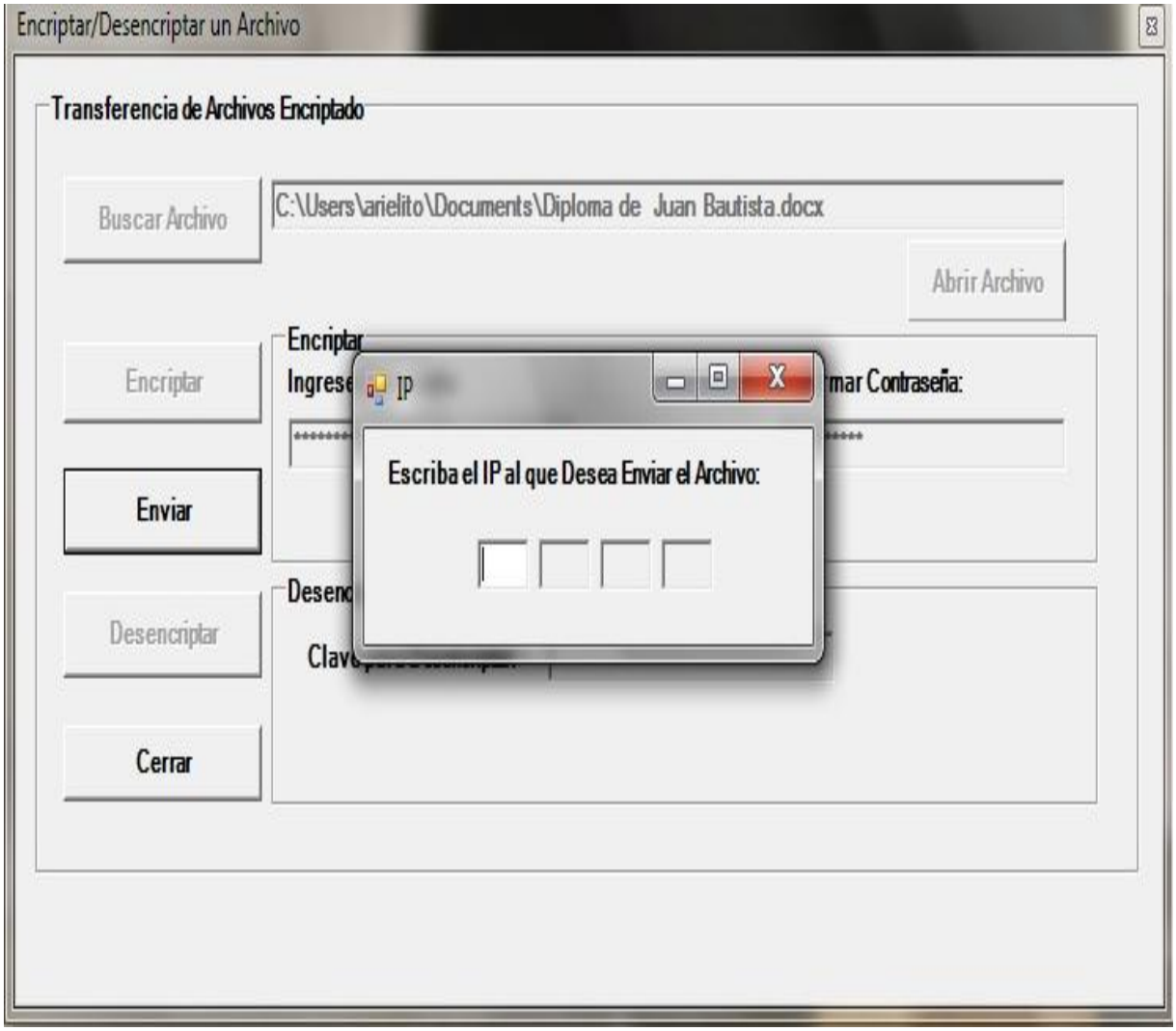
Paso 5: Ingresar Contraseña.



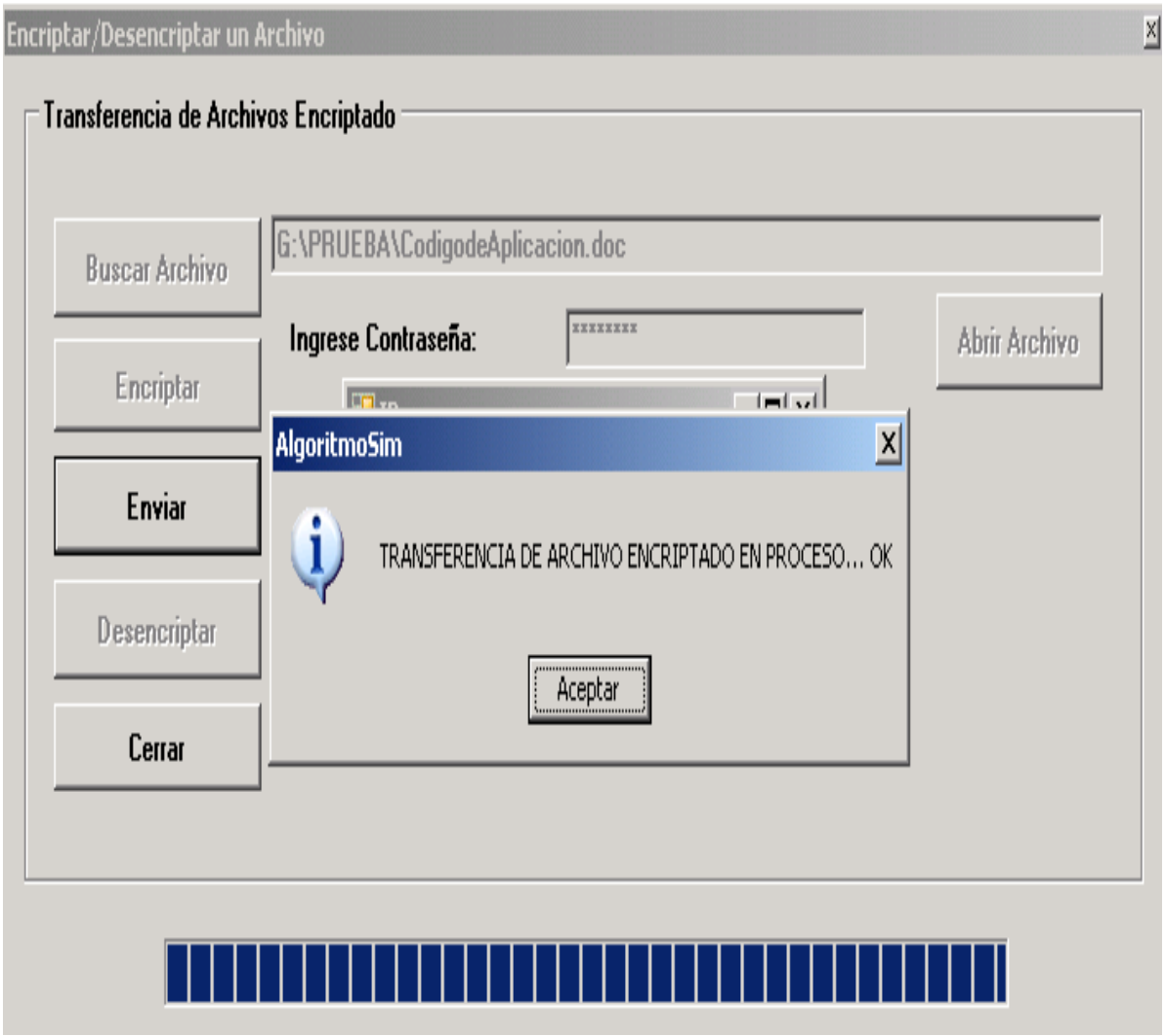
Paso 6: Confirmar contraseña



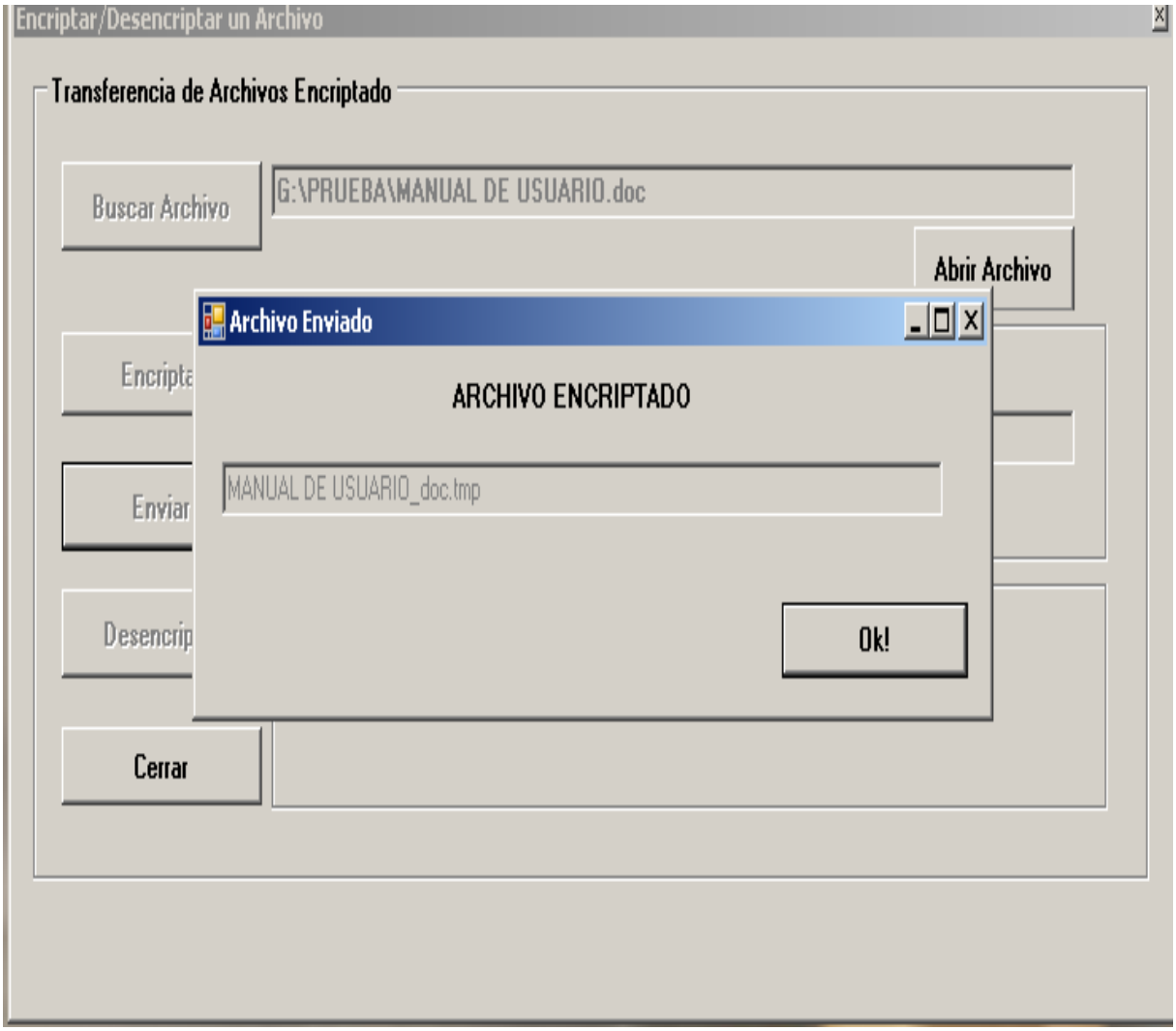
Paso 7: Enviar e Ingresar Dirección IP.



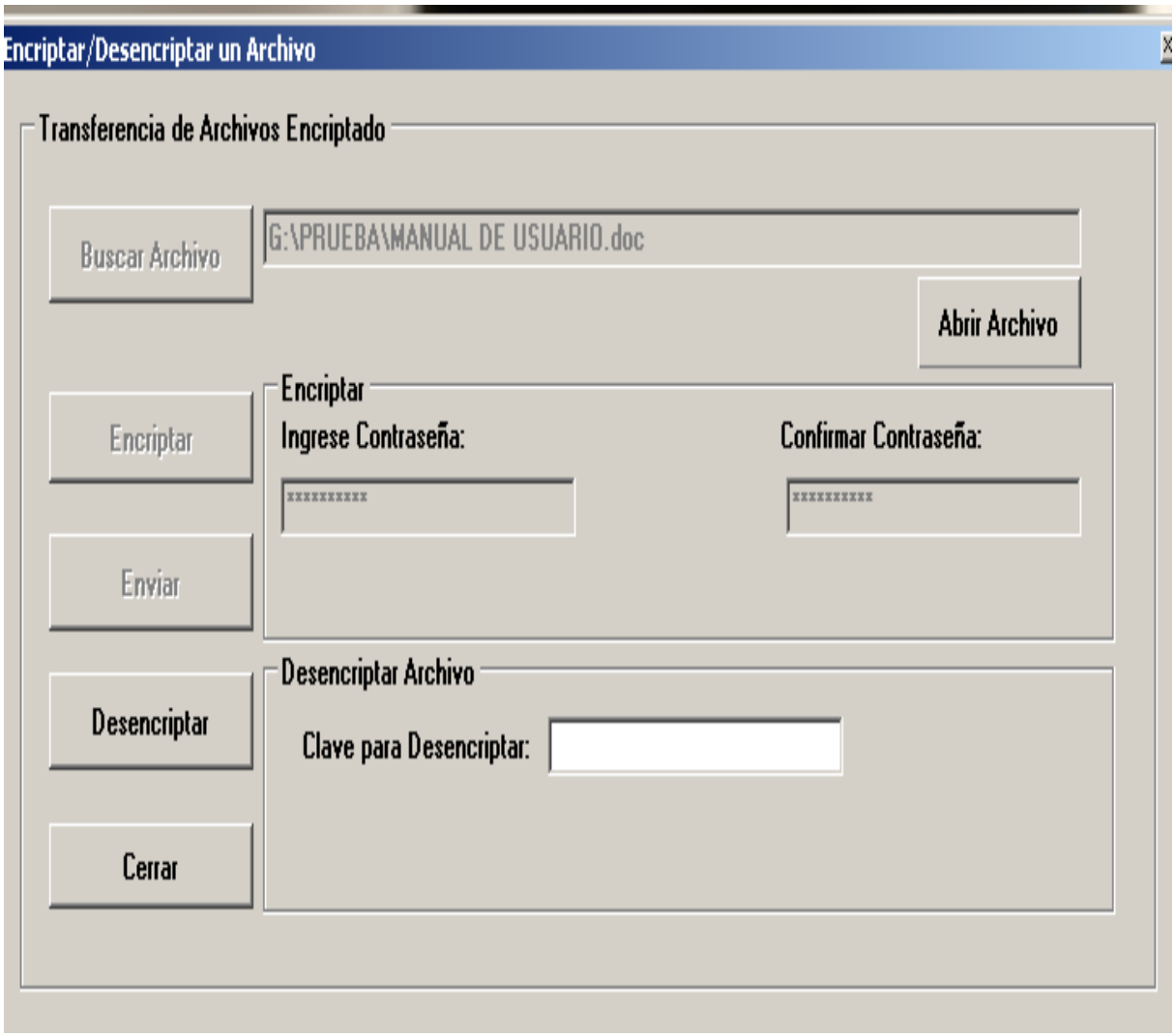
Paso 8: Confirmación, Archivo Transferido.



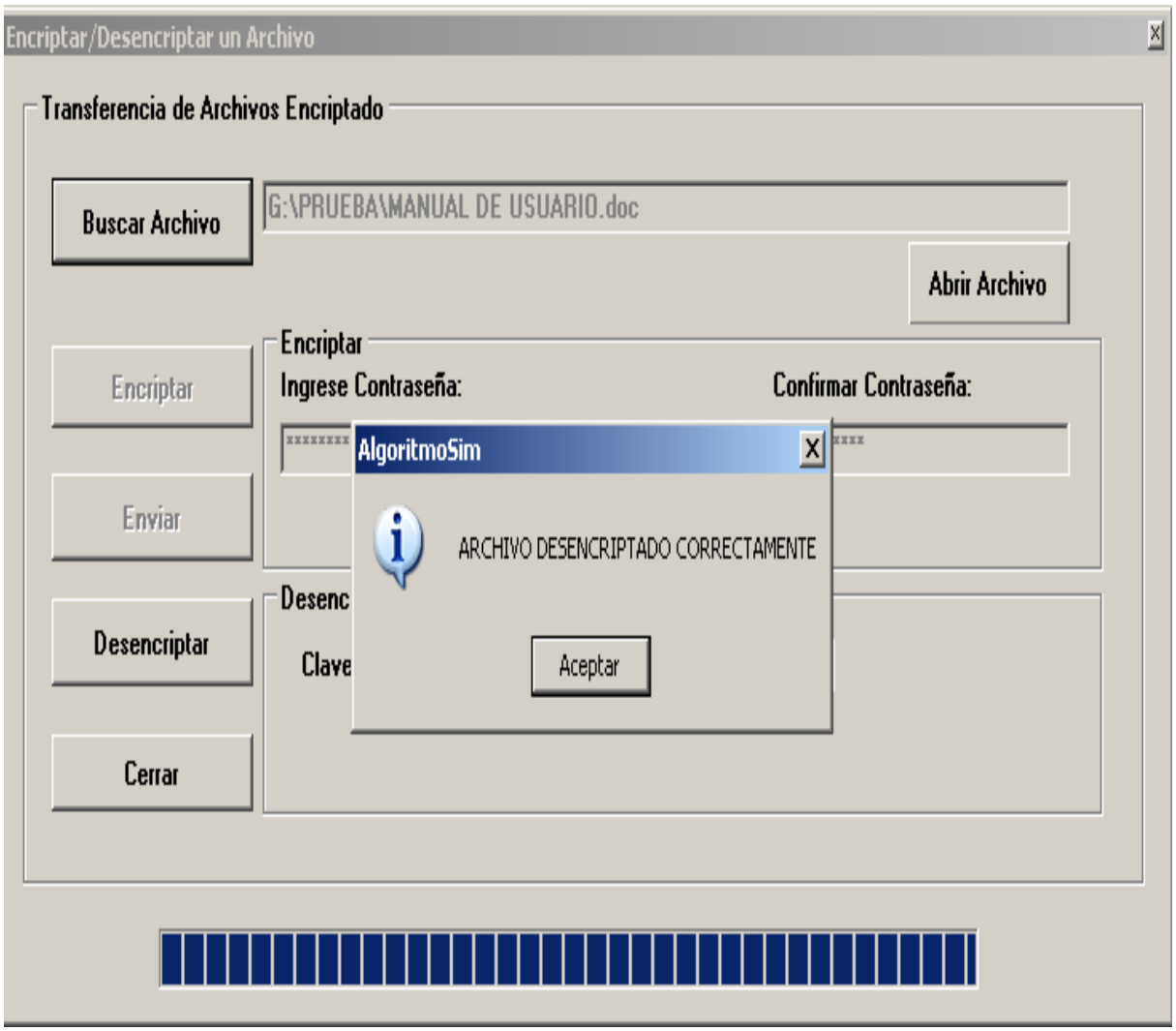
Paso 9: Confirmación Archivo Encriptado.



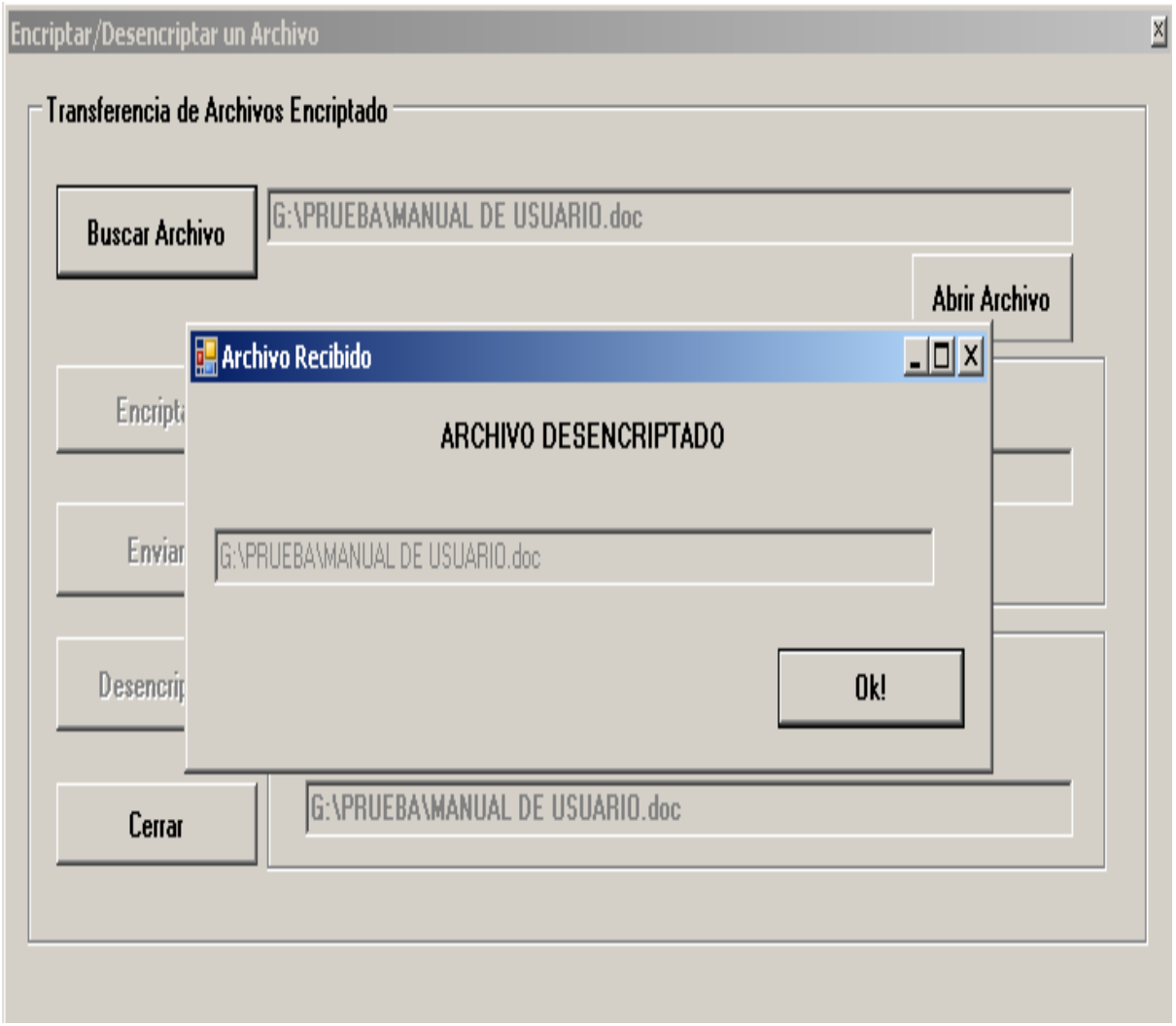
Paso 10: Confirmar Contraseña, para Desencriptar el Archivo.



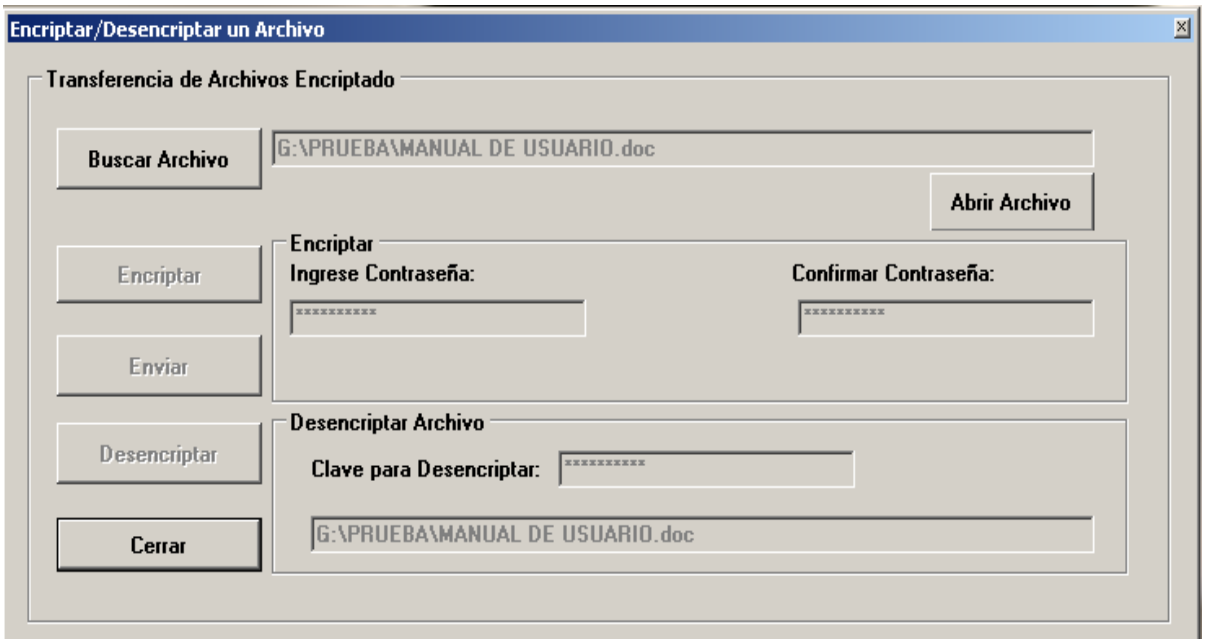
Paso 11: Confirmación Archivo Desencriptado.



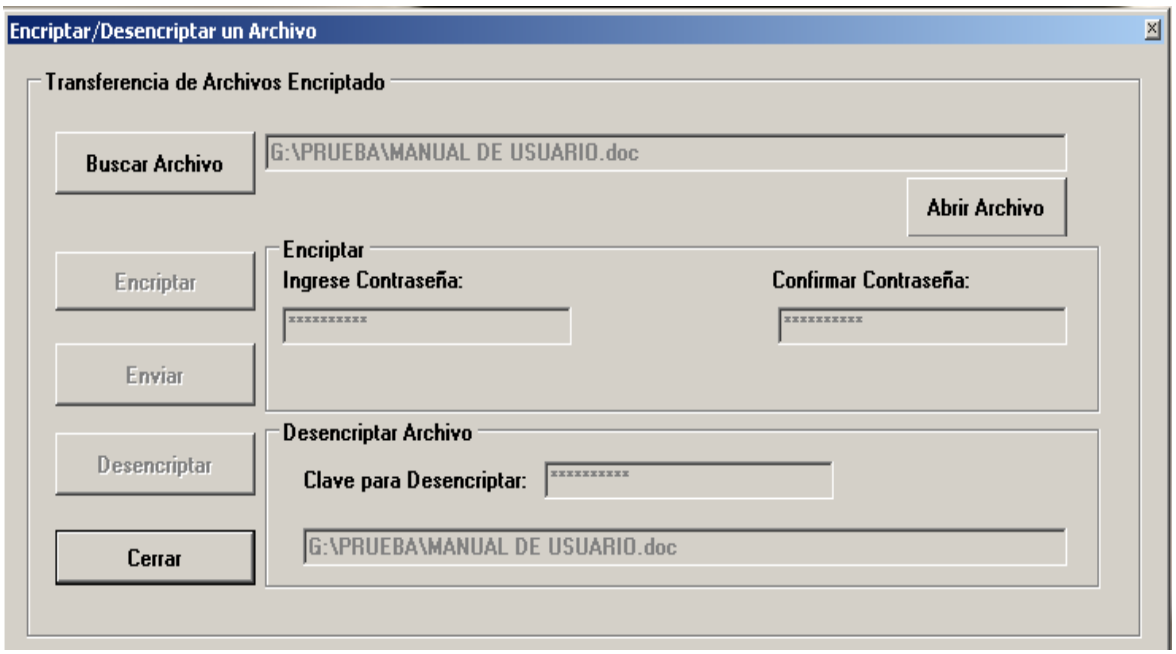
Paso 12: Mensaje Archivo Desencriptado.



Paso 13: Opcional Abrir Archivo Encriptado / Desencriptado.



Paso 14: Cerrar, Salir.



Paso 15: Salir de la Aplicación.

Nota:

- Para ambas opciones Encriptar/Desencriptar; el botón Abrir Archivo se encuentra activo para poder abrir el archivo Encriptado y Desencriptado.
- Cuando el archivo se encuentra Encriptado esta crea una copia con el mismo nombre, agregándole la extensión .tmp (este archivo es temporal).
- Para Desencriptar el Archivo, se selecciona el que tiene extensión .tmp; la pantalla se abre directamente donde se encuentra el archivo.
- Si el usuario da la Opción de Cerrar sin antes de Desencriptar el archivo o si olvidó la contraseña, el archivo original no sufre ninguna modificación, ya que el encriptado es una copia, y por tanto al seleccionar Cerrar este se elimina automáticamente.