**Universidad de San Carlos de Guatemala**
**Facultad de Ingeniería**
**Escuela de Ingeniería en Ciencias y Sistemas**

# SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6

**ERICK FERNANDO LUJÁN MONTES**
**Asesorado por: Ing. Carlos Roberto Iraheta Galicia**

**Guatemala, octubre de 2005.**

**UNIVERSIDAD SAN CARLOS DE GUATEMALA**


FACULTAD DE INGENIERÍA

# SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

**ERICK FERNANDO LUJÁN MONTES**

**Asesorado por: Ing. Carlos Roberto Iraheta Galicia**

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2005

**UNIVERSIDAD SAN CARLOS DE GUATEMALA**


FACULTAD DE INGENIERÍA

**NÓMINA DE JUNTA DIRECTIVA**

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| VOCAL I | |
| VOCAL II | Lic. Amahán Sánches Álvarez |
| VOCAL III | Ing. Julio David Galicia Celada |
| VOCAL IV | Br. Kenneth Issur Estrada Ruiz |
| VOCAL V | Br. Elisa Yazminda Vides Leiva |
| SECRETARIA | Inga. Marcia Ivonne Véliz Vargas |

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

| | |
|---|---|
| DECANO | Ing. Sydney Alexander Samuels Milson |
| EXAMINADOR | Ing. Edgar Estuardo Santos Sutuj |
| EXAMINADOR | Ing. Jose Ricardo Morales Prado |
| EXAMINADOR | Ing. Virginia Victoria Tala Ayerdi |
| SECRETARIO | Ing. Pedro Antonio Aguilar Polanco |

**HONORABLE TRIBUNAL EXAMINADOR**

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6,**

tema que me fuera asignado por la Coordinación de la Carrera de Ciencias y Sistemas en febrero de 2004.

**Erick Fernando Luján Montes**

Guatemala, agosto de 2005

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Privados y
Revisión de Trabajos de Graduación
Presente

Estimado Ingeniero:

Por este medio me permito informarle que he procedido a revisar el trabajo de graduación titulado: **SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6**, elaborado por el estudiante Erick Fernando Luján Montes, y que a mi juicio, el mismo cumple con los objetivos propuestos para su desarrollo.

Agradeciéndole de antemano la atención que le preste a la presente, me suscribo de usted, atentamente,

Carlos Roberto Iraheta Galicia
Col. 6475
Ingeniero en Ciencias y Sistemas
Asesor

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 3 de Mayo de 2005

Ingeniero
**Luis Alberto Vettorazzi España**
**Director de la Escuela de Ingeniería**
**En Ciencias y Sistemas**

Respetable Ingeniero Vettorazzi:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **ERICK FERNANDO LUJAN MONTES**, titulado: **"SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TTCS

*El Director de la Escuela de Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación titulado "SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6", presentado por el estudiante ERICK FERNANDO LUJAN MONTES, aprueba el presente trabajo y solicita la autorización del mismo.*

*ID Y ENSEÑAD A TODOS*


*Ing. Jorge Armin Mazariegos Rabanales*
*DIRECTOR*
*INGENIERIA EN CIENCIAS Y SISTEMAS*

*Guatemala, 24 de octubre del 2005*

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.473.05

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6,** presentado por el estudiante universitario **Erick Fernando Lujan Montes,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, Octubre de 2005

/cdes

## AGRADECIMIENTOS

Dios, creador del universo y dueño de mi vida, que me permite construir otros mundos mentales posibles, de poner en mí camino a las personas más importantes en mi vida.

Mis padres: Sonia Montes, por enseñarme que no hay límites, que lo que me proponga lo puedo lograr y que sólo depende de mi; Fernando Luján quien me infundió la ética y el rigor que guían mi transitar por la vida; gracias padre, por permitirme soñar y crecer con tu imaginación, a ambos por el apoyo incondicional que me dieron a lo largo de la carrera.

Mis hermanos: Brian, por ser un ejemplo y guía en mi camino; Sergio, por su apoyo en todo momento; a ambos, que sin ustedes no estaría aquí.

Mi familia: esto nunca hubiera sido posible sin el amparo incondicional de ellos; sin el amor de cada uno, esto también es vuestro premio.

El Ingeniero Carlos Iraheta, por su asesoría y dirección en el trabajo de investigación.

Mis amigos, en especial a Ana Domínguez, que sin duda alguna, sus consejos, experiencias y sobre todo, su apoyo y paciencia, contribuyeron en todos mis éxitos.

La Facultad de Ingeniería, por el soporte institucional dado para mi formación y por ende al pueblo de Guatemala.

Todas aquellas personas que de una u otra forma, colaboraron o participaron en mi formación como persona y profesional, hago extensivo mi más sincero agradecimiento.

**ACTO QUE DEDICO A**

Mis padres:
Sonia Elizabeth Montes Valenzuela y Luis Fernando Luján Garcia

Mis hermanos:
Brian Alexander Luján Montes y Sergio Geovanny Luján Montes

Mi familia:
A cada uno de ellos…

# ÍNDICE GENERAL

# ÍNDICE DE ILUSTRACIONES

## FIGURAS

## TABLAS

# GLOSARIO

**CA** *Certificate Authority*. Autoridad Certificante que valida certificados.

**CRL** Lista de Certificados Revocados. La autoridad certificadora se encarga de publicar dicha lista, la cual contiene la revocación de un certificado que lo hace inválido.

**D-H** Diffie-Hellman, es un algoritmo de intercambio de claves, se basa en el llamado problema de los logaritmos discretos, que se cree es computacionalmente tan complejo como el de la factorización de números primos.

**DES** *Data Encryption Estándar*. Esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM.

**DSA** *Directory System Agent*. Definido en la norma X.509 que especifica un modelo de conexión de servicios de directorio; dentro del DSA almacenan y mantienen datos de usuarios.

**FIREWALL** Herramienta para proteger una rede de ataques *hackers*.

**FTP** *File Transport Protocol*. Conjunto de reglas de transporte de archivos. Es un proceso que permite el intercambio de archivos entre una computadora local y una remota.

Permite utilizar varios comandos y permite el envío de archivos en ambas direcciones.

**HACKERS** Persona que tiene muchos conocimientos del mundo de las redes. Normalmente se dedican a comprobar la seguridad de las redes, intentando acceder a ellas de forma no autorizada, para examinar los fallos de seguridad y corregirlos.

**HDLC** *High-level Data Link Control*. Control de enlace para datos de alto nivel, protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO; especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación.

**HMAC** *Hashing for Messages Authentication Codes*. Código de autenticación de mensajes que utiliza funciones *hash* de un solo sentido (*One Way*)

**ICMP** *Internet Control Message Protocol*, conjunto de reglas que se utilizan para mantener el control de la información enviada.

**IETF** *Internet Engineering Task Force*. Grupo de trabajo de ingenieros de *Internet*, desarrolladores de estándares de *Internet*.

**IP** *Internet Protocol.* Protocolo de *Internet*; desarrollado 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 del Departamento Estadounidense de Defensa.

**ISO 7498-2** Descripción general de los servicios de seguridad y mecanismos relacionados que pueden ser proporcionados.

**LAN** *Local Area Network*. Red de Area local; red de computadoras limitada a un área inmediata, normalmente un edificio o piso de un edificio.

**MTA** *Message Transfer Agent*. Agente de Transferencia de mensajes, provee enrutamiento de correo electrónico y funciones de envío.

**MD5** *Message Digest* versión 5. Algoritmo de cifrado; toma un mensaje de entrada de longitud arbitraria y entrega una salida de 128 bit de longitud fija, llamado huella digital o Recopilación de mensaje (*Message Digest*).

**MAC** *Mandatory Access Control.* Control de acceso obligatorio; define políticas de seguridad definidas por el administrador y que los usuarios no pueden modificar. Esta política va más allá de establecer propietarios de archivos a que fija contextos, en donde se indica cuándo un objeto puede acceder a otro objeto.

**MAC** *Message Auhentication code*. Código de autentificación de mensaje, es un bloque de datos de tamaño fijo que se envía con un mensaje para investigar su origen e integridad. Son muy útiles para proporcionar autentificación e integridad sin confidencialidad.

**OSI** *Open Systems Interconection*. Interconexión de sistemas abiertos. Es un modelo de referencia que proporciona la base para el desarrollo de estándares relativos a las redes.

**PDU** *Protocol Data Unit*. Unidad de Datos de Protocolo, porción de un paquete de un protocolo determinado, que contiene datos.

**PKCS** *Public-Key Cryptography Standards*. Estandar de encriptación que ofrece un mayor nivel de seguridad.

**QoS** *Quality of Service*. Calidad de Servicio; rendimiento de los servicios con cierto nivel de calidad.

**ROAD WARRIOR** Trabajadores que pasan gran parte del tiempo fuera de la empresa, teletrabajadores, personas que necesitan acceder a la red de la empresa pero que están constantemente cambiando de ubicación.

**RSA** Algoritmo de clave pública creado en 1978 por Rivest, Shamir y Adlman.

**SCEP** Protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados

**SHA** *Secure Hash Algorithm*; algoritmo que utiliza la función *hash*.

**SSL** *Secure Socket Layer*; protocolo de seguridad desarrollado por Netscape, para permitir confidencialidad y autenticación en *Internet*.

**TCP** *Transmisión Control Protocol*; Protocolo de Control de transmisión, protocolo de transporte orientado a conexión.

**TCP/IP** *Transport Control Protocol / Internet Protocol*; conjunto de reglas que se utilizan para enviar información a través de *Internet*; protocolo orientado a la conexión.

**TELNET** Protocolo que permite iniciar una sesión en un sistema remoto.

**TOS** *Type of service*. Tipo de Servicio.

**TLS** *Transport Layer Security*; protocolo de seguridad creado por la *Internet Engineering Task Force* (IETF), que toma como base el SSL y otros protocolos.

**TTL** *Time To Live*. Tiempo de vida; indicación de tiempo durante el cual se considera válido un paquete.

**UDP** *User Datagram Protocol*. Protocolo orientado a la no conexión, no garantiza que todos los paquetes lleguen a su destino.

**VPN** *Virtual Private Network*. Red Privada Virtual; es construida sobre la infraestructura de una red pública. *Internet*.

# RESUMEN

Proteger la información es una de las tareas más importantes; cuando se utiliza el *Internet* se vuelve aún más vulnerable por lo que se necesitan mecanismos de seguridad para protegerla.

Se necesita implementar seguridad, como también el nuevo protocolo IPv6, el cual trabaja con el protocolo IPSec para implementar seguridad y es obligatorio en él. El IPSec está formado por un conjunto de protocolos y algoritmos, que se adaptan a cada caso, pudiendo determinar qué protocolo o algoritmo, según el implementador mejor se adapte, es modular, y con esto logra una adaptación al sistema cambiante.

Este trabajo consta de cuatro capítulos los cuales se describen a continuación.

El capítulo 1 trata sobre la seguridad de la información, los factores, amenazas, vulnerabilidades, ataques y contramedidas relacionadas a la misma, como también la seguridad manejada por cada capa del modelo OSI, criptologia y protocolos de seguridad.

En el capítulo 2 se muestra la seguridad por IP, el protocolo TCP/IP, IPv6, IPSec, sus definiciones, características, componentes. Los cuales son la base para implementar un sistema de seguridad con IPv6 e IPSec.

El capítulo 3 describe el funcionamiento de IPSec como también beneficios que se adquieren al implementarlo. La infraestructura de clave pública y su integración con IPSec. Como también los modos de uso de IPSec y ejemplos de aplicaciones reales donde se maneja seguridad a base de IPSec.

En el capítulo 4 se muestra un análisis de seguridad sobre el protocolo IPSec en IPv6. Este análisis puede utilizar antes de implementar el protocolo IPSec, con esto sabrá qué funcionamientos existen en IPSec para IPv6, los métodos de trabajo, las vulnerabilidades, ventajas y desventajas, como también se señalan las recomendaciones sobre el uso de IPSec en IPv6.

# OBJETIVOS

- **General**

La seguridad en IP con el protocolo IPSec para IPv6.

- **Específicos**

1. Describir la seguridad de la información.
2. Describir los protocolos de seguridad.
3. Definir qué es el IPv6.
4. Definir qué es el IPSec.
5. Describir el funcionamiento de IPSec.
6. Describir los modos de uso y ejemplos de implementación de IPSec.
7. Analizar la seguridad de IPSec en IPv6.
8. Definir las vulnerabilidades, ventajas, desventajas y recomendaciones sobre el uso de IPSec.

# INTRODUCCION

El Internet es un servicio cada día mas utilizado, por lo mismo nos ha dado a la obligación de implementar nuevos mecanismos de seguridad para proteger uno de los recursos mas importantes en él, la información.

Hoy en día existen muchas amenazas sobre nuestra información, por lo que debemos saber como evitarlas y asegurar una transferencia segura de información.

Dado la gran cantidad de información que se maneja en la actualidad se creo un nuevo protocolo, el ipv6, llamado también Internet 2. El IPV6 trabaja con distintos protocolos uno de ellos IPSec el cual sirve para implementar la seguridad. El IPSec esta formado por un conjunto de protocolos y algoritmos que habilitan un sistema para seleccionar los protocolos de seguridad requeridos, determinar los algoritmos a utilizar para cada servicio y colocar las llaves criptológicas requeridas.

El IPSec esta actualmente implementado en ipv4 y en ipv6, para este último es obligatoria la implementación. En una red de comunicaciones nos encontramos con diferentes problemas de seguridad dentro de ellos cabe destacar la autenticación, la integridad, el repudio y la confiabilidad, por lo cual implementar el protocolo IPSec resuelve estos problemas.

El IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP. Los componentes principales de la arquitectura de seguridad IPSec son, protocolo de seguridad, asociaciones de seguridad, manejo de clave y algoritmos de autenticación y encriptación.

Ademas IPSec ofrece un conjunto de servicios de seguridad, control de acceso, donde en el se previene el uso no autorizado de recursos, integridad sin conexión, cuando se modifica un datagrama IP individual esto lo detecta, autenticación del origen de los datos, protección antireplay, este detecta la integridad de una secuencia parcial, como también datagramas IP duplicados, encriptación y encriptación de flujo de trafico limitado.

IPSec posibilita a las aplicaciones un acceso seguro y transparente, hace el comercio electrónico mas seguro, permite tener una red segura sobre redes publicas, a los teletrabajadores ofrece el mismo nivel de confidencialidad que dispondría en la red local de su empresa.

# 1. SEGURIDAD Y PROTOCOLOS DE SEGURIDAD

## 1.1 Seguridad de la información

Cuando se habla de la seguridad de información generalmente se tiende a hablar de nueva tecnología, de nuevas aplicaciones, nuevos dispositivos hardware y nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo esta basado en tecnología moderna, para esto se debe conocer que la información:

- Esta es almacenada y procesada en computadoras
- Puede ser confidencial para algunas personas o a escala institucional
- Puede ser mal utilizada o divulgada
- Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y lo s últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que hoy se sufre un accidente en el centro de computo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Por tal motivo la seguridad es una prioridad clave, dado que la comunicación y la información se han convertido en un factor esencial del desarrollo social y económico. Las redes y los sistemas de información transmiten datos y ofrecen servicios, para todo eso su funcionamiento es fundamental e indispensable. Las redes son cada vez más convergentes y son capaces de servir de soporte a los mismos servicios, cada vez están más interconectadas y comparten parte de la misma infraestructura.

Las empresas, los ciudadanos y las administraciones públicas desean sacar el máximo partido de las posibilidades que ofrecen las redes de comunicación, por lo que la seguridad de estos sistemas es de suma importancia.

La seguridad de la red y de la información puede entenderse como la capacidad de un sistema de información para resistir, con un determinado nivel de confianza, los efectos de accidentes o actos malintencionados.

Tales sucesos o acciones podrían poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de datos almacenados o

transmitidos, y de los servicios relacionados ofrecidos a través de estas redes y sistemas. Estos incidentes de seguridad pueden agruparse del siguiente modo:

La comunicación electrónica puede ser interceptada y los datos copiados y modificados.

- Se pueden causar daños tanto por invasión de la privacidad de los individuos como por el uso indebido de los datos interceptados.

- El acceso no autorizado a ordenadores y redes de ordenadores se hace a menudo de forma malintencionada con el fin de copiar, modificar o destruir datos.

- Los ataques a *Internet* se han hecho bastante corrientes y en el futuro las redes telefónicas se pueden hacer más vulnerables.

- Programas malintencionados, como virus, pueden averiar los ordenadores, borrar o modificarlos datos.

- Algunos ataques recientes han sido particularmente destructivos y costosos.

- Las declaraciones falsas en nombre de personas o entidades podrían causar daños substanciales. Por ejemplo, los usuarios podrían descargar programas malintencionados de un sitio Web que se hace pasar por una fuente fiable, se podrían invalidar contratos o enviarse información confidencial a la persona equivocada.

- Muchos incidentes de seguridad se deben a acontecimientos imprevistos y no intencionados como catástrofes naturales (inundaciones, tormentas, terremotos), fallos del soporte físico o lógico y errores humanos.

La definición del estándar ISO 7498-2 [ISO, 1989] define cinco elementos básicos que constituyen la seguridad de un sistema: la confidencialidad de los datos, la autenticación de los datos, la integridad de los datos, el control de acceso (disponibilidad) y el no repudio.

Confidencialidad implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. Para poder tener acceso a los datos de manera segura la autenticación define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora. Integridad implica que los datos no han sido modificados o corrompidos de manera alguna desde su transmisión hasta su recepción. El control de acceso establece la forma en que el recurso está disponible cuando es requerido. El no repudio es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos:

1. Seguridad física: un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc.
2. Seguridad de procedimientos: elemento enfocado a las medidas de protección en los procesos y procedimientos.

3. Seguridad de personal: elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.
4. Seguridad de emanación de compromisos: elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.
5. Seguridad de sistemas operativos: elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.
6. Seguridad de comunicaciones: elemento enfocado a la transmisión segura de información a través de medios de comunicación.

Prevención es la palabra clave en Seguridad, se han desarrollado una gran diversidad de técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere, son este tipo de esfuerzos el objeto de estudio de este trabajo.

## 1.2 Factores que intervienen en la Seguridad Informática.

Existen varios factores que influyen en la seguridad informática los cuales se pueden dividir en cuatro grupos:

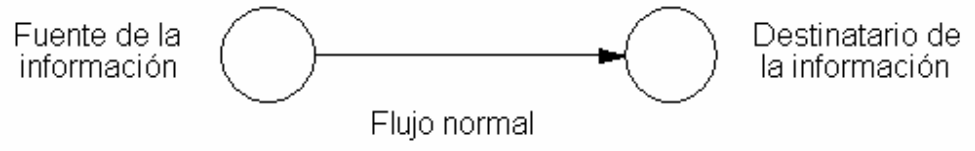
- Amenazas
- Vulnerabilidades
- Ataques
- Contramedidas

### 1.2.1 Amenazas

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

La siguiente figura modela un sistema, como un flujo de información.

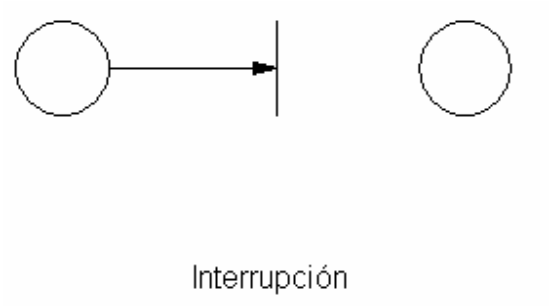
**Figura 1.** Flujo normal de comunicación




Las cuatro categorías generales de ataques son las siguientes:

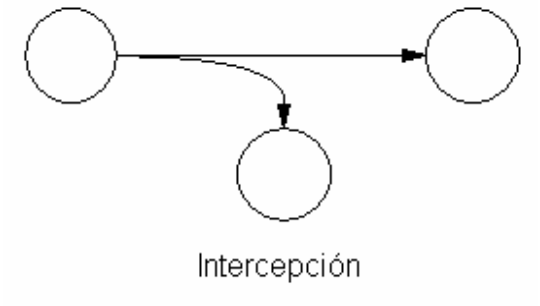
- **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

**Figura 2.** Flujo con interrupción de comunicación




- **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

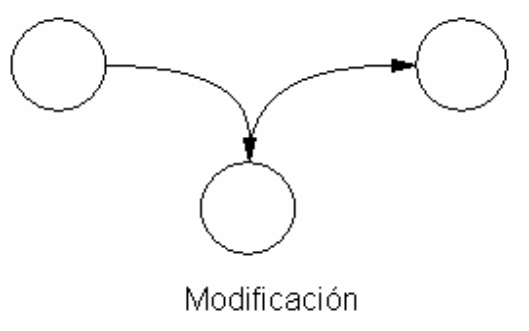
**Figura 3.** Flujo con intercepción de comunicación




- **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma

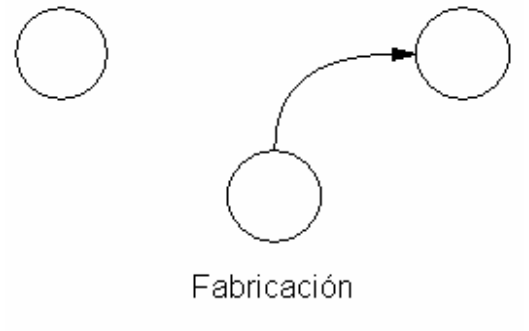
diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

**Figura 4.** Flujo con modificación de comunicación




- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

**Figura 5.** Flujo con fabricación de comunicación




Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

### 1.2.2 Vulnerabilidades

Todo software es realizado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

### 1.2.3 Ataques

Se entiende como ataque a medios por los cuales se explotan las vulnerabilidades, donde se aprovecha dicha para vulnerabilidad para realizar los dos tipos de ataques, ataques pasivos y ataques activos.

#### 1.2.3.1 Activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa un millón de pesetas en la cuenta A” podría ser modificado para decir “Ingresa un millón de pesetas en la cuenta B”.

- **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, *Web*, FTP, etc.

#### 1.2.3.2 Pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

### 1.2.4 Contramedidas

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos.

Todas estas contramedidas se pueden generar después del análisis de riesgo. Un análisis de riesgo es un proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo de la prevención de esta pérdida.

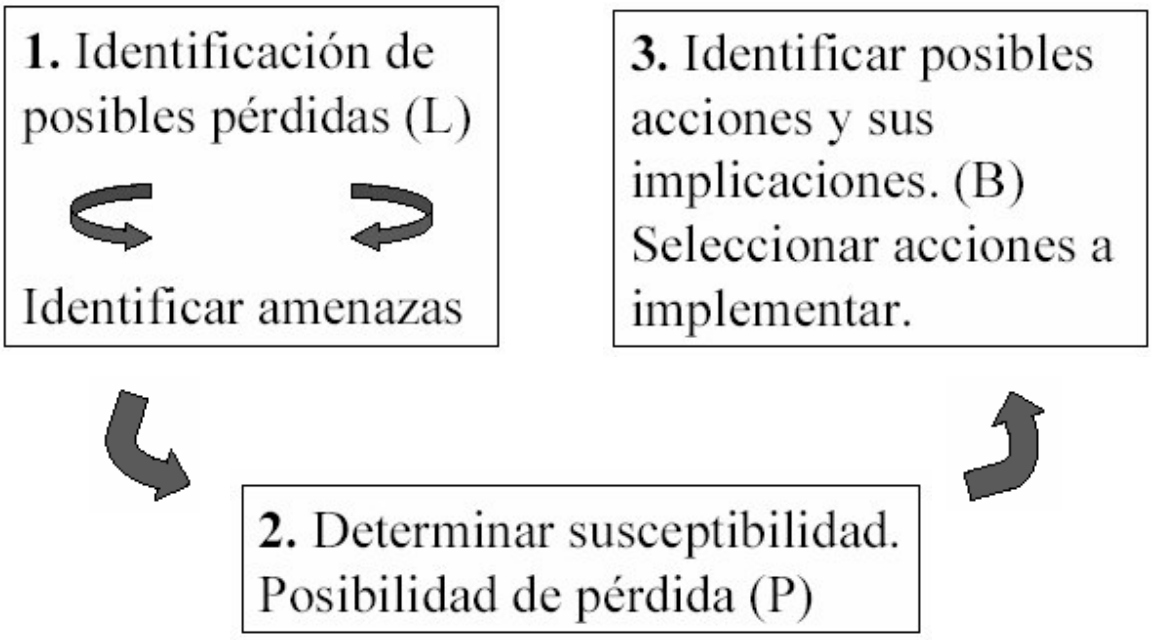
Su análisis no sólo lleva a establecer un nivel adecuado de seguridad, permite conocer mejor el sistema que vamos a proteger.

La información que se obtiene en un análisis de riesgos es la siguiente:

- Determinación precisa de los recursos sensibles de la organización.
- Identificación de las amenazas del sistema.
- Identificación de las vulnerabilidades específicas del sistema.
- Identificación de posibles pérdidas.
- Identificación de la probabilidad de ocurrencia de una pérdida.
- Derivación de contramedidas efectivas.
- Identificación de herramientas de seguridad.
- Implementación de un sistema de seguridad eficiente en costes y tiempo.

La siguiente figura nos muestra los pasos del análisis de riesgos:

**Figura 6.** Pasos para un análisis de riesgos



## 1.3 Modelo OSI y Seguridad por Capas

### 1.3.1 Modelo OSI

El modelo OSI (*Open Systems Interconection*), Interconexión de sistemas abiertos), es utilizado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red.

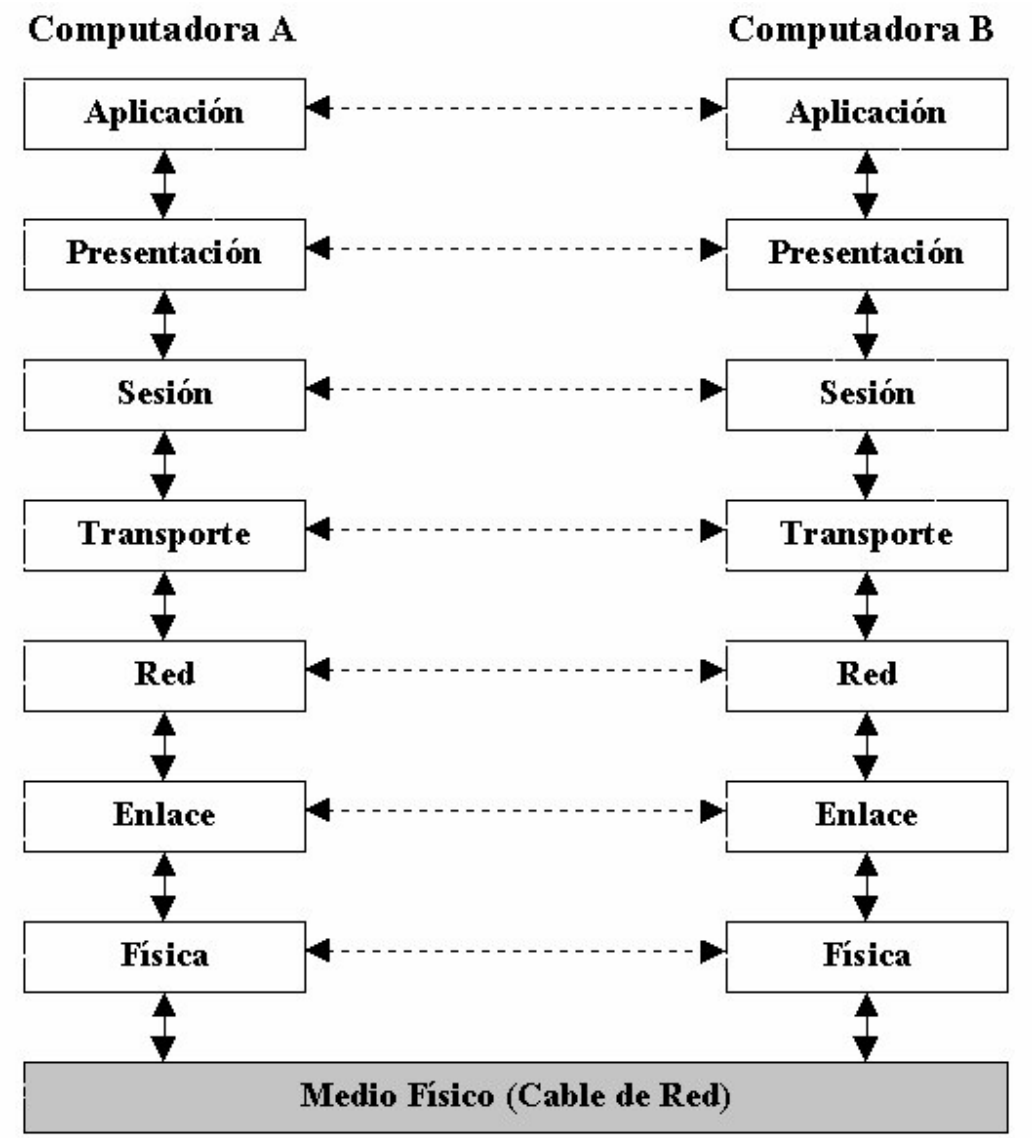
**Figura 7.** Capas del modelo OSI


Como se muestra en la figura, las capas OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red están en la parte de abajo, mientras las funciones que atienden los detalles de las aplicaciones del usuario están arriba.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los

servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de la misma computadora.

**Figura 8.** Relación entre capas del modelo OSI



Con esta última figura se puede apreciar que a excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su contraparte en la otra computadora. La información que envía una computadora debe de pasar por todas las capas inferiores, La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información.

Por ejemplo, si la capa de red envía información desde la computadora A, esta información se mueve hacia abajo a través de las capas de Enlace y Física del lado que envía, pasa por el cable de red, y sube por las capas de Física y Enlace del lado de el receptor hasta llegar a la capa de red de la computadora B.

La interacción entre las diferentes capas adyacentes se llama interfase. La interfase define que servicios la capa inferior ofrece a su capa superior y como esos servicios son accesados. Además, cada capa en una computadora actúa como si estuviera comunicándose directamente con la misma capa de la otra computadora. La serie de las reglas que se usan para la comunicación entre las capas se llama protocolo.

Así mismo, el desarrollo de protocolos esta basado en los servicios definidos en las capas de comunicación del modelo estándar OSI, para entender apropiadamente las características de los protocolos de seguridad y su intervalo de aplicación, se ha elaborado una marco de trabajo que esquematiza una relación entre los servicios y las capas de protocolos.

En la tabla I, se puede apreciar los servicios proporcionados por cada capa de red.

**Tabla I**. Servicios de seguridad en las capas del modelo OSI

| Servicio de Seguridad | Capa Física | Capa de Enlace | Capa de Red | Capa de Transporte | Capa de Sesión | Capa de Presentación | Capa de Aplicación |
|---|---|---|---|---|---|---|---|
| Autenticación de entidad extremo (*Peer Entity*) | | | SI | SI | | | SI |
| Autenticación del origen de los datos | | | SI | SI | | | SI |
| Servicios de Control de acceso | | | SI | SI | | | SI |
| Confidencialidad de la conexión | SI | SI | SI | SI | | | SI |
| Confidencialidad orientada a no conexión | | SI | SI | SI | | | SI |
| Confidencialidad de un campo selectivo | | | | | | SI | SI |
| Confidencialidad del flujo de tráfico | SI | | SI | | | | SI |
| Integridad orientada a no conexión | | | SI | SI | | | SI |
| Integridad de un campo selectivo | | | | | | | SI |
| Origen, no repudio | | | | | | | SI |
| Recepción, no repudio | | | | | | | SI |

Nos podemos dar cuenta que conforme vamos avanzando desde la capa física nos encontramos que solo presenta dos servicio de seguridad, de igual manera la capa de enlace. La capa de red con siete servicios de seguridad soportados y transporte solo con seis. La capa de sesión con ninguno, la capa de presentación con un servicio, en la capa de aplicación es la que presenta todos los servicios de seguridad.

### 1.3.2 Capa física

Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio y especifica bits de control, mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto mecánico de la internase física.
- Describir el aspecto eléctrico de la internase física.
- Describir el aspecto funcional de la internase física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.
- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

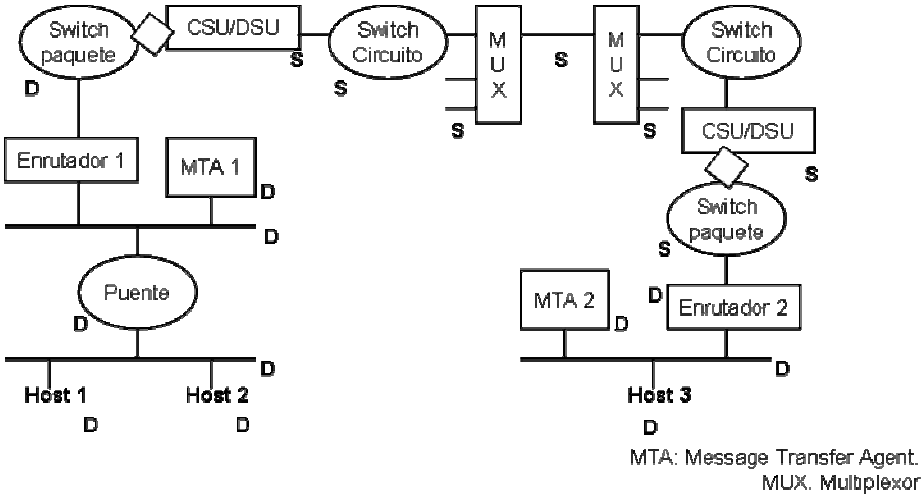
En esta capa se tiene una dependencia significativa de la tecnología de red que se utilice. El equipo y todo lo demás cambia si hay modificación de tecnología de comunicación: Ethernet, SDH, SONET, etc.

Los servicios de seguridad son:

- Confidencialidad (incluyendo confidencialidad del flujo de trafico), no se provee servicio, pero se da soporte a las capas superiores para control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es individual o a nivel de circuitos conmutados.

En la Figura 9 se esquematiza un escenario común de componentes de capa física, se distinguen con la letra S aquellos componentes con capacidad de protección de datos y cifrado, y con la letra D aquellos que son los puntos débiles por proteger.

**Figura 9.** Ejemplo de seguridad en la capa física en una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 34.

### 1.3.3 Capa de enlace

Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información.

Todo esto para:

- Detectar errores en el nivel físico.-
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.

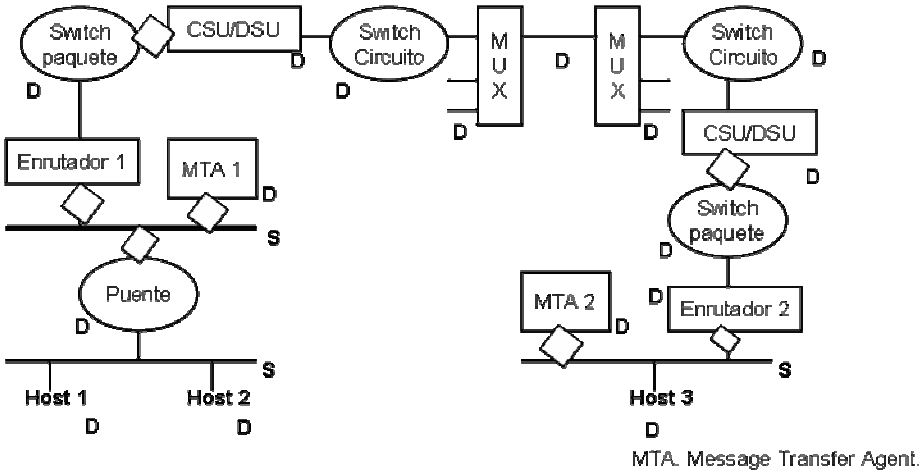
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes. Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.
- En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

Los servicios de seguridad son:

- Confidencialidad, control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es en los *hosts* individuales y en los segmentos de la *LAN*.

En la Figura 10 se esquematiza un escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

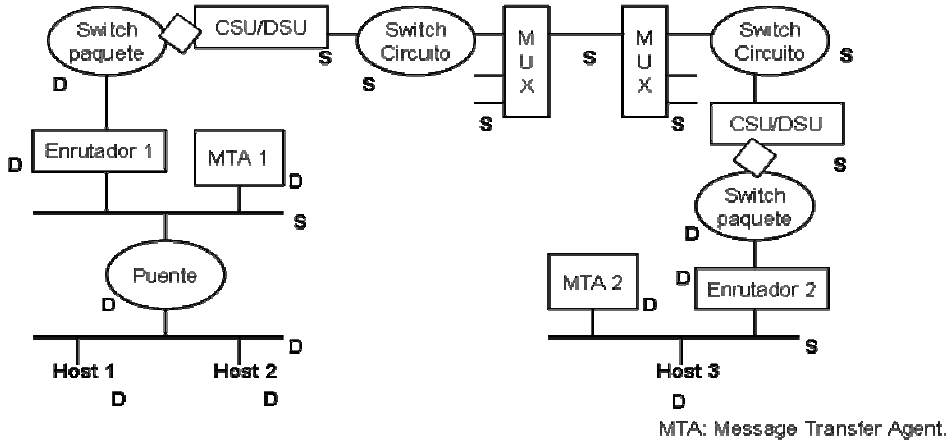
**Figura 10.** Ejemplo de seguridad en la capa de enlace en una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 35.

En la Figura 11, se muestra la conjunción de los ejemplos de la capa 1 y 2, se aprecia su complemento y necesidad de aplicación de seguridad en las capas superiores.

**Figura 11.** Ejemplo de seguridad en las capas física y de enlace en una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 35.

### 1.3.4 Capa de red

Este nivel define varios puntos a tomar en cuenta:

- Define el enrutamiento y el envío de paquetes entre redes.
- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

Podemos dividir este nivel en dos capas para mayor comprensión, las cuales son: Capa de Red Inferior y Capa de Red Superior.

- **Capa de red inferior:**

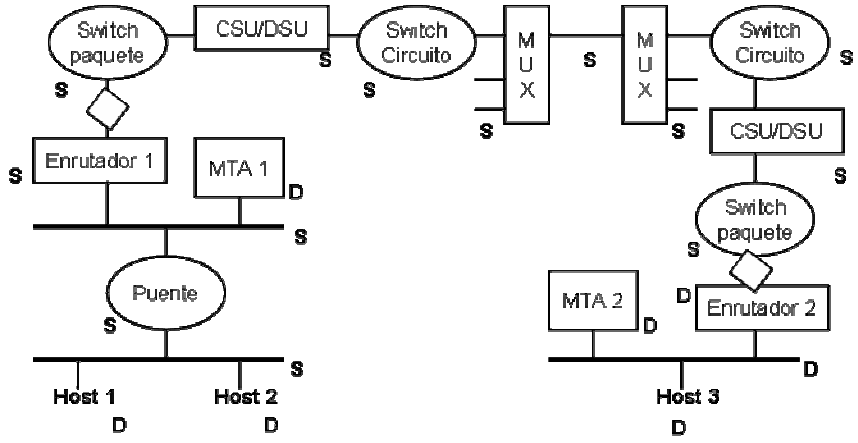
En la subcapa inferior de esta capa se tiene una alta dependencia de la tecnología de red y menor sobre el conjunto de protocolos que se utilicen.

Los servicios de seguridad son:

- Confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a conexión y a no conexión (dependiente de la red). La granularidad de protección radica en los *hosts* (por conexión) y en el enrutador (*LAN*).

En la Figura 12 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

**Figura 12.** Ejemplo de seguridad en la capa de red inferior en una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 36.

- **Capa de red superior:**

En la subcapa superior de esta capa no se tiene dependencia de la tecnología de red, aunque sí moderada sobre el conjunto de protocolos que se utilicen (el tunelaje de IP disminuye esto considerablemente).

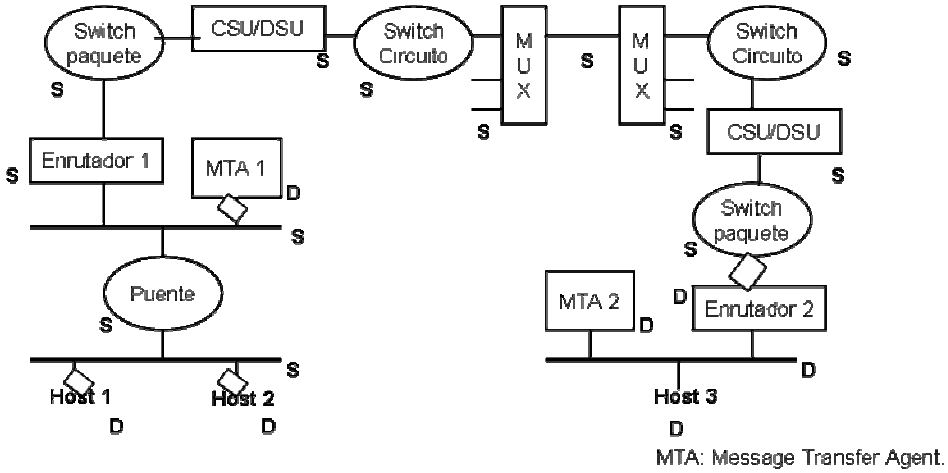
Los servicios de seguridad son:

- Confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a no conexión y a secuencia parcial. La granularidad de protección radica en los *hosts*, en la red o seguridad de calidad de servicio (QoS).

En la Figura 13 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos

componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

**Figura 13.** Ejemplo de seguridad en la capa de red superior de una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 37.

### 1.3.5 Capa de transporte

Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a el procesamiento. Además, garantiza una entrega confiable de la información.

Este nivel define varios puntos a tomar en cuenta:

- Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).
- Este nivel define como direccionar la localidad física de los dispositivos de la red.

- Asigna una dirección única de transporte a cada usuario.
- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

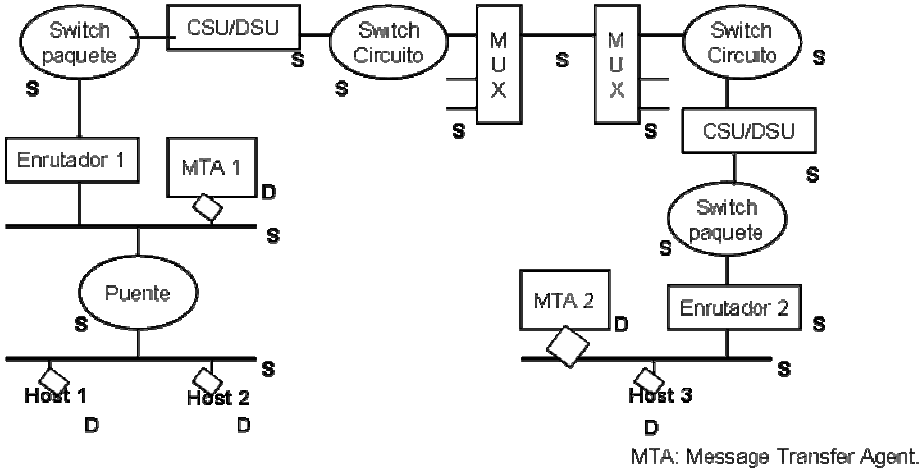
En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice.

Los servicios de seguridad son:

- confidencialidad, control de acceso, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a no conexión e integridad orientada a conexión con recuperación de datos. La granularidad de protección radica en los *hosts* por conexión.

En la Figura 14 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

**Figura 14.** Ejemplo de seguridad en la capa de red superior de una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 38.

### 1.3.6 Capa de sesión

Proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos.

Este nivel define varios puntos a tomar en cuenta:

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

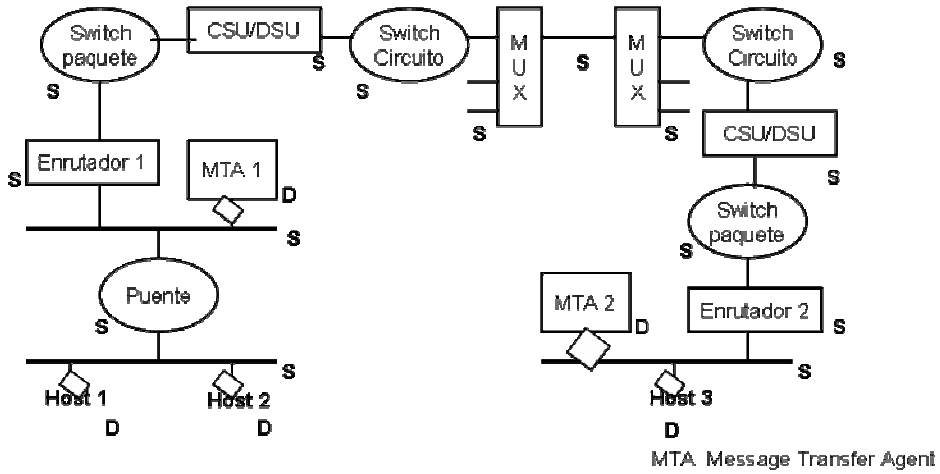
En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice.

Los servicios de seguridad son:

- Integridad orientada a conexión, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a conexión y control de acceso. La granularidad de protección radica en las sesiones.

En la Figura 15 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

**Figura 15.** Ejemplo de seguridad en la capa de sesión de una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 34.

### 1.3.7 Capa de aplicación

Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.

Proporciona aspectos de comunicaciones para aplicaciones especificas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

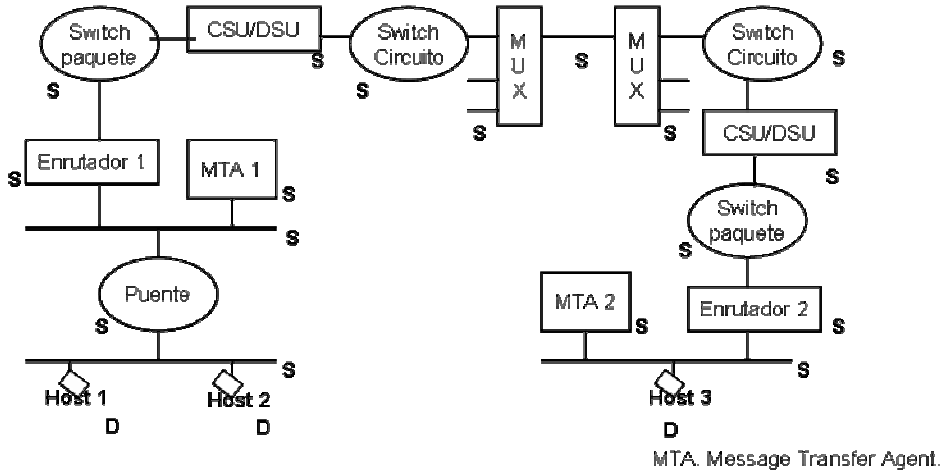
En esta capa no se tiene dependencia de la tecnología de red. La dependencia es significativa sobre las aplicaciones.

Los servicios de seguridad son:

- Confidencialidad (orientado a conexión, a no conexión, o a un campo selectivo), autenticación del origen de los datos, autenticación de la entidad extremo, integridad (orientada a conexión y a no conexión, con opción a recuperación) y no repudio (en el origen y recepción). La granularidad de protección radica en los usuarios, aplicaciones y PDUs (*Protocol Data Unit*).

En la Figura 16 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

**Figura 16.** Ejemplo de seguridad en la capa de presentación de una red de paquetes




Fuente: Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec.** Pagina 39.

## 1.4 Criptología

En el mundo real, si alguna persona quiere proteger los expedientes de sus alumnos los guardará en un armario ignífugo, bajo llave y vigilado por guardias, para que sólo las personas autorizadas puedan acceder a ellos para leerlos o modificarlos; si queremos proteger nuestra correspondencia de curiosos, simplemente usamos un sobre; si no queremos que nos roben dinero, lo guardamos en una caja fuerte.

Pero la tecnología va avanzando y esos métodos anteriores se utilizan cada vez menos, con base a redes disponemos de todas estas medidas que nos parecen habituales, y una forma de protección va a venir de la mano de la criptografía.

El cifrado de los datos nos va a permitir desde proteger nuestro correo personal para que ningún curioso lo pueda leer, hasta controlar el acceso a

nuestros archivos de forma que sólo personas autorizadas puedan examinar (o lo que quizás es más importante, modificar) su contenido, pasando por proteger nuestras claves cuando conectamos a un sistema remoto o nuestros datos bancarios cuando realizamos una compra a través de *Internet*.

La criptología (del griego krypto y logos, estudio de lo oculto, lo escondido) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones para nuestro caso una red de computadoras.

Esta ciencia está dividida en dos grandes ramas:

- La criptografía, ocupada del cifrado de mensajes en clave y del diseño de criptosistemas.
- El criptoanálisis, que trata de descifrar los mensajes en clave, rompiendo así el criptosistema.

La criptografía en la actualidad se puede ver en multitud de software y hardware destinado a analizar y monitorizar el tráfico de datos en redes de computadoras; si bien estas herramientas constituyen un avance en técnicas de seguridad y protección, su uso indebido es al mismo tiempo un grave problema y una enorme fuente de ataques a la intimidad de los usuarios y a la integridad de los propios sistemas.

Aunque el objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente la privacidad o confidencialidad de los datos, sino que se busca además garantizar la autenticidad de los mismos (el emisor del mensaje es quien dice ser, y no otro),

su integridad (el mensaje que leemos es el mismo que nos enviaron) y su no repudio (el emisor no puede negar el haber enviado el mensaje).

Los algoritmos criptográficos proveen confidencialidad de datos al convertir un mensaje (texto plano) en garabatos (cibertexto) y visceversa.

### 1.4.1 Criptosistemas

Cuando el emisor emite un texto en claro, que es tratado por un cifrador con la ayuda de una cierta clave, creando un texto cifrado (criptograma). Este criptograma llega al descifrador a través de un canal de comunicaciones, como una red y este convierte el criptograma de nuevo en texto claro, apoyándose ahora en otra clave, esta clave puede o no ser la misma que la utilizada para cifrar. Este texto claro ha de coincidir con el emitido inicialmente para que se cumplan los principios básicos de la criptografía moderna: en este hecho radica toda la importancia de los criptosistemas.

Es obvio, a la vista de lo expuesto anteriormente, que el elemento más importante de todo el criptosistema es el cifrador, que ha de utilizar el algoritmo de cifrado para convertir el texto claro en un criptograma. Usualmente, para hacer esto, el cifrador depende de un parámetro exterior, llamado clave de cifrado (o de descifrado, si hablamos del descifrador) que es aplicado a una función matemática irreversible, al menos, computacionalmente, no es posible invertir la función a no ser que se disponga de la clave de descifrado.

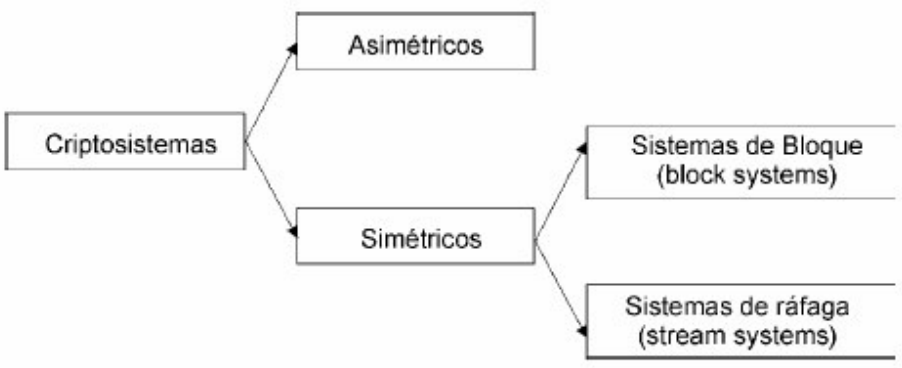
De esta forma, cualquier conocedor de la clave y por supuesto, de la función, será capaz de descifrar el criptograma, y nadie que no conozca dicha clave puede ser capaz del descifrado, aún en el caso de que se conozca la función utilizada.

La gran clasificación de los sistemas de criptografía se hace en función de la disponibilidad de la clave de cifrado/descifrado. Existen, por tanto, dos grandes grupos de criptosistemas:

- Criptosistemas de clave pública o asimétricos
- Criptosistemas de clave secreta o simétricos

Como lo muestra la siguiente figura.

**Figura 17.** Clasificación de Criptosistemas




#### 1.4.1.1 Simétricos

Denominamos criptosistema de clave secreta (de clave privada, de clave única o simétrico) a aquel criptosistema en el que la clave de cifrado puede ser calculada a partir de la de descifrado y viceversa. En la mayoría de estos sistemas, ambas claves coinciden, y por supuesto han de mantenerse como un secreto entre emisor y receptor: si un atacante descubre la clave utilizada en la comunicación, ha roto el criptosistema.

Hasta la década de los setenta, la invulnerabilidad de todos los sistemas dependía de este mantenimiento en secreto de la clave de cifrado. Este hecho presentaba una gran desventaja: había que enviar, aparte del criptograma, la clave de cifrado del emisor al receptor, para que éste fuera capaz de descifrar el mensaje. Por tanto, se incurría en los mismos peligros al enviar la clave, por un sistema que había de ser supuestamente seguro, que al enviar el texto plano. De todos los sistemas de clave secreta, el único que se utiliza en la actualidad es DES (*Data Encryption Standard*).

Por si esto no fuera suficiente, el hecho de que exista al menos una clave de cifrado/descifrado entre cada dos usuarios de un sistema haría inviable la existencia de criptosistemas simétricos en las grandes redes de computadores de hoy en día: para un sistema de computación con usuarios, se precisarían claves diferentes, lo cual es obviamente imposible en grandes sistemas. Todos estos motivos han propiciado que el estudio de los cifradores simétricos (excepto DES) quede relegado a un papel histórico.

Los sistemas de cifrado de clave única se dividen a su vez en dos grandes grupos de criptosistemas:

- Cifradores de flujo, que son aquellos que pueden cifrar un sólo bit de texto claro al mismo tiempo, y por tanto su cifrado se produce bit a bit,

- Cifradores de bloque, que cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una única unidad.

#### 1.4.1.2 Asimétrico

Los criptosistemas de clave pública o asimetricos, la clave de cifrado se hace de conocimiento general, se le llama clave pública. Sin embargo, no ocurre lo mismo con la clave de descifrado, clave privada, que se ha de mantener en secreto. Ambas claves no son independientes, pero del conocimiento de la pública no es posible deducir la privada sin ningún otro dato.

Tenemos pues un par clave pública-clave privada; la existencia de ambas claves diferentes, para cifrar o descifrar.

Cuando un receptor desea recibir una información cifrada, ha de hacer llegar a todos los potenciales emisores su clave pública, para que estos cifren los mensajes con dicha clave. De este modo, el único que podrá descifrar el mensaje será el legítimo receptor, mediante su clave privada.

Asi también estos se dividen en dos:

- Algoritmos de bloque (Block) que no poseen memoria interna, los mismos bloques utilizados para el texto plano son siempre relacionados a los bloques del cibertexto.

- Los sistemas de ráfaga (Stream) poseen memoria interna, los bloques del texto plano, no siempre son transformados a bloques idénticos de cibertexto.

## 1.5 Protocolos de seguridad

Dentro del contexto del modelo de interconexión OSI, podemos darnos cuenta en la tabla II, algunos de los protocolos de criptografía más utilizados y reconocidos como estándares por la IETF.

La parte mas importante con respecto al trabajo de investigación es la capa 3, capa de red, como se describe en los objetivos, en particular AH y ESP que son parte del conjunto de protocolos denominado IPSec.

**Tabla II.** Capas y protocolos de criptografía

| Capa | Nombre | Protocolos |
|---|---|---|
| 7 | Aplicación | X.400, MSP, X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves. |
| 6 | Presentación | |
| 5 | Sesión | SSL |
| 4 | Transporte | TLSP |
| 3 | Red | NLSP,ESP,AH |
| 2 | Enlace de datos | SILS |
| 1 | Física | Enlace síncrono |

A continuación se detallaran los protocolos más importantes así como los relacionados con el objetivo del trabajo.

### 1.5.1 *Secure Socket Layer* (SSL)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en *Internet*. SSL opera como una capa adicional entre *Internet* y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos.

Solicitud de SSL:

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciéndo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio.

Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el SSL *Handshake*.

SSL *Handshake*:

Durante el hanshake se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL.

Los pasos que se siguen son los siguientes:

- *Client Hello*: El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio.. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define como cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

- *Server Hello*: El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algorítmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

- Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la

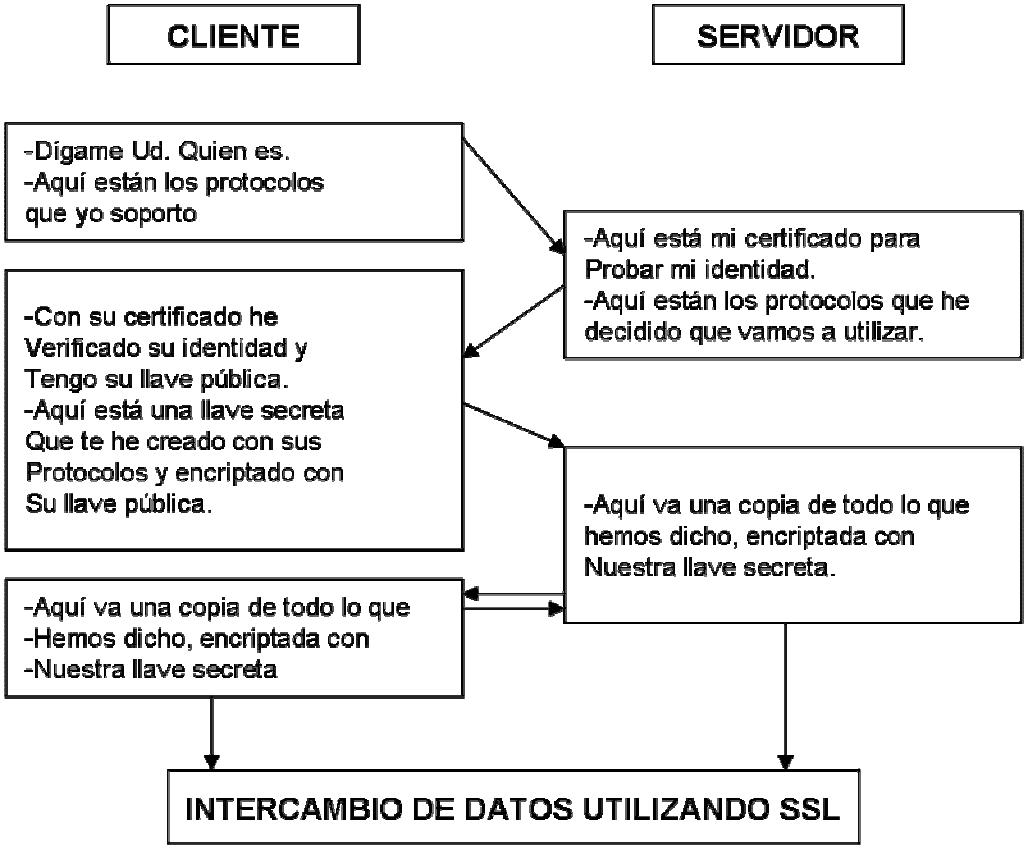
autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algorítmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el *handshake* tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

- Verificación: En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fué enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el *handshake* se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El *handshake* se realiza solo una vez y se utiliza una llave secreta por sesión.

En la figura 18 se ilustra el proceso de *handshake*:

**Figura 18.** Proceso de *Handshake*




Intercambio de datos:

Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un *digest* (utilizando un algoritmo de hash de una vía acordado durante el *handshake*), encriptan el mensaje y el *digest* y se envía, cada mensaje es verificado utilizando el *digest*.

Terminación de una sesión SSL:

Usando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

### 1.5.2 *Transport Layer Security* (TLS)

TLS es el estándar creado por la IETF como el protocolo de la capa de transporte. Surgió como respuesta a SSL de Netscape y PCT de Microsoft, se consideró negativo para la industria el manejo de dos protocolos similares, asi que se estableció TLS [RFC2246, 1999]. Está basado en SSL, de hecho se considera una actualización, versión 3.1 de SSL y presenta las siguientes modificaciones:

- Requiere soporte para el algoritmo DSA y D-H, RSA es opcional.
- El algoritmo de generación de llaves está modificado, utiliza MD5 y SHA-1 con HMAC como función pseudo aleatoria, a diferencia del algoritmo de llaves MAC definido en SSL.
- Contiene un conjunto más completo de alertas.

TLS es la propuesta por el grupo de trabajo de la IETF, sin embargo, ha habido mayor desarrollo sobre SSL.

### 1.5.3 *Authentication Header* AH*, Encapsulating Security Payload* (ESP)

Tanto AH como ESP pueden ser aplicados ya sea en forma individual o en forma combinada. Cada protocolo puede, a su vez, ser operado en una de dos formas: modo transporte o modo túnel.

En el modo transporte, los mecanismos de seguridad del protocolo se aplican sólo a las capas más altas de los datos y la información pertinente a la capa de operación cuando está contenida en el encabezado de IP el cual queda desprotegido, es decir, “abierto”, “llano” o “plano”. En modo túnel, tanto los datos de los protocolos de las capas superiores como el encabezado IP del datagrama IP son protegidos o “tuneleados” a través del encapsulamiento.

*Authentication Header* AH, es un mecanismo que provee las funciones de una integridad fuerte y de autentificación para datagramas IP. La integridad garantiza que el datagrama no sea alterado en forma inesperada o maliciosa, y la autentificación verifica el origen del datagrama (nodo, usuario, red, etc.). AH solo no acepta toda forma de encriptamiento, por lo cual no puede proteger la confidencialidad de cualesquiera datos enviados sobre *Internet*.

AH está orientado a mejorar la seguridad en el *Internet* global en situaciones donde importar, exportar o usar encriptamiento puede ser ilegal o estar restringido por disposiciones de gobiernos locales. AH ha de estar libre de tales complicaciones, razón por la cual ofrece el servicio de autentificación de paquetes IP.

Con esto se reduce la frecuencia de ataques basados en IP *spoofing*. AH asume la forma de un encabezado colocado entre el encabezado de IPv4 o

IPv6 y la siguiente trama del protocolo de la capa más alta, tales como TCP, UDP, ICMP, etc.

El encabezado *Encapsulating Security Protocol* (ESP) realiza funciones de integridad y de confidencialidad para datagramas IP. Como ya lo hemos dicho, la integridad asegura que el datagrama no haya sido alterado en forma inesperada o maliciosa, y la confidencialidad asegura la privacidad de los datos usando técnicas criptográficas.

El protocolo ESP tiene un diseño flexible que le permite trabajar con diferentes algoritmos de encriptamiento (también nombradas transformadas).

El protocolo ESP, como AH, se diseñó para trabajar en dos modos: túnel y transporte. La diferencia radica en el contenido de la porción ESP_*Payload* del datagrama IP. En modo túnel, un datagrama completo se encapsula y se encripta dentro de ESP_*Payload*. Cuando se hace esto, las direcciones verdaderas IP, origen y destino, pueden ser ocultas como un mero dato transitando en *Internet*. Un uso típico de este modo es cuando se esconde un servidor o una topología durante una conexión *firewall-to-firewall* sobre una red virtual privada (VPN).

En el modo transporte, en contraste, sólo la trama de los protocolos de las capas superiores (TCP, UDP, ICMP, etc.) se coloca en la porción encriptada ESP_*Payload* del datagrama.

# 2. SEGURIDAD IP

El protocolo *Internet Protocol*, IP, es uno de los más usados para la interconexión de redes tanto en ambientes académicos como corporativos, y naturalmente lo es también en la *Internet* pública. Su flexibilidad y sus poderosas capacidades lo han impuesto como un vehículo de interconectividad por un largo tiempo.

La fuerza de IP radica en su facilidad y su flexibilidad para el envío de grandes volúmenes de información en pequeños datagramas a través de los diversos esquemas de enrutamiento.

Sin embargo, IP presenta ciertas debilidades. La forma en que el protocolo enruta los paquetes hace que las grandes redes IP sean vulnerables a ciertos riesgos bien conocidos de seguridad. Uno de ellos es el llamado *IPSpoofing*, en el cual un intruso ataca cambiando la dirección del paquete IP, haciéndolo aparecer como si éste se hubiese originado en otro lugar.

Otro de tales ataques es la intromisión en una transmisión IP mediante el uso de un analizador de protocolos, lo que permitiría hacer un seguimiento del tráfico en la red. Mencionamos como un último tipo de ataque a IP aquel realizado cuando el intruso irrumpe en una sesión establecida y se enmascara como si fuese una de las partes en esa comunicación.

Debido a que estas vulnerabilidades limitan y complican el uso de las grandes redes IP (incluyendo por supuesto a toda *Internet*) en comunicaciones altamente sensibles, un grupo internacional organizado bajo el *Internet Engineering Task Force* (IEFT) desarrolló el IP *Security* (IPSec) *protocol suite*,

como un conjunto de extensiones para IP que ofrecen servicios de seguridad en el nivel de red (de acuerdo con el modelo de capas de ISO de OSI).

La tecnología de IPSec se basa en la criptografía moderna, lo que garantiza, por un lado, la privacidad y, por otro, una autentificación fuerte de datos.

El protocolo TCP/IP, el mas utilizado hoy en día, la seguridad es escasa, tiene muchas vulnerabilidades si se implementa sin ninguna otra tecnología de seguridad. Una de las tecnologías que se acopla muy bien a el es el IPSec, que viene a suplir con todas las necesidades de seguridad del protocolo TCP/IP.

## 2.1 Protocolo TCP/IP

TCP se diseñó para un entorno que resultaba poco usual para los años 70 pero que ahora es habitual. El protocolo TCP/IP debía conectar equipos de distintos fabricantes. Debía ser capaz de ejecutarse en diferentes tipos de medio y enlace de datos. Debía unir conjuntos de redes en una sola *Internet* de forma que todos sus usuarios pudiesen acceder a un conjunto de servicios genéricos. Más aún, los desarrolladores, académicos, militares y gubernamentales de TCP/IP querían poder conectar nuevas redes sin necesidad de detener el servicio.

Estos requisitos perfilaron la arquitectura del protocolo, la necesidad de independencia de tecnología del medio y una conexión automática a una red en crecimiento, condujo a la idea de transmitir datos por la red troceándolos en pequeños paquetes y encaminándolos cada uno como una unidad independiente. Las funciones que garantizan el envío y entrega fiable de datos se situaron en los host origen y destino, por ello, los fabricantes los fabricantes debían mejorar sus esfuerzos para diseñar equipos de alta calidad.

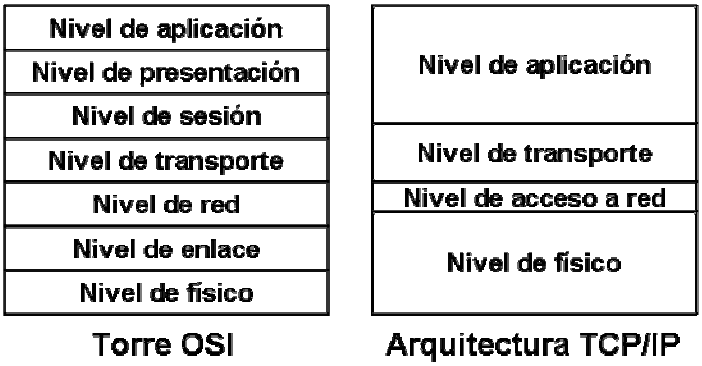
Al hacerlo así, los protocolos de TCP/IP consiguieron escalarse muy bien ejecutándose en sistemas de cualquier calibre. Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados y la tarea de:

- Empaquetar datos.
- Determinar el camino que deben seguir.
- Transmitirlos por el medio físico.
- Regular su tasa de transferencia según el ancho de banda del medio disponible y la capacidad del receptor para absorber los datos.
- Ensamblar los datos entrantes para que mantengan la secuencia correcta y no haya pérdida de trozos.
- Comprobar los datos entrantes para ver si hay trozos pérdidos.
- Notificar al transmisor que los datos se han recibido correctamente u erróneo.
- Entregar los datos a la aplicación correcta.
- Manejar eventos de errores y problemas.

El resultado es que el software de comunicaciones es complejo. Con un modelo de capas resulta más sencillo relacionar las funciones de cada protocolo con un nivel específico e implementar el software de comunicaciones de forma modular.

El modelo de comunicación de datos OSI se vio fuertemente influido por el diseño de TCP/IP. Las capas o niveles de OSI y la terminología de OSI se ha convertido en un estándar de la cultura de las comunicaciones de datos. Los fabricantes de hardware y software deben desarrollar el diseño de sus sistemas en base al modelo OSI el cual es un estándar de la industria. A continuación se muestran las capas de TCP/IP y de OSI:

**Figura 19.** Capas del Modelo OSI Y TCP/IP




### 2.1.1 Capa de aplicación

Es el nivel mas alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continuo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

### 2.1.2 Capa de transporte

La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia.

Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la capa de aplicación, una computadora de propósito general puede tener varios programas de aplicación accesando la red de redes al mismo tiempo. La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para verificar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

### 2.1.3 Capa de acceso a la red

Capa de interfaz de red. El software TCP/IP de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Una interfaz de red puede consistir en un dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que las máquinas están conectadas directamente) o un complejo subsistema que utiliza un protocolo de enlace de datos propios (por ejemplo, cuando la red consiste de conmutadores de paquetes que se comunican con anfitriones utilizando HDLC).

Y existen dos protocolos de red:

- IPv4
- IPv6.

IPv4 (*Internet Protocol* versión 4) es el protocolo de capa de red más popular hoy en día y tiene la infraestructura de enrutamiento muy madura. El direccionamiento es uno de los componentes más importantes de un protocolo de red, IPv4 maneja direcciones de 32 bits (232 computadoras2) representadas en notación decimal separada por puntos A.B.C.D, cada símbolo es un byte y representa una parte de dirección de red y otra de computadora. La dirección de red se obtiene con un AND lógico con la máscara de red, todas las direcciones IP van acompañadas de una máscara de red.

- Por ejemplo, una dirección IPv4 válida de Red es

192.168.0.1/24

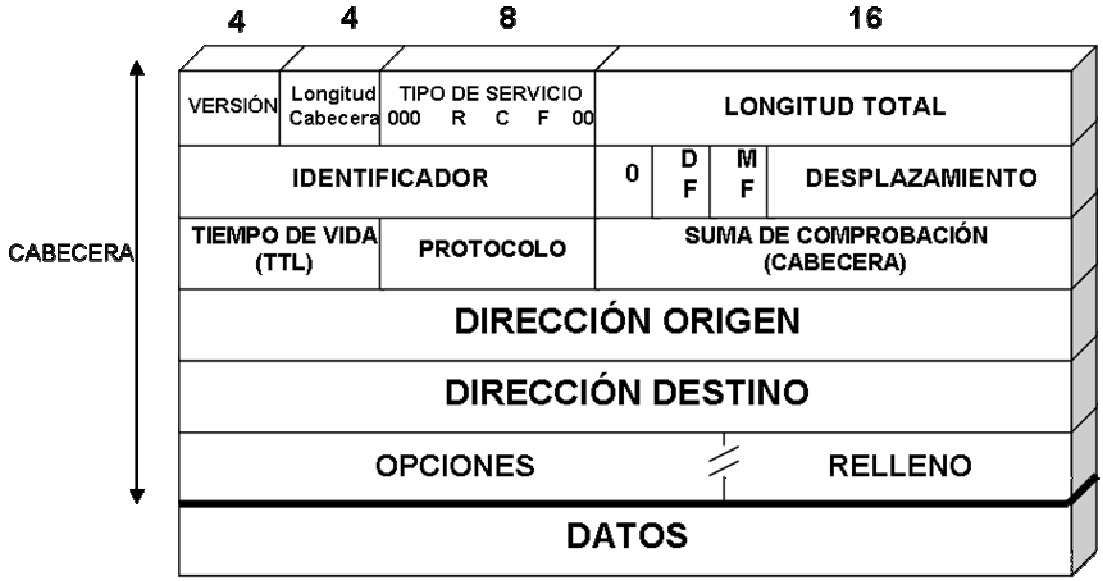
Una dirección IPv6 es de 128 bits de longitud y su representación es diferente, números hexadecimales separados por dos puntos, el concepto de máscara es similar y se ha implementado una jerarquía mucho más rica para disminuir los problemas de enrutamiento y direccionamiento.

- Por ejemplo, una dirección IPv6 válida de Red es:

3ffe:8070:100f:1:a00:20ff:fec6:ba27/64 que indica la región geográfica, la institución, subred y computadora de forma única en la red mundial experimental de IPv6.

La figura 20, muestra los componentes del encabezado de IPv4.

**Figura 20.** Datagrama IPv4




Cada uno descrito a continuación:

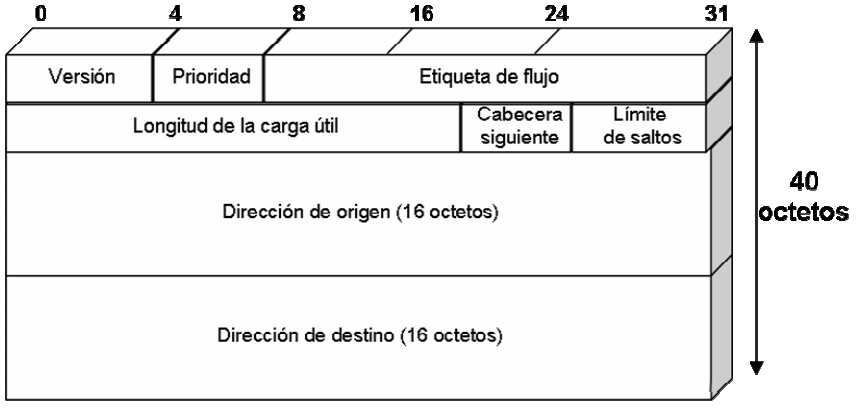
- Versión: es un campo de 4 bits utilizado para indicar la versión, un 4 para IPv4, se utiliza para validar compatibilidad.
- Longitud cabecera: indica la longitud del encabezado en 32 bits.
- Tipo de servicio (TOS): se utiliza para indicar los requerimientos de tráfico de un paquete, no ha sido utilizado y se encuentra en revisión por la IETF.
- Longitud total: la longitud total del datagrama3 en bytes, incluyendo el encabezado. Indica el tamaño total del datagrama a la capa de red en el extremo receptor.
- Identificador: es un campo de 16 bits para identificar de manera única un datagrama IP. Este campo se utiliza principalmente para

fragmentación, identifica de manera única cuál paquete IP pertenece a un datagrama IP.

- Banderas: Solo han sido definidos dos bits de los tres reservados. El primer bit especifica la no fragmentación del paquete. El segundo bit indica si es el último fragmento de un datagrama o si hay otros, este bit se utiliza también para la reconstrucción de los datagramas fragmentados.
- Offset de fragmentación: indica el *offset* del paquete IP dentro del datagrama IP.
- Tiempo de vida (TTL): un contador para eliminar ciclos, se asigna un valor por omisión, y cada enrutador en la trayectoria lo decrementa en 1.
- Protocolo: indica el protocolo de transporte.
- Suma de Comprobación: se utiliza para validar la integridad del encabezado IP.
- Dirección origen y dirección destino: indica las direcciones de 32 bits del fuente y destino del paquete, respectivamente.

La figura 21, muestra los componentes del encabezado de IPv4.

**Figura 21.** Encabezado IPv6



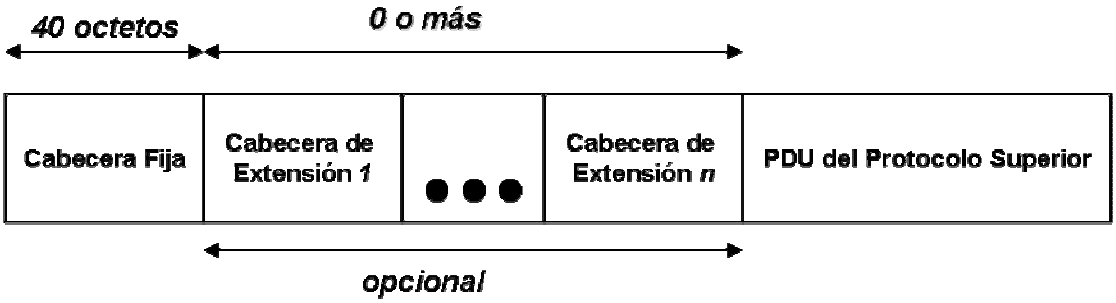
Cada uno descrito a continuación:

- Versión: indica la versión, 6 para IPv6.
- Prioridad: campo de 8 bits para indicar los requerimientos de tráfico del paquete, similar a TOS de IPv4.
- Etiqueta de flujo: campo de 20 bits, experimental.
- Longitud de carga útil: campo de 16 bits que indica la longitud de la carga útil sin incluir el encabezado IPv6.
- Cabecera Siguiente: campo de 8 bits, para indicar el uso de cabeceras de extensión.
- Límite de saltos: campo de 8 bits similar al TTL de IPv4.
- Dirección origen y destino: campos de 128 bits para las direcciones fuente y destino del paquete, respectivamente.

Las Cabeceras de Extensión IPv6 son similiares a las opciones IPv4

- Nuevas opciones que incluyen servicios adicionales, Cada cabecera de opción recibe un identificador único,
- Evitan que los datagramas compartan campos que no utilizan
- Routers hacen caso omiso de opciones no dirigidas a ellos.

**Figura 22.** Datagrama IPv6



### 2.1.4 Capa física

Define las características del medio, su naturaleza, el tipo de señales, la velocidad de transmisión, la codificación, etc. Son responsables de la transmisión de paquetes por el medio físico. La transmisión es entre dos dispositivos que están físicamente conectados.

## 2.2 IPV6

Como una iniciativa de alta tecnología tiene el mismo tipo de desarrollo que *Internet* tuvo en sus inicios, es decir en los círculos académicos, militares y de gobierno para pronto ampliarse al público que demanda aplicaciones que se caracterizan por requerir de banda ancha y a la cual puedan acceder no solamente los usuarios sino múltiples artefactos de un usuario como por ejemplo las refrigeradoras, microondas, etc., para lo que se requiere ampliar el ya casi agotado recurso de direcciones IP de Ipv4 por lo que se encuentra en su fase de prueba ya el Ipv6 que proporcionará un espectro mayor de direcciones para este fin.

El direccionamiento IP tal como se lo ha conocido y estudiado hasta ahora (IPv4), pronto será reemplazado por la versión IPv6, en la practica no existió IPv5.

Los ingenieros y diseñadores de TCP/IP han reconocido la necesidad de hacer una actualización al protocolo IP desde finales de los años 80's, cuando se empezó a ver que las direcciones IP's existentes no iban a poder soportar el continuo crecimiento de *internet*. Las principales razones por las cuales se cambiará a IPV6 son las siguientes:

- Limitaciones de direcciones IP. La crisis de falta de direcciones IP se ha venido agrandando en los últimos años y es uno de los motivantes más fuertes para la actualización del protocolo.
- Desempeño. A pesar que IP tiene un desempeño muy bueno, algunas de las decisiones de diseño realizadas hace más de vente años pueden ser modificadas brindándole un mejoramiento.
- Seguridad. A pesar de ser considerado un aspecto perteneciente a capas superiores de la red, la seguridad ha emergido como una área en la que la siguiente versión de IP podría brindar algunas funciones muy útiles.
- Auto configuración. El configurar los nodos de IPV4 siempre ha sido complejo, pero los administradores de red y los usuarios preferirían ser capaces de conectar a una computadora a la red y comenzar a utilizarla en cierta forma del modo *plug and play*.
- El aumento en la disponibilidad de direcciones IP también trae consigo la posibilidad de un mejor soporte para configurarlas y una movilidad a través de diferentes redes utilizando diferentes puntos de acceso.

### 2.1.1 Seguridad y autenticación

IPV4 no incorpora características reales de seguridad, sino que fue diseñado simplemente como un protocolo para el intercambio de información. Sin embargo esto no evita que sea utilizado en redes gubernamentales o militares donde las restricciones por seguridad deben ser muy cuidadosas.

Las metas de seguridad para telecomunicaciones se pueden definir por tres características básicas:

- Autentificación. La capacidad de determinar de manera confiable que los datos han sido recibidos tal como fueron enviados y verificar que cada una de las entidades es en realidad quien dice ser.
- Integridad. La capacidad de determinar de manera confiable que los datos no han sido modificados durante el tránsito desde la fuente al destino.
- Confidencialidad. La capacidad de transmitir datos que solo puedan ser leídos o utilizados por la entidad a la cual van dirigidos y por nadie más.

La integridad y la autentificación se pueden alcanzar mediante el uso de la encripción y el uso de llaves, las cuales también sirven para autentificar a la fuente.

El problema de la seguridad en *internet* como en cualquier tipo de seguridad radica en que es difícil crearla, particularmente en una red abierta en donde los paquetes pueden recorrer cualquier número de redes desconocidas y donde los "*sniffers*" pueden estar trabajando sin ser detectados. Estos son los vacíos significantes en materia de seguridad a pesar de estar en uso mecanismos de encripción y firmas digitales.

También mientras que los ataques al tráfico IP incluyen cosas como la intercepción, donde los datos transmitidos pueden ser robados por una tercera entidad no autorizada, también existen otros puntos los cuales deben ser vistos por la seguridad en el protocolo IP como son:

- Ataques DoS (*Denial of Service*) que ocurren cuando una entidad utiliza las transmisiones de la red para de alguna manera evitar que un usuario autorizado tenga acceso a los recursos de la red. Por ejemplo un atacante puede *floodear* a un servidor con peticiones y de esta manera

tirar el sistema, o el ataque puede consistir en la transmisión repetida de mensajes de e-mail muy largos con la intención de llenar el ancho de banda de un usuario o sitio con tráfico de basura.

- Ataques de *Spoofing* los cuales ocurren cuando una entidad transmite paquetes que representan de manera falsa a una entidad de origen. Esto es por ejemplo cuando se manda un mensaje de mal con *header* indicando que es enviado por el presidente de los Estados Unidos.

O ataques más insidiosos ocurren cuando los paquetes son enviados con una dirección de fuente incorrecta en el *header*. De la misma forma es complicado el aspecto del manejo e intercambio de llaves. La arquitectura de seguridad de IP demanda la utilización de llaves para los propósitos de autentificación y verificación. Y un aspecto difícil es la manera en que la comunidad de *internet* puede administrar y distribuir de manera segura las llaves y al mismo tiempo asociar de manera correcta estas llaves con entidades.

## 2.3 IPSec

IPSec esta compuesto de un conjunto de estándares con los cuales dan al IP funciones de seguridad basadas en criptografía, proporciona confidencialidad, integridad y autenticidad de datagramas de IP.

Es modular, con esto se puede seleccionar de un conjunto de algoritmos, el deseado sin afectar a las otras partes de la implementación. Pero existen ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad.

Las características de IPSec lo hacen único debido a que implementa seguridades en la capa de red más que en la de aplicaciones.

Dado que el protocolo IPSec asegura a la red por sí misma, se garantiza que las aplicaciones que se estén usando en la red sean, en efecto, seguras. Existen ya numerosos productos que implementan IPSec. Sin embargo, también es cierto que no es necesariamente la elección correcta para una solución de seguridad para un administrador de red.

Para ofrecer seguridad en el nivel de IP es necesario que IPSec sea parte del código de red en todas las plataformas participantes, incluyendo sistemas Windows NT, UNIX y Macintosh, pues de otra manera una aplicación dada podría fracasar al intentar usar las funciones de seguridad del protocolo. Sin embargo, para una red virtual privada, IPSec ofrece, en efecto, las facilidades al nivel de la capa de red requeridas.

IPSec ofrece tres facilidades principales:

- Una función de autentificación, referida como *Authentication Header* (AH),
- Una función combinada de autentificación/encriptamiento llamada *Encapsulating Security Payload* (ESP)
- Una función de intercambio de llaves.

Para las redes virtuales privadas (VPN), tanto la autentificación como el encriptamiento son, por lo general, deseables, pues:

- Aseguran que usuarios no autorizados no penetren en la VPN y

- Aseguran que los usuarios no autorizados en *Internet* no puedan leer mensajes privados enviados sobre la VPN.

Ambas características son deseables y la mayoría de las implementaciones se adaptan más a ESP que a AH. La función de intercambio de llaves permite realizar esta función ya sea en forma manual o bien en forma automática.

Evidentemente, la aceptación generalizada de un IP seguro está propiciada por la necesidad de usuarios corporativos y gubernamentales para conectar sus infraestructuras *WAN/LAN* a *Internet* para

- El acceso a servicios de *Internet* y
- El uso de la *Internet* como una componente del sistema de transporte *WAN*.

Los usuarios requieren aislar sus redes y al mismo tiempo enviar y recibir tráfico sobre *Internet*. Los mecanismos de seguridad IP proporcionan la base para una estrategia de seguridad. Debido a que los mecanismos de seguridad IP han sido definidos en forma independiente de su uso, ya sea con el IP, de uso mayoritario en la actualidad, o con IPv6, la organización de estos mecanismos no depende del desarrollo de IPv6. Es pues altamente probable que se extienda el uso de las características de seguridad de IP aún antes de que IPv6 venga a ser más popular.

### 2.3.1 Componentes

Dentro del IETF, se estableció el IP *Security Protocol Working Group*, en donde se desarrolló la especificación completa de IPSec. Obteniendo siete componentes:

- Arquitectura (*Architecture*): Establece los conceptos generales: requisitos de seguridad, definiciones y mecanismos característicos de la tecnología de IPSec.

- Carga útil de seguridad de encapsulación *(Encapsulating Security Payload*) ESP: Describe el formato del paquete y las definiciones generales relacionadas para el uso de ESP para el encriptamiento de paquetes, y opcionalmente la autentificación.

- Cabecera de Autenticación (*Authentication Header*) AH: Describe el formato del paquete y las definiciones generales relacionadas para el uso de AH para la autentificación de paquetes, así como su algoritmo MAC (*Message Authentication Code*).

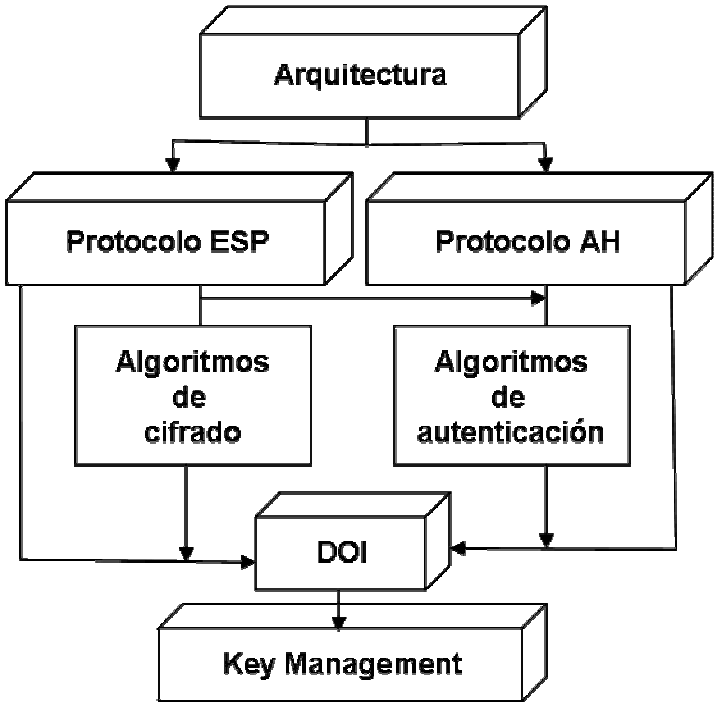
- Algoritmo de encriptación (*Encryption Algorithm*): Documentos que describen cómo los diversos algoritmos de encriptamiento son utilizados por ESP, tales como DES, Triple-DES, RC5, IDEA,CAST, BLOWFISH y RC4.

- Algoritmo de Autenticación (*Authentication Algorithm*): Documentos que describen cómo los diversos algoritmos son usados por AH y por la opción de autentificación de ESP.

- Administración de Llaves (*Key Management*): Documentos que describen los esquemas para administración de las llaves.

- Dominio de interpretación (*Domain of Interpretation*) DOI: Contiene parámetros necesarios para diversos documentos relacionados entre sí. Estos incluyen identificadores para algoritmos de autentificación y de encriptamiento aprobados, así como también parámetros operacionales tales como tiempos de vigencia de llaves (*key lifetime*).

**Figura 23.** Componentes de IPSec




### 2.4.2 Asociación de seguridad

El concepto de asociación de seguridad (*Security Association*) SA es fundamental en IPSec. Tanto AH como ESP, hacen uso de asociaciones de

seguridad y una función importante de IKE es el mantenimiento y establecimiento de las asociaciones de seguridad. Cualquier implementación de AH o ESP debe soportar el concepto de asociación de seguridad.

Una SA es una conexión *simplex* o unidireccional, ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor, que permite servicios de seguridad al tráfico que transporta. Una SA permite servicios de seguridad mediante el uso de AH o de ESP pero no de ambos. Si ambos no se aplican en un flujo de tráfico, entonces existirán dos (o más) SAs para permitir la protección al flujo de tráfico.

Para asegurar la comunicación bidireccional típica entre dos *Hosts* o dos puertas de enlace, se requieren dos asociaciones de seguridad (uno en cada sentido).

Una SA es identificada únicamente por un triplete consistente en un índice de parámetros de seguridad (SPI), una dirección IP de destino y un identificador de protocolo de seguridad (AH o ESP).

Definen dos tipos de SAs:

- Modo transporte.
- Modo túnel.

Una SA en modo transporte es una asociación de seguridad entre dos terminales. En IPv4 una cabecera de protocolo de seguridad aparece inmediatamente después de la cabecera IP y cualquier opción y antes que ningún protocolo de capas superior.

En IPV6 las cabeceras de protocolo de seguridad se situarán después de la cabecera IP base y extensiones pero deben aparecer antes o después de la cabecera de opciones de dirección (*destination*) y antes de los protocolos de capas superiores.

En el caso de ESP una SA en modo de transporte proporciona servicios de seguridad solamente para los protocolos de las capas superiores, no para la cabecera IP o cualquier cabecera de extensión precedente a la cabecera ESP. En el caso de AH la protección también se extiende a las porciones seleccionadas de la cabecera IP, porciones seleccionadas de las cabeceras de extensión y las opciones seleccionadas (contenidas en la cabecera IPV4, la cabecera de extensión *Hop-by-Hop* de IPV6, o la cabecera de extensión de destino de IPV6).

Una SA en modo túnel es en esencia una SA aplicada a un túnel IP. Siempre que el final de una asociación sea una puerta de enlace segura, la SA debe estar en modo túnel.

Para una SA en modo túnel, hay una cabecera IP externa que especifica el destino de proceso de IPSec, además de una cabecera interna que especifica el destino (aparentemente último del paquete). La cabecera del protocolo de seguridad aparece después de la cabecera IP externa y antes de la interna. Si se emplea AH en modo túnel permite proteger parte de la cabecera IP externa, además de todo el paquete IP entunelado. si usamos ESP solo se permitirá proteger al paquete entunelado y no a la cabecera externa.

Se deben de cumplir con lo siguiente, para la asociación de seguridad:

- Un host debe soportar el modo de transporte y el modo túnel.

- Para suportar únicamente el modo túnel se requiere una puerta de enlace de seguridad. Si soporta el modo de transporte, este modo solo debe usarse cuando la puerta de enlace de seguridad actúe como host (por ejemplo para la administración de la red).

**IKE *Internet Key Exchange* (IKE)**

Los mecanismos de seguridad de IPSec se basan en que las entidades deben establecer una negociación, en la cual ambas partes se ponen de acuerdo en los algoritmos criptográficos utilizados, en qué claves utilizar, y otros parámetros. Para esta negociación es necesario el protocolo IKE, conocido también como *Internet Security Association and Key Management Protocol* (ISAKMP/Oakley).

El IETF ha definido el protocolo IKE para realizar la función de gestión automática de claves como el establecimiento de las SAs correspondientes.

Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley.

ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.

Dicha negociación se lleva a cabo en dos fases:

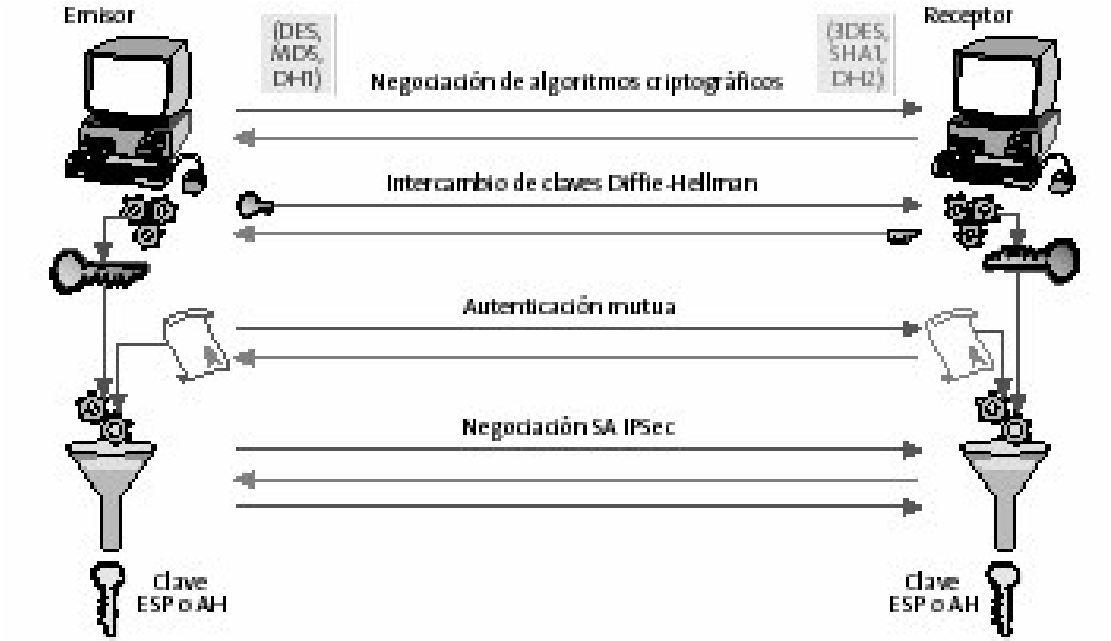
1. La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación. Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

    - El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.

- En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la **PKI** (Infraestructura de Clave Pública).

En la Figura 24 se representa de forma esquemática el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

**Figura 24.** Funcionamiento del protocolo IKE




Fuente: Santiago Pérez Iglesias. **Análisis del protocolo IPSec.** Pagina 57.

#### 2.3.2.1 Funcionalidad

El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, el punto terminal de la SA, y de los servicios opcionales seleccionados dentro del protocolo. Por ejemplo, AH proporciona autenticación del origen de los datos e integridad sin conexión para datagramas IP. La precisión de estos servicios estará en función de la "granularidad" de la asociación de seguridad con la que se emplea AH.

AH ofrece además servicio *anti-replay* (integridad de secuencia parcial). El Protocolo AH es el apropiado cuando la confidencialidad no se requiere confidencialidad (o cuando no esta permitida por prohibición de gobiernos). AH también autenticación para porciones de la cabecera IP (pero no de las partes mutables en la ruta), que pueden ser necesarias en algunos contextos.

ESP proporciona de forma opcional confidencialidad del tráfico (cuya fuerza depende del algoritmo de encriptación utilizado). Además proporciona, también de forma opcional, autenticación como en el caso anterior. Si se negocia la autenticación para una SA con ESP el receptor también elige si fuerza a cumplir un servicio *anti-replay* con las mismas características que las ofrecidas por AH. El alcance de la autenticación ofrecida por ESP es más estrecho que el del ofrecido por AH, por ejemplo: las cabeceras que quedan por fuera de la cabecera ESP no están protegidas. Si solo se desea aportar autenticación únicamente a las capas superiores, entonces ESP es la elección apropiada y es más eficiente en tamaño que usar ESP encapsulado con AH. Aunque la confidencialidad y la autenticación son opcionales, no se pueden omitir ambas, al menos una debe ser escogida.

Si se elige el servicio de confidencialidad, entonces una SA con ESP (en modo túnel)

Entre dos puertas de enlace pueden ofrecer confidencialidad en un flujo de tráfico parcial. El uso del modo túnel encriptar las cabeceras IP internas, ocultando las identidades de la (última) vía de tráfico y el destino. También usar relleno en la carga de ESP para ocultar el tamaño de los paquetes.

#### 2.3.2.2 Combinación

Los datagramas IP transmitidos sobre una SA individual permiten la protección con exactamente un protocolo de seguridad, o AH o ESP, pero no con ambos.

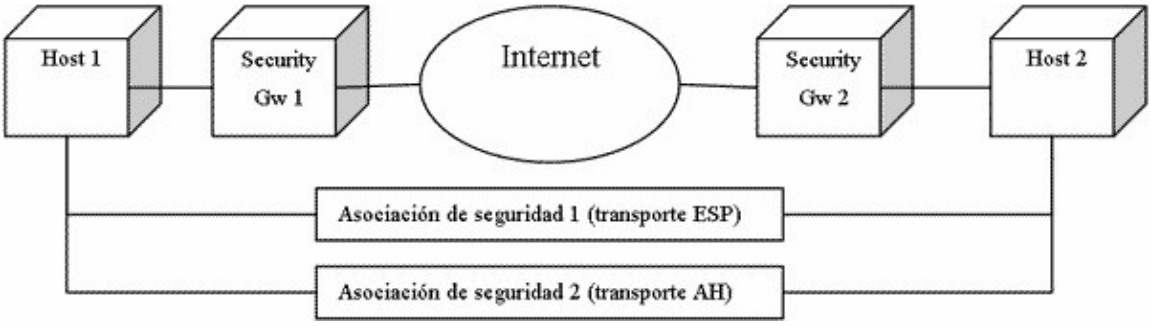
Algunas veces las políticas de seguridad pueden solicitar una combinación de servicios, para un flujo de tráfico particular, que no se puede conseguir con una única SA. En estos casos será necesario emplear múltiples SA para implementar la política de seguridad requerida. Se aplica el termino "SA bundle" a una secuencia de asociaciones de seguridad a través de la cual se debe procesar el tráfico para satisfacer la política de seguridad.

Las asociaciones de seguridad pueden estar combinadas en "SA *bundles*" de dos formas:

- Transporte adyacente
- Entonelado iterado

Transporte adyacente: se aplican más de un protocolo de seguridad sobre el mismo datagrama IP, sin utilizar entunelado. Esta combinación de AH y ESP permite sólo un nivel de combinación:

**Figura 25.** Combinación de seguridad transporte adyacente

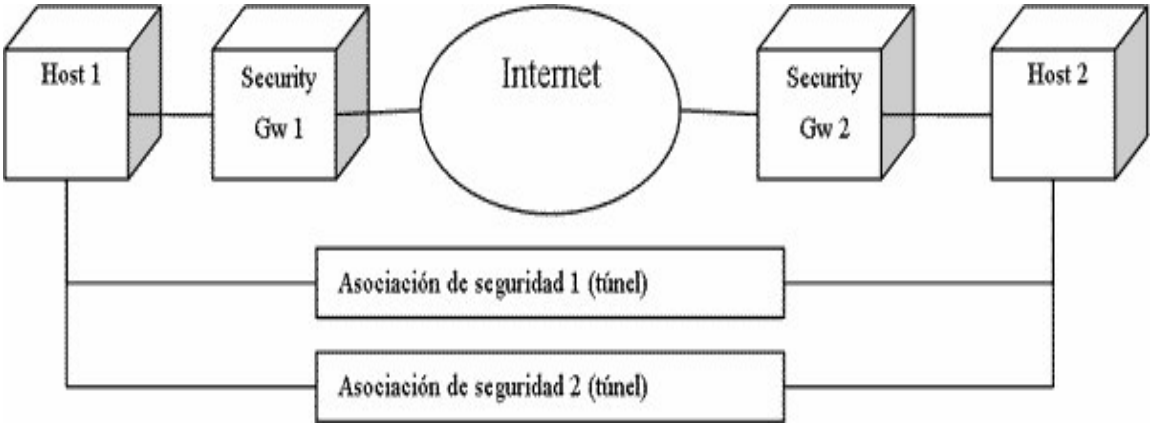



Entunelado iterado: se refiere a la aplicación o al uso de múltiples capas de protocolos de seguridad a través de entunelado IP. Esta combinación permite múltiples niveles de anidamiento. Cada túnel se puede originar o terminar en nodos diferentes a lo largo de la ruta.

Hay tres tipos básicos de entunelado iterado:

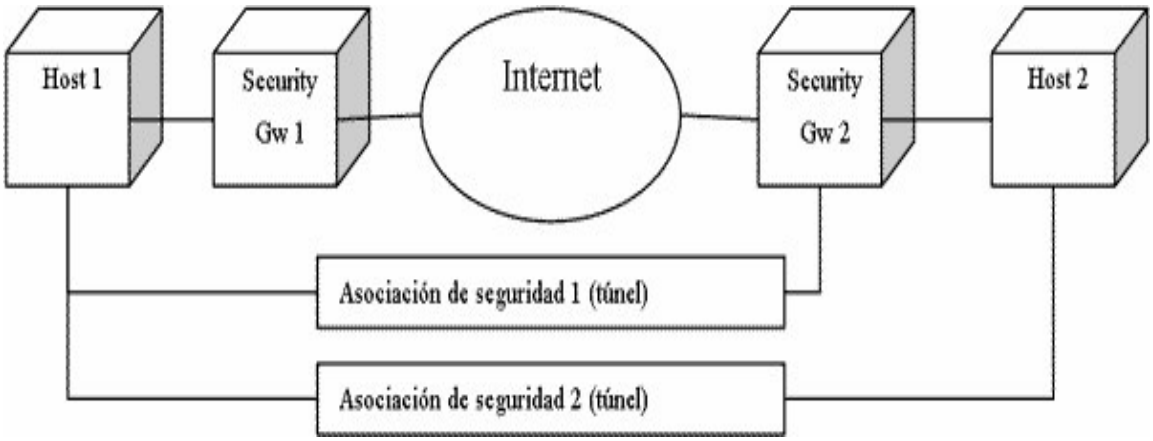
1. Ambas terminaciones de la SA son las mismas. Cualquiera de los túneles (interno o externo) puede hacerse con AH o ESP:

**Figura 26.** Combinación de seguridad entunelado iterado 1



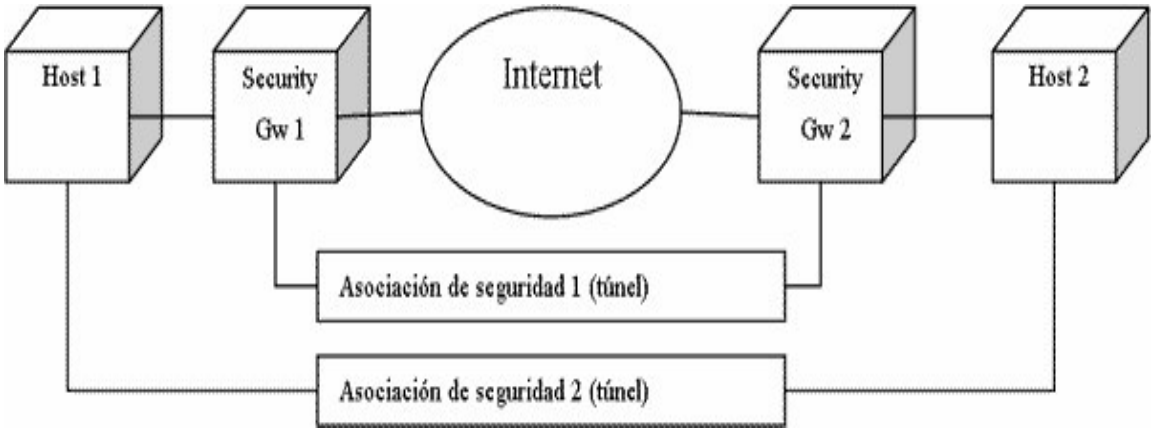
2. Una terminación de la SA es la misma. Cualquiera de los túneles (interno o externo) puede hacerse con AH o ESP:

**Figura 27.** Combinación de seguridad entunelado iterado 2




3. Ninguna de las terminaciones es la misma:

**Figura 28.** Combinación de seguridad entunelado iterado 3



#### 2.3.2.3 Base de datos

En IPSec hay dos bases de datos que detallan el procesamiento del tráfico:

- La base de datos de política de seguridad (SPD)
- La base de datos de asociación de seguridad (SAD)

La primera especifica las políticas que determinan el tratamiento de todo el tráfico IP de entrada o salida de un *Host* y puerta de enlace segura. La segunda contiene los parámetros asociados a cada SA.

También se define un selector, que es un conjunto de campos con valores del protocolo IP y capas superiores que son usados por la SPD para mapear el tráfico con una política por ejemplo una SA.

**SPD**

Contiene los servicios que se ofrecerán a los datagrama IP y en qué modalidad. La forma de esta base de datos y su interfaz no se especifican. Para cada implementación IPSec debe haber una interfaz de administración que permita al administrador del sistema manejar la SPD.

Los paquetes de entrada y salida son propensos a ser tratados por IPSec y la SPD debe especificar que acción ha de realizar en cada caso.

**Selectores**

El manejo de las SA debe soportar los siguientes parámetros selectores para facilitar el control de la granularidad de las SA:

- Dirección IP de destino.
- Dirección IP de origen.
- Nombre: hay dos casos; Identificación de usuario (*user* ID) y nombre del sistema (*Host*, puerta de enlace de seguridad, etc.).
- Nivel de sensibilidad de datos: requeridos para todos los sistemas que proporcionen seguridad de flujo de información.
- Protocolo de la capa de transporte: obtenido de la cabecera "*Protocol*" en IPv4 o de la "*Next Header*" en IPv6.
- Puertos de destino y origen: puertos TCP/UDP

**SAD**

Cada SA tiene una entrada en la SAD y cada entrada define los parámetros asociados a esa SA. Los campos de la SAD usadas en el procesamiento de IPSec son los siguientes:

- Contador de números de secuencia.
- Desbordamiento del contador de secuencia.
- Ventana *anti-replay*.
- Algoritmo de autenticación AH, Claves, etc.
- Algoritmos de encriptación ESP, Claves, IV *mode*, IV (vector de inicialización), etc.
- Tiempo de vida de la SA.
- Modo del protocolo IPSec (túnel, transporte, etc.).

#### 2.3.2.4 Parámetros

Los parámetros por negociar en una SA, tanto para AH como para ESP son los siguientes:

- Número de secuencia
- Sobreflujo del número de secuencia
- Ventana de *antireply*
- Tiempo de vida
- Modo
- Destino del túnel
- Parámetros PMTU

**Número de secuencia**

Un campo de 32 bits utilizado en el procesamiento de paquetes de salida, es parte de los encabezados de AH y/o ESP, su valor inicial es 0, se incrementa en uno cada vez que la SA es utilizada, se utiliza para detectar ataques del tipo "*replay*".

**Sobreflujo del número de secuencia**

Campo utilizado en el procesamiento de paquetes de salida y se establece cuando hay sobre flujo del campo de número de secuencia. La política determina qué hacer si este campo está activado.

**Ventana de *antireply***

Campo utilizado en el procesamiento de paquetes de entrada. Se activa si IPSec detecta paquetes retransmitidos por *hosts* sospechosos.

**Tiempo de vida**

El tiempo de validez de una SA, se especifica en términos de bytes asegurados con la SA, no se recomienda enviar más de 4Gb de paquetes utilizando la misma SA. Para evitar la pérdida de la conexión segura, se manejan dos límites, *soft* y *hard*. Al llegar al límite *soft* el *kernel* es notificado para que inicie una nueva negociación antes del límite *hard* que es cuando la SA expira.

**Modo**

Los valores son: túnel, transporte o indistinto. Si el valor es indistinto la SA puede ser utilizada para modo túnel o modo transporte.

**Destino del túnel**

Campo utilizado para modo túnel, indica la dirección IP de destino del encabezado exterior.

**Parámetros PMTU**

IPSec no fragmenta o reensambla paquetes, sin embargo, agrega un encabezado IPSec y por lo tanto impacta la longitud del PMTU. IPSec debe

participar en la determinación del PMTU (*Protocol Maximum Transfer Unit*), una SA mantiene dos valores: el PMTU y el campo de edad.

### 2.3.3 Servicios

IPSec ofrece servicios de seguridad en la capa de IP habilitando un sistema para seleccionar protocolos de seguridad necesarios, determinar algoritmos a utilizar en los servicios y colocar en cualquier lugar las llaves criptográficas requeridas para cumplir con los servicios solicitados. Se utilizan dos protocolos para proveer seguridad: uno para autentificación, diseñado para el encabezado del protocolo AH, y otro combinado para autentificación/encriptamiento diseñado para el formato del paquete en el protocolo ESP.

Los servicios proporcionados son:

- Control de acceso
- Integridad sin conexión
- Autentificación de origen
- Rechazo de paquetes retocados (como una forma de integridad secuencial parcial)
- Confidencialidad (encriptamiento)
- Confidencialidad limitada por el flujo del tráfico

**Tabla III.** Servicios de IPSec

| | AH | ESP (sólo encriptación) | ESP (encriptación más autentificación) |
|---|---|---|---|
| **Control en el acceso** | √ | √ | √ |
| **Integridad sin conexión** | √ | | √ |
| **Autentificación de origen** | √ | | √ |
| **Rechazo de paquetes retocados** | √ | √ | √ |
| **Confidencialidad** | | √ | √ |
| **Confidencialidad limitada por el flujo del tráfico** | | √ | √ |

**Control de acceso: autenticación y autorización**

Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte "TOS" y otros campos.

Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso de tráfico hacia máquinas especialmente protegidas.

**Integridad y autenticación de origen de los datos**

El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

**Rechazo de paquetes retocados**

La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

**Confidencialidad**

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado

es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Ésta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis de tráfico es un riesgo que debe considerarse seriamente, recientemente se ha documentado la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH. Es previsible que este tipo de ataques se harán más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.

# 3. FUNCIONAMIENTO IPSEC

El funcionamiento de IPSec lo podremos observar en la siguiente figura

**Figura 29.** Funcionamiento de IPSec


*Internet Security Association and Key Management Protocol* (ISAKMP)

Alice, que utiliza una aplicación en el equipo A, envía un mensaje a Bob B.

A continuación los pasos:

1. La unidad de IPSec en el equipo A comprueba la lista de filtro IP en la directiva activa para buscar la correspondencia con la dirección o el tipo de tráfico de los paquetes de salida.

2. La unidad de IPSec notifica a ISAKMP para iniciar las negociaciones de seguridad con el equipo B.

3. El servicio ISAKMP en el equipo B recibe una solicitud de negociaciones de seguridad.
4. Los dos equipos realizan un intercambio de clave, establecen un ISAKMP y una clave secreta compartida.

5. Los dos equipos negocian el nivel de seguridad para la transmisión de información, establecen un par de IPSec SA y las claves para asegurar los paquetes IP.

6. Al utilizar la IPSec SA y clave de salida, la unidad de IPSec en el equipo A firma los paquetes por integridad, y cifra los paquetes si se ha negociado la confidencialidad.

7. La unidad IPSec en el equipo A transfiere los paquetes al tipo de conexión apropiado para la transmisión al equipo B.

8. El equipo B recibe los paquetes asegurados y los transfiere a la unidad de IPSec.

9. Al utilizar la SA y la clave de salida, la unidad de IPSec en el equipo B comprueba la firma de integridad y descifra los paquetes.

10. La unidad de IPSec en el equipo B transfiere los paquetes descifrados a la unidad TCP/IP, que los transfiere a la aplicación de recepción.

Alice y Bob no ven ninguno de los procesos. Los enrutadores o interruptores estándar en la ruta de información entre los interlocutores no necesitan IPSec. De manera automática envían los paquetes IP cifrados al destino. Sin embargo, si un enrutador funciona como un cortafuego, puerta de

seguridad o servidor proxy, debe habilitar el filtrado especial para habilitar los paquetes IP asegurados y poder pasar.

## 3.1 Beneficios

Entre los beneficios que aporta IPSec, cabe señalar que:

Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.

Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación. Las *extranets* son un ejemplo.

Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Es importante señalar que cuando citamos la palabra "seguro" no nos referimos únicamente a la confidencialidad de la comunicación, también nos estamos refiriendo a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad.

Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

Cuando se implementa IPSec en un router, éste provee una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro servido por el router.

Por otro lado, IPSec está debajo de la capa de transporte (TCP, UDP), así pues resulta “transparente” para las aplicaciones. No hay necesidad de cambiarlas, ni desde el punto de vista del usuario ni del servidor cuando IPSec se incorpora al *router* o al *firewall*.

También se tiene que IPSec puede ser “transparente” a los usuarios finales. Como una política general, puede asumirse que no es necesario involucrar a los usuarios en los mecanismos de seguridad.

IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable. Tal característica es útil para empleados que accedan a la red desde el exterior vía telefónica. Además, es posible asegurar una subred virtual dentro de una organización para aplicaciones sensibles.

Brinda privacidad, integridad, y autentificación para el comercio electrónico.

Satisface rigurosos requerimientos para la transmisión de información sensible en *Internet*.

Al implementarse sobre las redes no se afecta a la base instalada.

## 3.2 Infraestructura de clave pública PKI

Bajo el nombre de PKI (Infraestructura de Clave Pública) se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios.

Su misión debe ser la seguridad en las transacciones electrónicas con su entorno claves y gestionando eficientemente certificados confiables, para lograr las conocidas garantías de autenticación, confidencialidad y no repudiación.

Su implementación funcional permite proporcionar como mínimo los siguientes servicios:

- Servicios de Certificación: Garantías de autenticidad, confidencialidad e integridad de los datos a través de una plataforma de certificación, gestión de usuarios, control de revocados, etc

- Servicios de certificación temporal y timbre digital

- Disponer de un conjunto homogéneo y compatible de soluciones criptográficas

- Asesoramiento y apoyo en cuanto a soluciones disponibles ante problemas que surjan en la implementación de otros proyectos

**Principales componentes de PKI**

En este apartado se describen las principales características de los distintos elementos que se deben interrelacionar correctamente para lograr una organización coherente de los sistemas de clave pública, ellos son:

- Una Autoridad de Certificación
- Certificados Digitales y listas de Revocación
- Pares de claves matemáticamente relacionadas, disponiendo encada par de una clave privada y una clave pública

Tales elementos se desarrollan dentro de una estructura formal determinada por:

- Políticas de Certificación
- Manuales de Procedimientos

Una Autoridad de Certificación representa al usuario que ha sido reconocido por el resto en un determinado entorno como certificador de las identidades digitales de todos. Es el órgano responsable de la emisión de los certificados, luego de una correcta verificación por los métodos que considere en la política de certificación. Es el principal proveedor de la tecnología de criptografía asimétrica. Debe contar con medidas de seguridad que infundan la total confianza requerida para considerara a su gestión seria y exitosa y ostentar altos niveles de calidad en la prestación y disponibilidad de sus servicios.

La función básica de una AC reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados.

Posibles maneras de identificar autoridades certificantes pueden ser:

- Por organización: la autoridad certificante emite certificados a individuos afiliados a una organización.

- Por residencia: emite certificados a individuos basándose en una dirección geográfica. Desde el punto de vista gubernamental podría decirse que asumen la responsabilidad por estos certificados en debido estado.

- Por persona: es un caso especial donde la certificación no reclama la inserción de su nombre en el certificado con una persona física o entidad. Está establecido par acomodar a usuarios que desean encubrir su identidad cuando hacen uso de las facilidades de seguridad.

Una Autoridad de Certificación puede valerse en su desempeño de Autoridades de Registro cuya misión es realizar meticulosamente la verificación de las personas (validación de identidad) que requieren la emisión de un certificado y realizar la solicitud formal pertinente (Registro de presentaciones). Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

Las Políticas de Certificación y los Manuales de Procedimiento rigen el funcionamiento general de la PKI definiendo cuestiones tan esenciales como el tipo de certificado a emitir por la Autoridad de Certificación, el alcance de la

información almacenada en el certificado, los procedimientos de registro, el tipo y alcance del compromiso de la Autoridad de Certificación con los usuarios y viceversa, las restricciones en el uso del certificado, etc. Además, en todo momento debe considerarse que su confección debe ser de total conformidad con lo estipulado en la legislación vigente sobre el tema.

La Publicación de certificados y de las listas de revocación de los mismos deben ser publicadas en un directorio, los usuarios de la PKI deben tener acceso para la comprobación de firmas. Además, se le debe prestar atención a la no publicación de datos sensibles.

La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de teletrabajadores o usuarios móviles.

### 3.3 Integración de IPSec con una PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso.

En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec.

Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de

forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3 como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado.

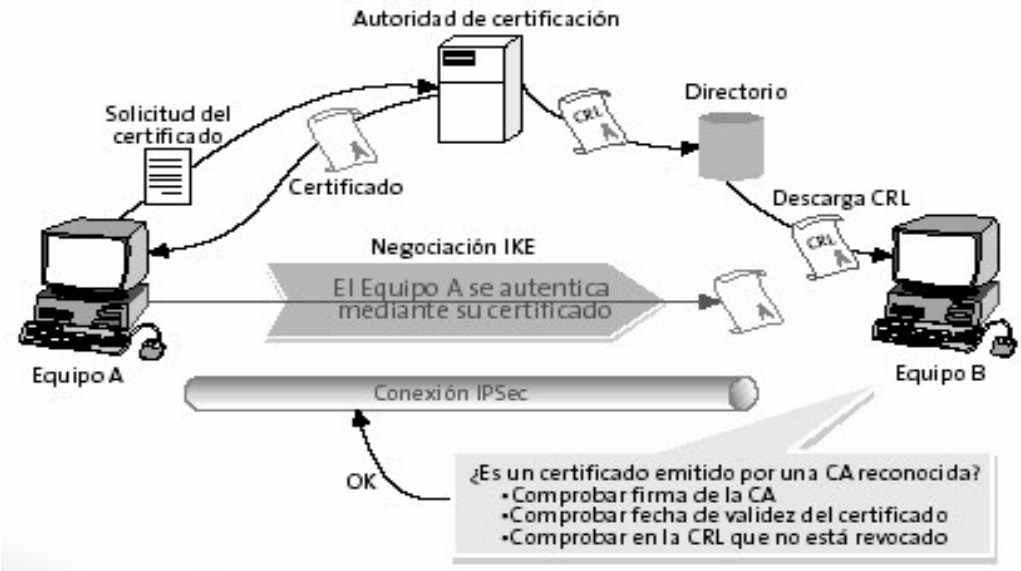
Esto hace que existan varias alternativas según el fabricante de que se trate. En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP al directorio de la PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Para la solicitud y descarga de certificados existe un protocolo denominado SCEP, que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

En la Figura 33 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

**Figura 30.** Integración de una PKI en IPSec




Fuente: Santiago Pérez Iglesias. **Análisis del protocolo IPSec.** Pagina 59.

## 3.4 Modos de uso y ejemplos de aplicación

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP.

A continuación veremos como el protocolo IPSec proporciona una solución viable para tres escenarios:

1. Intranet o Interconexión segura de redes locales.
2. Acceso seguro de usuarios remotos.
3. Extranet o conexión de una corporación con sus partners y proveedores.

### 3.4.1 Intranet

Conexión segura de redes locales o intranet se entiende una red de comunicaciones basada en una infraestructura de comunicaciones pública o privada que conecta todos los puntos de trabajo de una empresa y que tiene como medio común IP.

La mayoría de las corporaciones utiliza IP como medio de transporte universal, y las que todavía no usan IP tienen planes de migrar completamente a esta tecnología en un futuro próximo. Asimismo, la naturaleza distribuida de las empresas hace necesaria una infraestructura de comunicaciones que interconecte todas sus oficinas o puntos de venta.

En la Figura 31 se muestra un ejemplo de intranet en entorno financiero. Dicha intranet conecta todas las oficinas bancarias con el centro de proceso de datos (CPD) de un gran banco.

La seguridad es vital en este entorno, y los requisitos de confidencialidad e integridad de las comunicaciones se cubren perfectamente mediante el uso de la tecnología IPSec.

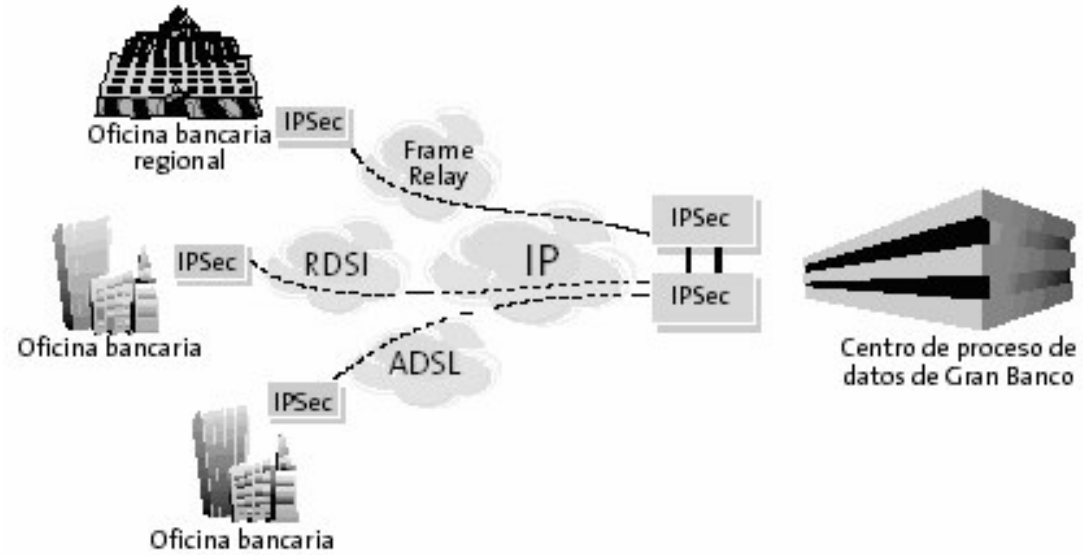
En la actualidad, incluso las oficinas bancarias más pequeñas disponen de una infraestructura informática que consta de una red local con varios PCs que usan una variedad de aplicaciones y protocolos para los que es imposible o muy costoso añadir mecanismos de seguridad. Sin embargo, todo el tráfico de esta red local está basado en IP o puede ser encapsulado en IP, de modo que la instalación de un *gateway* IPSec es la mejor solución para garantizar la seguridad de las comunicaciones de la oficina con el exterior.

Como puede observarse en la Figura 34, es habitual que las oficinas bancarias, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso.

Para grandes bancos con presencia multinacional y oficinas dispersas en muchos países esta diversidad será mayor, de forma que incluso podría plantearse la conexión de algunas oficinas directamente a través de *Internet*. En cualquier caso, IPSec garantiza la protección de las comunicaciones con independencia de la tecnología de acceso empleada. En cuanto al centro de proceso de datos, los requisitos críticos son la fiabilidad y la capacidad para mantener un elevado número de sesiones simultáneas.

En el mercado están disponibles *gateways* IPSec comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 25.000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las redes bancarias más grandes.

**Figura 31.** Interconexión de redes locales en entorno financiero




Fuente: Santiago Pérez Iglesias. **Análisis del protocolo IPSec.** Pagina 60.

### 3.4.2 Acceso seguro de usuarios remotos

La mayoría de las empresas necesitan proporcionar a sus usuarios algún procedimiento para el acceso remoto a los recursos corporativos. Estos usuarios con necesidades de acceso remoto pueden ser agentes de ventas, teletrabajadores o directivos en viaje de negocios; en todos los casos se requiere la necesidad de poder acceder de forma segura a los sistemas informáticos de la empresa a cualquier hora y en cualquier lugar, incluso en el extranjero.

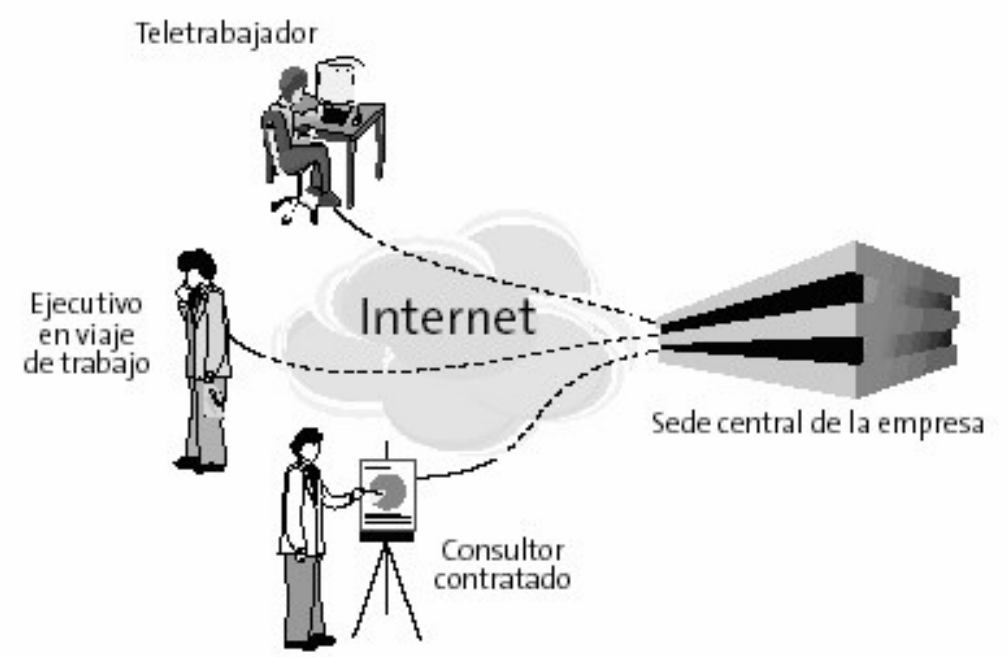
Además, las previsiones de futuro apuntan a que estas necesidades de acceso remoto van a crecer espectacularmente. La tecnología IPSec permite comunicar el PC del usuario remoto a las máquinas del centro corporativo, de modo que se soporten todas las aplicaciones IP de forma transparente. Mediante la instalación de un software en el PC, denominado "cliente IPSec", es posible conectar remotamente dicho equipo móvil a la red local de la corporación de forma totalmente segura, con la ventaja de que el usuario remoto, desde cualquier lugar del mundo, del mismo modo que si estuviese físicamente en su oficina, podrá:

- Leer y enviar correo.
- Acceder a discos compartidos en red.
- Acceder al servidor web corporativo.
- Consultar la agenda.

El uso del estándar IPSec permite garantizar la confidencialidad y la autenticación de las comunicaciones extremo a extremo, de modo que esta solución de acceso remoto se integra perfectamente con los sistemas de seguridad de la red corporativa.

En la Figura 32 se presenta un escenario típico de acceso remoto seguro a una corporación.

**Figura 32.** Acceso seguro de usuarios remotos a una corporación.




Fuente: Santiago Pérez Iglesias. **Análisis del protocolo IPSec.** Pagina 61.

En nuestro ejemplo esta corporación, o empresa, se dedica a la producción de software informático. Esta empresa, al igual que cualquier compañía del sector de las tecnologías de la información, comparte una serie de características únicas.

Podemos destacar la deslocalización de los recursos humanos, ya que cada vez es más habitual que los empleados trabajen fuera de su oficina, bien por estar en viaje de trabajo o bien por estar en su casa como teletrabajadores.

También será muy frecuente la colaboración en proyectos de consultores externos contratados, para los cuales es necesario habilitar acceso a los recursos de la empresa.

Dada la creciente competitividad en el sector informático, la protección de la propiedad intelectual, de la información estratégica y de nuevos productos, e incluso de la propia imagen de la empresa, imponen requisitos de control de acceso y de confidencialidad que hacen imprescindible la implantación de un sistema de acceso remoto que sea suficientemente seguro.

El protocolo IPSec permite construir una solución que cumple estos requisitos de seguridad. En este entorno, los usuarios remotos dispondrán de un software instalado en su PC de trabajo que les permitirá establecer una conexión segura con la red local de la compañía. La variedad de sistemas operativos no supone dificultad alguna, ya que todos los sistemas operativos recientes como Windows o Solaris incluyen un cliente IPSec.

Asimismo, para los sistemas operativos más difundidos, y que no integran IPSec, existen aplicaciones de cliente IPSec, tanto comerciales como de libre distribución. Incluso existe un cliente IPSec para Palm Pilot.

Para garantizar la seguridad de esta solución y evitar intrusiones, como las que han afectado a Microsoft y otras corporaciones en el pasado, es necesario complementar la tecnología IPSec con el uso, en los equipos remotos, de cortafuegos personales y autenticación fuerte mediante certificados digitales X.509 residentes en tarjeta inteligente.

Desde el punto de vista del administrador de la red informática de la corporación, los requisitos prioritarios serán la facilidad de gestión y la necesidad de autenticar de forma fiable a cada usuario. La integración de IPSec con una infraestructura de clave pública (PKI) proporciona una respuesta adecuada a estos requisitos.

### 3.4.3 *Extranet*

Por *extranet* se entiende una red de comunicaciones que interconecta a una empresa con todos los agentes con los cuales mantiene relaciones comerciales: consumidores, proveedores y *partners*.

En este escenario la interoperabilidad que ofrece el estándar IPSec es una ventaja clave frente a otras soluciones; cada empresa comprará equipos de fabricantes distintos, pero todos ellos podrán conectarse de forma segura utilizando IPSec como lenguaje común.

La tendencia actual es la aparición de *extranets* en las que convergen todas las empresas que participan en un mismo sector productivo. Previsiblemente, el comercio electrónico negocio a negocio (B2B) evolucionará en este sentido, para proporcionar puntos de encuentro virtuales en los que se establezcan relaciones comerciales de empresa a empresa de forma segura.

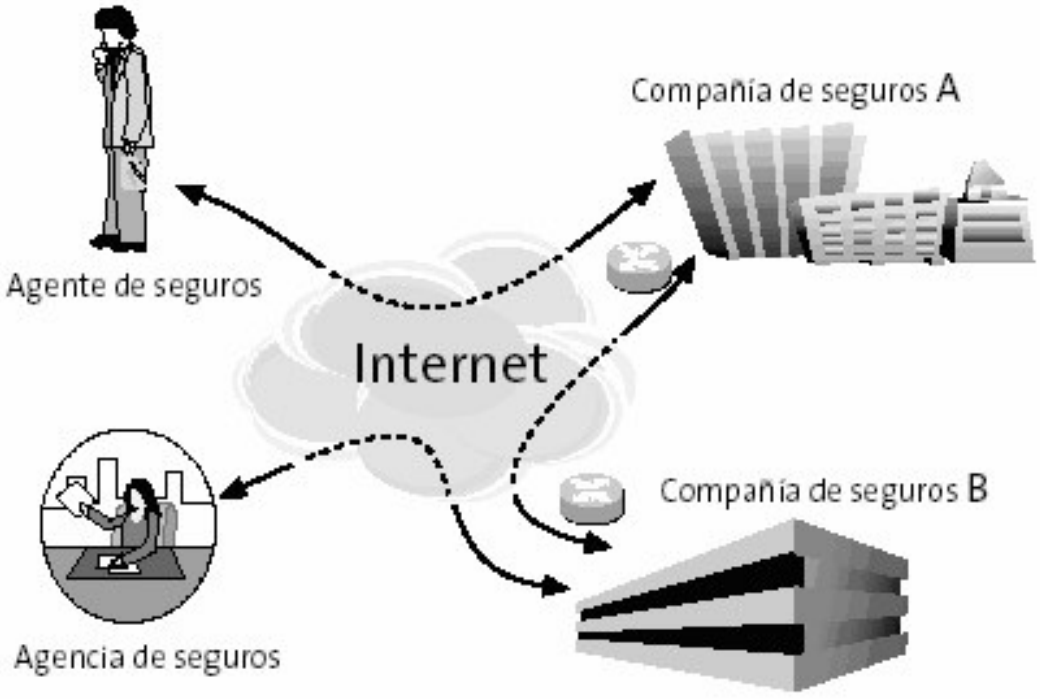
Estos mercados virtuales especializados se articularán de forma natural en torno a la elaboración de un producto o la provisión de un servicio concreto: fabricación del automóvil y el tipo de industria que lleva asociada, distribución y comercialización de alimentos, sector asegurador, etc.

En nuestro caso tomaremos como ejemplo el sector asegurador: una *extranet* que conecte las compañías aseguradoras y los agentes de ventas debe cumplir unos estrictos requisitos de seguridad, que incluso están regulados por normativas legales. Este es un ejemplo claro en el que IPSec aparece como la solución más apropiada, dado que es una tecnología avalada por estándares internacionales, garantiza la interoperabilidad entre los equipos

de distintos fabricantes y proporciona el más alto nivel de seguridad gracias a las técnicas criptográficas más modernas.

En la Figura 36 se muestra un esquema de una *extranet* para el sector de seguros. En dicha figura se puede observar como dos compañías se comunican de forma segura para intercambiar información sobre las pólizas de seguros. Al mismo tiempo los agentes de ventas y las oficinas de seguros pueden acceder a la información comercial necesaria para su negocio. Una *extranet* como esta puede llevarse a cabo perfectamente usando IPSec; para ello se requiere la instalación de un *gateway* IPSec en cada uno de los puntos de presencia de la *extranet*, mientras que el equipamiento de los agentes de ventas se reduce a un PC portátil con un cliente IPSec.

**Figura 33.** *Extranet* aplicada en el sector de seguros




Fuente: Santiago Pérez Iglesias. **Análisis del protocolo IPSec.** Pagina 62.

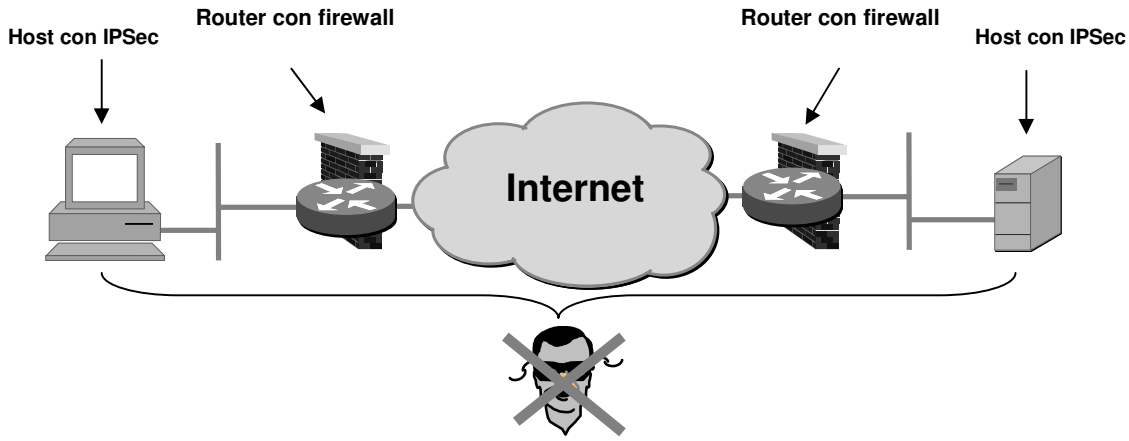
# 4. ANÁLISIS DE SEGURIDAD IPSEC EN IPV6

## 4.1 Funcionamiento de IPSec en IPV6

Para aplicar IPSec en IPV6 existen los siguientes modos de funcionamiento:

- Modo Transporte
- Modo Túnel

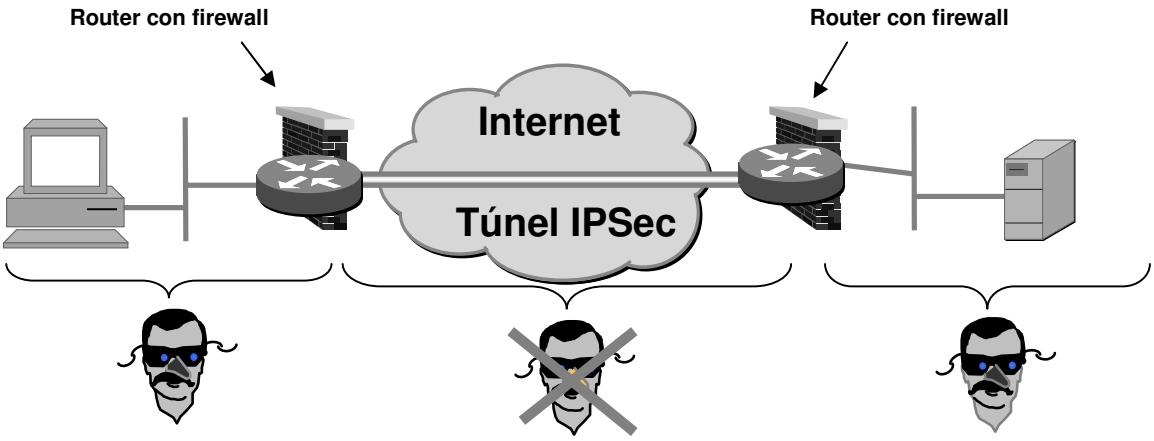
**Figura 34.** IPSec Modo Transporte




El la figura 34 se muestra un esquema en el cual se encuentran dos hosts de los cuales para que funcione el IPSec en modo trasporte, se tiene que implementar IPSec en ambos host, el cual se tiene una comunicación segura de extremo a extremo.

Para la figura 34 el cual nos muestra dos *routers* con *firewall* de los cuales ya se ha implementado el IPSec desde los hosts y con esto se asegura de un extremo al otro se tenga seguridad.

**Figura 35.** IPSec Modo Túnel




El la figura 35 se muestra un esquema en el cual se encuentran dos *hosts*, como también dos *routers* de los cuales para que funcione el IPSec en modo túnel, se tiene que implementar IPSec en ambos *routers* los cuales ejecutan una pasarela de seguridad. Este modo de funcionamiento de IPSec permite incorporarlo sin tener que modificar los *hosts*.

El IPSec utiliza dos protocolos para la protección de los paquetes IP, *Authentication Header* (AH), *Encapsulated Security Payload* (ESP), y el funcionamiento de IPSec en IPV6 se tiene las siguientes combinaciones:

- AH en modo trasporte
- ESP en modo transporte
- AH en modo túnel (Tiene el mismo efecto que en modo trasporte)
- ESP en modo túnel

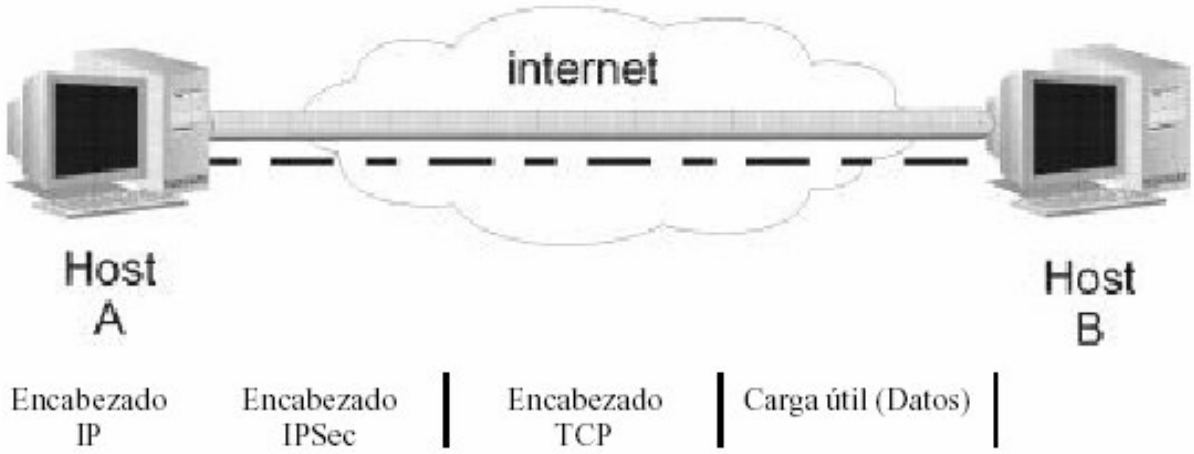
**Modo Trasporte**

El modo transporte,  este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP).

Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

En la figura 36 se describe el modo trasporte de IPSec, el cual consta de un *host* A y un *host* B, los cuales están comunicados en modo trasporte.

**Figura 36.** IPSec en Modo Trasporte




Con esto podemos resumir lo siguiente, para modo trasporte:

- Provee protección de los niveles superiores (*payload* de IP).

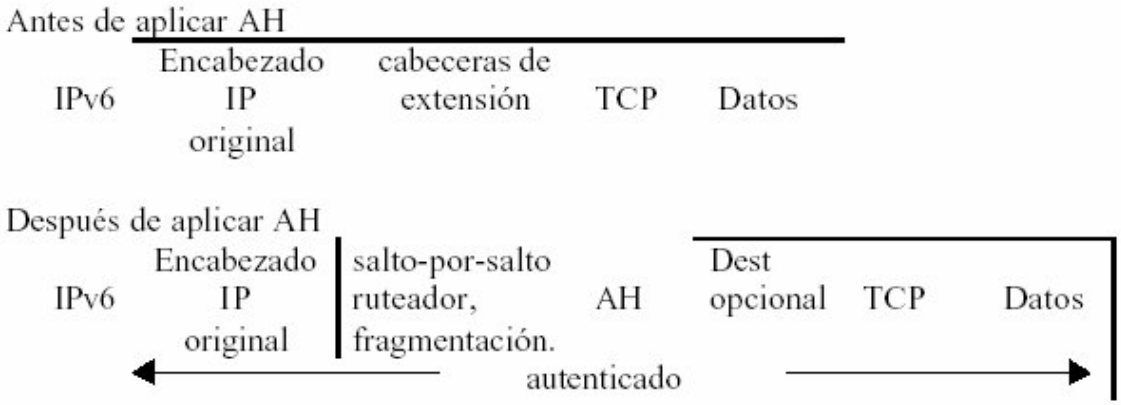
- Se utiliza en comunicaciones extremo a extremo entre *hosts*.
- ESP cifra y opcionalmente autentica el campo de datos de IP.
- AH autentica campo de datos de IP y parte de la cabecera.

- **AH en Modo Trasporte**

AH se inserta después de la cabecera IP, y antes del protocolo de capa superior (TCP, UDP, ICMP, ETC.) o antes de cualquier cabecera propia de IPSec que ya se haya incluido.

La figura 37 describe AH en modo trasporte para ipv6.

**Figura 37.** AH en Modo Trasporte en IPv6

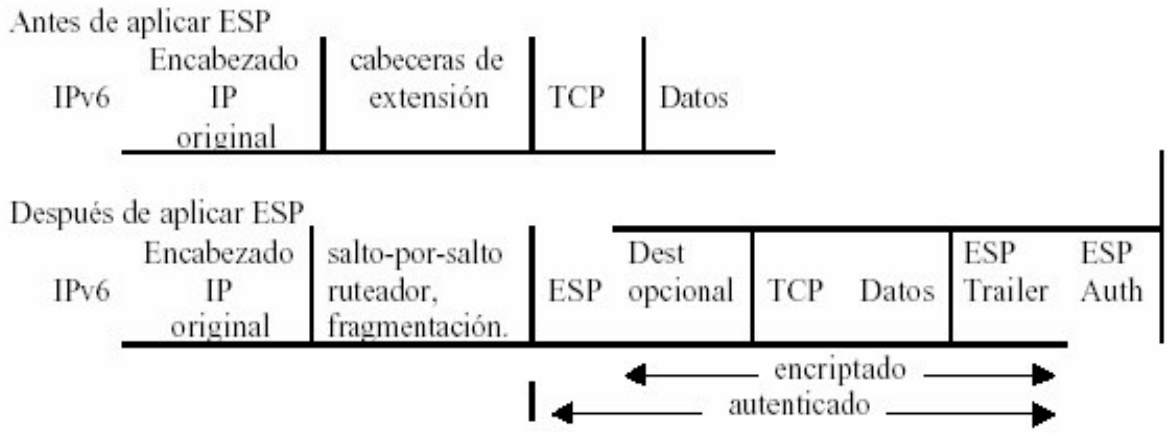



- **ESP en Modo Trasporte**

ESP se inserta después de la cabecera IP, y antes del protocolo de capa superior (TCP, UDP, ICMP,…) o antes de cualquier cabecera propia de IPSec que ya se haya incluido,

La figura 38 describe ESP en modo trasporte para ipv6.

**Figura 38.** ESP en Modo Trasporte en IPv6




**Modo Túnel**

En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red.

El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

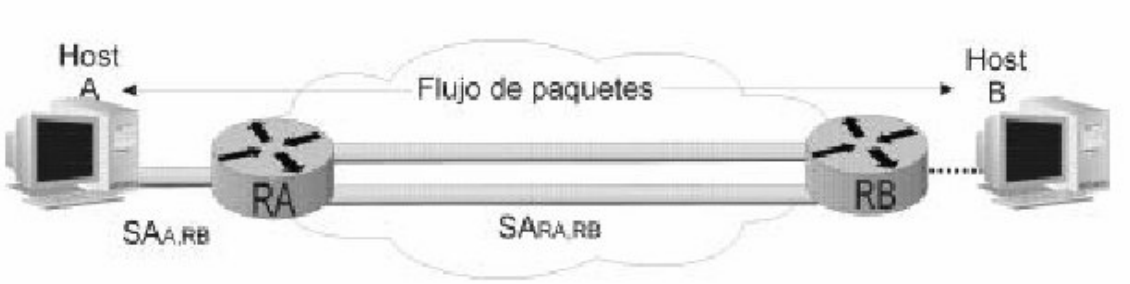
Este modo principalmente es empleado por los *gateways* IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo.

Cuando se utiliza ESP en modo túnel, se puede ocultar la identidad de los nodos que se están comunicando.

Como también, para ESP o AH, se pueden establecer Redes Privadas Virtuales (RPV) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en *Internet*.

En la figura 39 se describe el modo túnel de IPSec, el cual consta de un host A y un host B, los cuales están comunicados en modo túnel.

**Figura 39.** IPSec en Modo Túnel




Con esto podemos resumir lo siguiente, para modo túnel:

- Provee protección del paquete IP completo.
- Se trata criptográficamente un paquete entero con cabecera IP y de seguridad.
- Se añade un cabecera IP exterior.
- Los *routers* no tienen acceso a la cabecera interior.
- La cabecera exterior puede tener direcciones fuente y destino diferentes a la interior (encapsulada).
- Se utiliza entre extremos SA que son *routers* o *firewalls* con IPSec.

- Los *hosts* detrás del *firewall* pueden implementar comunicaciones seguras sin tener IPSec (su *firewall* implementa el túnel seguro con el *firewall* de la red de destino).
- ESP cifra y opcionalmente autentica el paquete IP interno.
- AH autentica el paquete IP interno y parte de la cabecera IP externa.

- **AH en Modo Túnel**

En éste modo la cabecera interna posee el origen y destino finales, mientras que la cabecera interna posee direcciones distintas (las de las puertas de enlace).

La cabecera AH protege a toda la cabecera interna, incluida la totalidad de la Cabecera IP interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transferencia.

La figura 40 describe AH en modo túnel para ipv6.

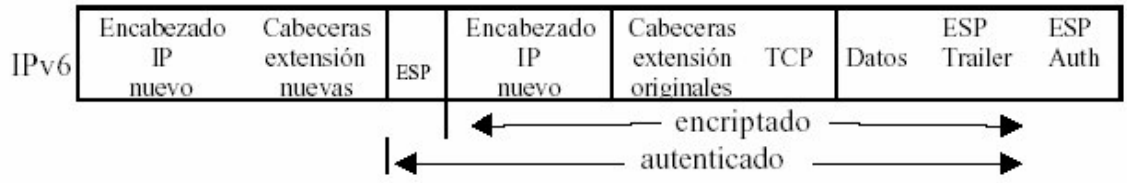
**Figura 40.** AH en Modo Túnel en IPv6


- **ESP en Modo Túnel**

En éste modo la cabecera interna posee el origen y destino finales, mientras que la cabecera interna posee direcciones distintas (las de las puertas de enlace). ESP protege a toda la cabecera interna, incluida la totalidad de la Cabecera IP interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transferencia.

La figura 41 describe ESP en modo túnel para ipv6.

**Figura 41.** ESP en Modo Túnel en IPv6




## 4.2 Métodos de Trabajo

Existen varios métodos de trabajo para implementar IPSec, de los cuales detallaremos cuatro:

- Seguridad extremo-a-extremo.
- Redes privadas virtuales.
- *Road Warrior*
- Túneles anidados

- **Seguridad extremo-a-extremo.**

Este método de trabajo no es de los mas comunes, este consiste en tener un túnel donde se conectan los *routers* e entre ellos. Cada *hosts* esta conectado por un túnel a su *router* respectivo.

Este método de trabajo no es muy recomendable para las empresas, porque se requiere de un túnel de conexión entre cada *hosts*.

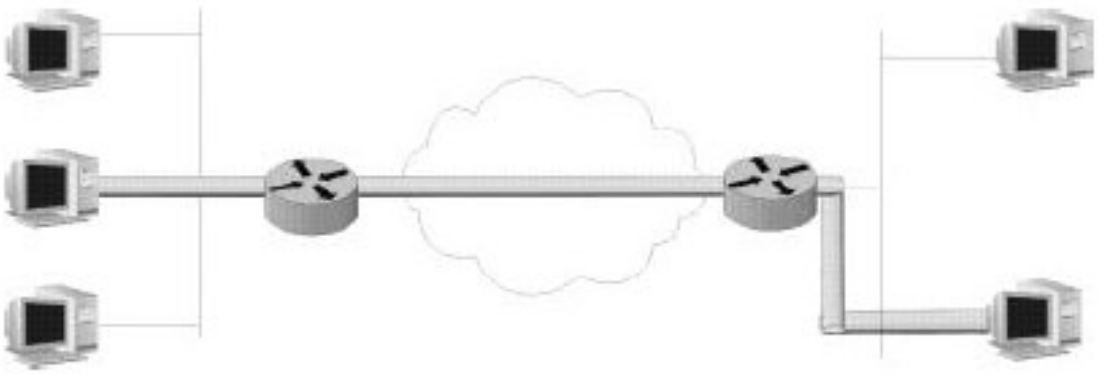
Es un método muy seguro porque se tiene perfecto control sobre la maquina que se requiere seguridad si en dado caso ese es el objetivo.

Los costos soy muy elevados en la implementación, dado la implementación de cada túnel sobre cada *host*.

La seguridad que se logra es de extremo a extremo, es decir de *host* a *host*.

La figura 42 muestra un diagrama del método de trabajo de IPSec de seguridad extremo a extremo.

**Figura 42.** Método de trabajo de IPSec en IPV6, seguridad extremo a extremo



- **Redes privadas virtuales.**

Una red privada virtual (*Virtual Private Network*) es uno de los mas implementados, donde mediante un proceso de encapsulación, y en este caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte.

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a *Internet* público, todo esto con la seguridad que provee IPSec para la transportación de sus datos.

Las implementaciones de VPN conjuntamente con IPSec representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos.

Reduce significativamente el costo de la transferencia de datos de un lugar a otro, con una buena implementación y configuración de IPSec las empresas sacan provecho de todas las ventajas que el IPSec provee.

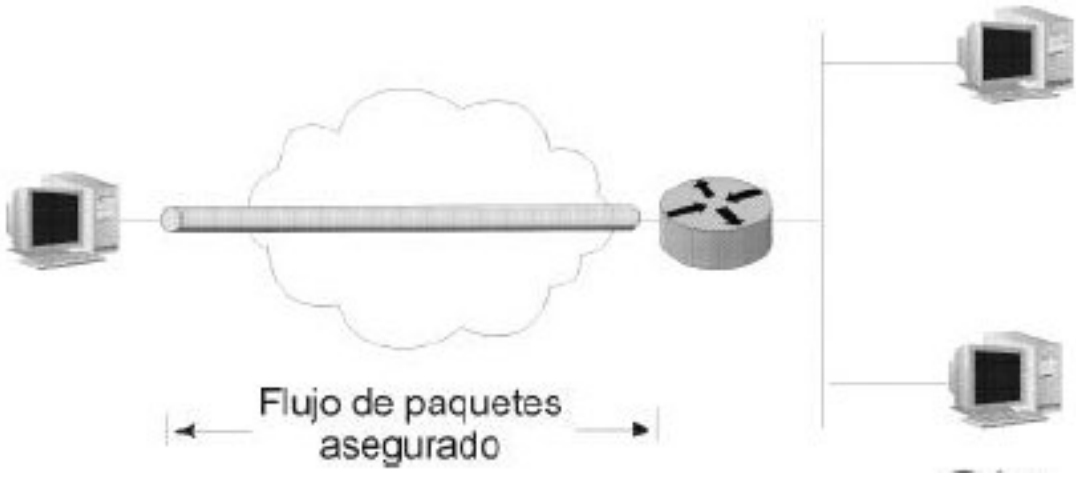
**Figura 43.** Método de trabajo de IPSec en IPV6, redes privadas virtuales

- ***Road Warrior***

Los trabajadores que pasan gran parte del tiempo fuera de la empresa, como teletrabajadores o los llamados "*road warriors*", personas que necesitan acceder a la red de la empresa pero que están constantemente cambiando de ubicación.

Ahora lo que se permite es a un ordenador personal o portátil el acceso a la red corporativa, manteniendo la privacidad.

**Figura 44.** Método de trabajo de IPSec en IPV6, *road warrior*




- **Túneles anidados**

Este método de trabajo de IPSec, no es muy recomendable, por lo complicado de su construcción, mantenimiento y consume de recursos de red.

Un ejemplo que se puede describir en la figura 45 es, el *host* A envía un paquete al *host* B, la política indica que debe ser autenticado con el *router* RB, donde existe una VPN entre el *router* RA y RB.

**Figura 45.** Método de trabajo de IPSec en IPV6, túneles anidados


## 4.3 Vulnerabilidades

El protocolo IPSec es un excelente paso para implementar seguridad principalmente como esta el *Internet* hoy en día.

Pero nada puede estar 100% seguro, existen errores, malas implementaciones, configuraciones erróneas, pueden que hallan fallas en diversas circunstancias.

Si se implemento y configuro correctamente el IPSec, los protocolos pueden proveer de un *e-bussines*, donde se protegerán y estarán listos para defenderse, que tendrán seguridad en sus datos.

Bien implementado y configurado correctamente pueden aprovechar la velocidad y el alcance del *Internet* sin que estén propensos a los peligros de un ataque.

Al rentar líneas dedicadas seguras, son muy costosas, para esto se pude implementar muy bien IPSec para reducir el costo así como también tener la seguridad requerida.

IPSec esta compuesto por una estructura de criptografía, fundamentos de red y un conjunto de protocolos definidos por la RFCs, los cuales pueden ser usados o implementados por distintos vendedores en diversas maneras.

Una vulnerabilidad que se pasa por alto muy a menudo es la de los algoritmos, el algoritmo DES es una clara evidencia, los datos se incrementan y cada vez es mas fácil descifrarlos, para evitar esto hay que hacer que los algoritmos cambien continuamente.

Los protocolos de IPSec tienes en cuenta esto, donde se tienen opciones a especificar algoritmos obligatorios.

Pero la implementación de estos algoritmos o requisitos es responsabilidad del implementador, que debe estar conciente de que funcionan correctamente.

*Existe una organización llamada TruSecure Corporation*, es una división de ISCALabas, esta se enfoca en certificar productos IPSec, que se implementen y cumplan con el RFCs para IPSec. Como IPSec es relativamente una nueva tecnología, que próximamente se vera muy común con la venida del IPV6, es muy importante que exista una organización como esta que certifique y de credibilidad sobre el IPSec.

**Ejemplos de ataques al IPSec**

Existen numerosas especulaciones y escenarios donde se define el protocolo para que opere el IPSec, donde cada uno de ellos puede ser desafiado puesta en prueba la seguridad.

Pero examinaremos dos, los cuales son los que se podrían llevar a cabo en el mundo real

Para esto definimos dos ataques:

- *Cut-And-Past Attack*
- *Session Hijacking*

***Cut-And-Past Attack*:**

Este ataque solo es posible en dos redes que utilizan IPSec y un túnel entre dos *routerds* que comunican las redes. Donde el requisito es si el atacante tiene acceso al segundo host entre las dos redes.

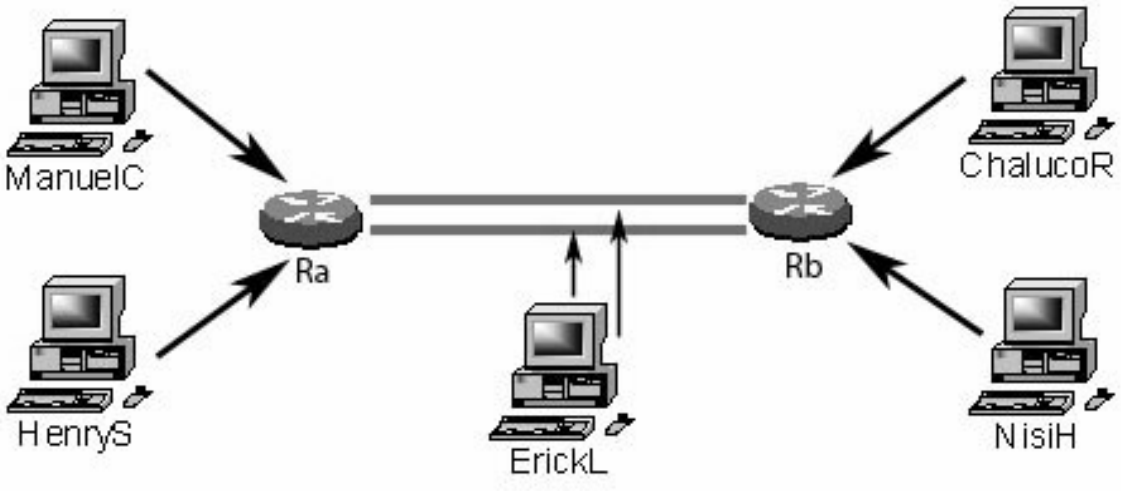
El ataque consiste en que ErickL tiene un *sniffer*, con el cual logra atrapar un paquete encriptado proveniente de ManuelC a ChalucoR. ErickL sigue con el *sniffer* y atrapa también un paquete enviado de HenryS a NisiH.

ErickL copia datos cifrados de un paquete de ManuelC en un paquete de HenryS para NisiH. El router B trata de descifrar el paquete de ManuelC para ChalucoR y lo envía a NisiH. Esta parte no es tan facil como pareciera puesto que algunos otros requisitos referentes a los números de serie usados en paquetes de IPSec y se tiene que asegurar que el paquete de ManuelC es genuino y no llegue al *router* B si los paquetes son falsos.

IPSec incluye varios métodos de protección para el *replay-attack*, siendo estos una dificultad mas para realizar este ataque.

La figura 46 ilustra lo explicado anteriormente.

**Figura 46.** Vulnerabilidad, diagrama de ataque *Cut-And-Past Attack*




***Session Hijacking***

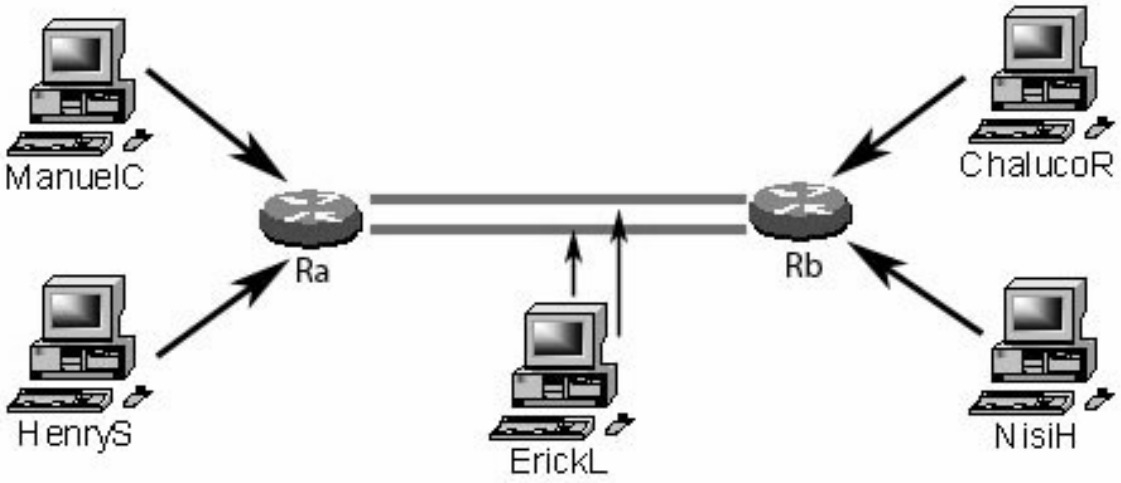
Este ataque es similar al anterior ataque, HenryS puede crear paquetes que se intenten llegar a ChalucoR pero como si fueran enviados por ManuelC.

En vez de robar el paquete de ManuelC y de pedir al router B desencriptar el paquete de NisiH, ErickL ahora pega los datos de HenryS en el paquete de ManuelC, y este es descifrado por el *router* B y mandado hacia ChalucoR como si viniera de ManuelC.

Este ataque es mucho mas complicado para hacerlo en la practica, la secuencia de números y otras autenticaciones deben ser superados, a pesar de esto los ataques pueden ser factibles.

La figura 47 ilustra lo explicado anteriormente.

**Figura 47.** Vulnerabilidad, diagrama de ataque *Session Hijacking*




**Vulnerabilidades en los protocolos subyacentes o los *Host***

El protocolo IPSec confía en un gran número de tecnologías subyacentes para alcanzar la encriptación y autenticación.

Una asociación de seguridad, en su estado inicial se puede completar usando *Key Exchange methods* este definidos por otros protocolos.

Esto es un requerimiento para almacenar llaves y certificados en el sistema local, *host*. El algoritmo como Diffe-Helman se utiliza estableciendo y compartiendo un secreto entre los dos *host*. La vulnerabilidad en este especifico método para intercambio de llaves (*key Exchange*), en *hashing* o el algoritmo de encriptación, pueden fácilmente afectar la seguridad de IPSec.

Ahora se acepta el algoritmo de encriptación DES, y ahora es susceptible a los ataques de fuerza bruta (donde los ataques de fuerza bruta tratan de desencriptar los datos simplemente intentando cada valor posible) usando software y hardware. Si la protección que rodea al SADB fue quebrantada, entonces cada llave y los enlaces de IPSec que usan la base de datos pueden ser fácilmente obtenibles.

Incluso si existe un túnel seguro entre los dos hosts para un tipo de trafico especifico, si los *hosts*, ellos mismos se comprometen a una conexión separada no protegida, entonces todos los datos protegidos pueden estar disponibles para el atacante.

La localización y supervisión de los enlaces creados por IPSec son críticos. IPSec es simple, puede combinar una herramienta con otras medidas de seguridad tales como sistemas de detección de intrusos o *Host* Intrusión *Detection Systems* (HIDS), se puede configurar un *firewall* y otros mas.

## 4.4 Ventajas y Desventajas

El IPSec nos ofrece varias ventajas y algunas desventajas, pero esto es según cada caso, cada escenario que se presente.

A continuación las ventajas que nos ofrece:

1. El protocolo IP carece de seguridad, el IPSec vino a solventar dicha carencia, por lo que se ha convertido en el protocolo de seguridad muy potente y flexible.

2. Es una extensión del protocolo IP, lo cual no se tiene que cambiar a otra tecnología de comunicación además ofrece servicios criptográficos de seguridad basados en estándares definidos por el IETF, esto es muy importante porque genera un estándar común para todos, no dependiendo del fabricante, hardware, software o la plataforma.

3. EL IPSec es obligatorio en el protocolo IPV6, esto hace que estas sean más seguras.

4. Seguridad independiente de la aplicación, IPSec es la solución ideal para aquellos escenarios en que se requiera seguridad, independientemente de la aplicación, ofrece una implementación transparente sobre las aplicaciones. Con esto disminuye el impacto de implementación o los cambios posteriores a la implementación.

5. Puede ser transparente al usuario, donde se puede implementar IPSec sin modificar los host finales. Un ejemplo es el uso de IPSec en *routers*, donde los hosts finales pueden transferir datos entre ellos con la ayuda de los routers que a su vez tienen toda la seguridad que ofrece IPSec.

6. IPSec ofrece los servicios de integridad en las conexiones, garantía de que los datos recibidos por el receptor de la comunicación coinciden con los enviados por emisor, para conseguir estos objetivos IPSec ofrece dos mecanismos de seguridad que pueden usarse por separado o de modo conjunto, la cabecera de autenticación AH (*Autentication Header*) y la

cabecera de encapsulamiento de carga segura ESP (*Encapsulating Security Payload*).

7. IPSec es flexible y se adapta a nuestras necesidades, según sea el caso o escenario se pude implementar en dos modos de uso para cada cabecera, modo trasporte y modo túnel, en el primer caso se ofrece seguridad tanto a los protocolos de nivel superior como a las partes de la cabecera del datagrama IP no variables durante el camino del paquete, mientras que en el segundo se ofrece seguridad a todo el datagrama mediante el encapsulamiento de un paquete de nivel de red dentro de otro paquete de nivel de red.

8. Los costes directos, este es el caso de implementarlo en modo túnel, donde no se requiere de un costo sobre los usuarios.

9. IPSec ofrece encriptación y autenticación a nivel de red, a su vez estas dos forman parte del conjunto de tecnologías que combina IPSec para su seguridad, como Diffie Hellman, encriptación clave pública, DES, funciones *hash*.

10. Ofrece poca sobrecarga de procesamiento según sea el caso o el escenario, cuando se implementa ESP en modo trasporte, ofrece poco procesamiento, pero cuando se utiliza ESP en modo túnel, pero esto incrementa la carga de procesamiento.

11. IPSec al ser implementado, ofrece seguridad para un flujo concreto de un determinado usuario, con esto podemos darle seguridad a un determinado usuario donde se puede hacer desde el inicio hasta el fin de la transmisión de datos.

12. La reducción de administradores de red en capacitación, implementación, administración. Un ejemplo que a las personas encargadas de la implementación de IPSec, que si lo realizan en modo túnel, solo a ellas y nadie mas se tendría que darle capacitación, como también para administrar dicha implementación serian solo ellos.

13. Reducción de equipos, donde se puede dar una ventaja competitiva en el coste de nuevos equipos, se podría reducir a tal grado que al implementar IPSec los usuarios finales no tendrían que cambiar a nuevos equipos que se adapten a el, como también el equipo adicional debajo de los *routers*.

Las desventajas del uso de IPSec son muy pocas, porque en el esta un conjunto de protocolos y tecnologías, es modular, consta de varias alternativas en su configuración. Puede que en alguno de ellos exista una desventaja para un caso o escenario en particular, pero implementando la alternativa puede que ya no halla dicha desventaja.

Las desventajas que se presentan en el uso de IPSec son:

1. Es complejo porque se necesita mucho conocimiento de distintas tecnologías y protocolos para su implementación. Como esta compuesto el IPSec de ellas, se tiene que saber que opciones seleccionar, que tecnología o protocolo se adapte mejor a nuestro caso o escenario.

2. La mala implementación del IPSec puede llevar a no tener seguridad, y que no funcione todo en conjunto el IPSec.

3. La sobrecarga de procesamiento, se produce cuando se implementa de mala manera IPSec con modo túnel utilizando el protocolo ESP

4. Puede no brindar seguridad para los casos y escenarios donde se implementa en modo túnel, porque existiría inseguridad en los routers.

5. Puede llegar a consumir gran parte los recursos de red y degradar el rendimiento de la misma, cuando se implementa de mala manera o se utiliza demasiados túneles anidados.

## 4.5 Recomendaciones sobre el uso de IPSec en IPV6

Para que IPSec funcione de manera eficiente y se adapte muy bien a nuestras necesidades, podemos seguir los siguientes puntos:

1. Hacer un análisis de requerimientos completo.

2. Analizar la mejor opción a seguir, seleccionando cada protocolo o tecnología que se compone IPSec que mejor se ajuste al caso o escenario.

3. Se debe de tener conocimiento de las distintas tecnologías que se acoplan o se integran a IPSec, para tomarlas todas en cuenta y decidir de la mejor manera. Cisco ofrece un conjunto de tecnologías sobre IPSec, será un buen punto de partida.

4. Un plan de implementación donde se tenga los pasos a seguir a implementar IPSec, separados secuencialmente según sea prerrequisito de alguno, por ejemplo:

   Estos pasos generales para implementar IPSec en el sistema operativo Linux:

   a. Parchar y recompilar el *kernel* con soporte para *FreeS/Wan*, añadiendo soporte para IPSec, y los algoritmos de cifrado a implementar.
   b. Generar claves RSA.
   c. Configurar el archivo ipsec.conf con las directivas a utilizar.
   d. Activamos una conexión que se halla definido, con esto ya tendremos una *sesion* IP cifrada entre los equipos que hallamos configurado.

5. Capacitarse sobre IPSec, sus tecnologías y protocolos, para no cometer errores que más tarde se convierten en vulnerabilidades, Cisco una de las empresas que mas provee hardware que soporta IPSec ofrece cursos de capacitación.

6. Si se requiere poco procesamiento de datos se utilice el IPSec en modo transporte.

7. Conocer los estándares definidos por el IETF que se basa IPSec, antes de la implementación, cerciorarse de que el hardware y el software a ser usados por IPSec cumplan los estándares establecidos. Todo esto para que sea todo totalmente compatible, no importando el fabricante, hardware, software o la plataforma.

8. Basarse en los métodos de trabajo de IPSec, seguridad extremo a extremo, redes privadas virtuales, *road warrior*, túneles anidados, estos varían en su implementación, pero se puede crear una buena base a partir de ellos y crear la solución que se adapte a nuestras necesidades.

9. Definir bien las directivas de IPSec, donde las directivas consisten en un conjunto de filtros, acciones de filtrado y reglas a utilizar en nuestra implementación.

10. El uso de IPSec conjunto con un *firewall* nos puede dar mayor seguridad y puede resolver los siguientes casos:

    - Como el IPSec no puede controlar el comportamiento del usuario, el puede compartir sus claves como enviar datos confidenciales con destino un *host* fuera de la empresa, con el *firewall* permitiría el acceso específicamente a *hosts* de la red.

    - Como todo administrador de red puede tener errores, donde a mayor sea la red es posible que se pase por alto un *host*, o un servidor por el cual no se tenga seguridad. El *firewall* formaría una barrera para aquellos que no son los de nuestra red o los permitidos.

    - *Firewall* protege a los servidores de debilidades, permitiendo el acceso solamente a los servidores que se sabe que son seguros y denegando el acceso a los otros servidores.

11. El uso de certificados para la autenticación de dispositivos, puede ser la mejor opción a utilizar, algunas veces. La idea con los certificados es tener una CA (*Certificate Authority - Autoridad Certificante*) que actúa de validadora de certificados, si un certificado (que provenga de cualquier lado en *Internet*) esta firmado por la CA en la que nosotros confiamos, entonces asumimos que este certificado es un certificado válido. Por otro lado, y antes de asumir la validez de un certificado firmado, se revisa lo que se llama la CRL (*Certificate Revocation List* - Lista de Certificados Revocados), que es un archivo donde están todos los certificados en los que no se confia más (y que han sido firmados en algún momento por nuestra CA), en esta lista van a parar todos los certificados que por alguna razón han sido comprometidos.

Pero además hay que tener en cuenta consideraciones técnicas sobre el uso de IPSec:

**Autenticación de dispositivos**

Utilizar certificados X509 para la autentificación de dispositivos, por las siguientes razones:

- Es el método más seguro.
- Es el método más dimensionable.

Como también la generación de claves RSA de 1024 bits, y la utilización del algoritmo DH.

**Integridad de datos**

Para la autentificación de paquetes se puede utilizar muy bien el protocolo AH como el ESP, pero se puede tomar en cuenta lo siguiente:

- Las pruebas indicaron que ESP consume el mismo volumen de recursos del CPU que AH.

- Con el protocolo ESP podemos asegurar la encriptación de paquetes.

Y se recomienda la utilización de HMAC con ESP para la autentificación de paquetes, como también puede ESP-HMAC-MD5 como ESP-HMAC-SHA.

**Encriptación de datos**

Cualquier encriptación de datos consume recursos del CPU, pudiendo para algún caso o escenario omitirse. No omitirse en un caso donde se necesite la encriptación esto es totalmente no recomendable, sino que en algunos no es necesaria, con el simple establecimiento de autentificación de paquetes se puede proporcionar la seguridad que se requiere.

Por lo que se recomienda para estos casos, la utilización de NULL con ESP, donde ESP se aplicara al paquete sin encriptación.

Pero en dado caso se necesita encriptar los datos, se recomienda implementar ESP-3Des, que es mas seguro que DES.

**El equipo con capacidades IPSec**

Existen equipos con capacidades de implementación de IPSec, para el caso de los equipos con capacidad IPSec se pude tomar en cuenta lo siguiente:

- Por razones de dimensionabilidad, el dispositivo debería tener capacidades IKE, y debería ser compatible con la norma de certificación X509.

- Es importante que el dispositivo admita el método de encriptación ESP_NULL.

- En el otro caso, donde se requiere la encriptación de los datos, el equipo debería tener las capacidades de hacerlo y recomendamos 3DES. Estimando que AES puede ser el estándar de encriptación mas popular en un futuro, es deseable que se tenga capacidades AES.

- Si se tiene una alta velocidad de conexión a *Internet*, es recomendable un dispositivo VPN/IPSec con tarjeta de encriptación (tarjeta aceleradora), ya que con esto reduce considerablemente el volumen de proceso de la CPU cuando se utiliza el protocolo IPSec.

- Implementar IPSec en dispositivos con capacidades para ello, que contiene varios protocolos y estándares en los cuales se rigieron, es mucho mas rentable y fácil la configuración que en equipos donde se tenga la solución a implementar.

## CONCLUSIONES

1. El IPSec está formado por un conjunto de protocolos y algoritmos modularmente, con lo que se puede implementar en distintas formas, seleccionando el protocolo o algoritmo que mayor se adapte a nuestras necesidades.

2. El IPSec es muy seguro, pero con una mala implementación puede que no sirva de nada toda la configuración de los distintos módulos que comprende. La mala implementación se debe a factores humanos, físicos, procedimientos, organización, pasos, requerimientos etc.

3. IPSec puede ofrecer seguridad a una red o sólo en un computador en específico, según sea la implementación en modo túnel que proporciona seguridad extremo a extremo donde se tiene que implementar IPSec en los computadores, en modo transporte que proporciona seguridad a toda la red que se conecte a los *routers* en los cuales se implemento IPSec.

4. IPSec está basado en estándares definidos por el IETF, no existirá problemas de compatibilidad, es independiente del fabricante, hardware, software o plataforma en que se implementó.

5. El IPSec es un estándar de seguridad, flexible y potente, es modular, flexible porque se pueden implementar y adaptar a cualquier circunstancia, siendo modular para poder seleccionar de un conjunto de protocolos para su implementación, y potente por la arquitectura que lo conforma.

6. IPSec permite a las aplicaciones operar de forma remota con un acceso seguro y transparente; donde se ofrece el mismo nivel de confidencialidad que dispondría en la red local de su empresa. Muchas de estas aplicaciones dedicadas al comercio electrónico IPSec las lleva a niveles más seguros.

## RECOMENDACIONES

1. Para que nuestra red esté segura hay que utilizar un conjunto de tecnologías y protocolos modularmente que lo vuelve muy potente y flexible.

2. Para la implementación de IPSec hay que tener conocimiento amplio de todas las tecnologías, protocolos que podemos utilizar, para escoger la mejor que se adapte a nuestro caso o escenario, el hardware que podemos utilizar para la implementación de IPSec, como también nuevas tecnologías que se adaptan a él.

3. El IPSec soluciona varios problemas de seguridad, pero hay que mantener actualizados los módulos que éste comprende para evitar posibles vulnerabilidades.

4. IPSec es obligatorio para IPV6 pero también se puede implementar en IPV4, éste sería un buen inicio para las empresas que no planean implementar IPV6 y necesitan seguridad. El IPSec es compatible con IPV4 o soportado en él.

5. Motivar a entidades públicas o privadas, a la implementación del protocolo IPV6; donde se desarrollen nuevas redes, servicios y aplicaciones sobre IPV6 para así, poder ofrecer toda la seguridad de IPSec.

6. IPSec es un estándar que proporciona servicios de seguridad a la capa IP, pero algunas veces no es suficiente, también hay que establecer políticas de seguridad en la empresa, planes de contingencia, planes de

reacción, como también el monitoreo constante de la red, con esto se tendría más control y más seguridad sobre la red.

# BIBLIOGRAFÍA


1. Seguridad de las redes y de la información
   **http://216.239.39.104/search?q=cache:1jNDJBdVtZoJ:europa.eu.int/information_society/eeurope/2002/news_library/pdf_files/execsum_es.pdf+seguridad+informacion+redes+ataques&hl=es&ie=UTF-8**

2. Evaluación Seguridad de un Sistema de Información
   **http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml**

3. Ataques a nuestra información, cuales son las amenazas?
   **http://216.239.39.104/search?q=cache:Ou9gTcyBW_0J:www.nextvision.com/notas/ATAQUES_A_NUESTRA_INFORMACION.pdf+seguridad+informacion+ataques+contramedidas+acciones&hl=es&ie=UTF-8**

4. Redes paranoicas contra ataques
   **http://216.239.39.104/search?q=cache:0f_7rSMbdcEJ:www.idg.es/comunicaciones/especial-avether160/Pag11.pdf+seguridad+informacion+redes+ataques&hl=es&ie=UTF-8**

5. FUNDAMENTOS DE SEGURIDAD
   **http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO/TEMA_3.htm**

6. Evaluación Seguridad de un Sistema de Información
   **http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml**

7. Amenazas deliberadas a la seguridad de la información
   **http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html**

8. Clasificación y tipos de ataques contra sistemas de información
   **http://www.delitosinformaticos.com/seguridad/clasificacion.shtml**

9. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN
   **http://216.239.39.104/search?q=cache:jo51PvO7RoMJ:www.textil.org/extranet/inf/Revista10/paginas/8seguridad.pdf+contramedidas+seguridad+informacion+red&hl=es&ie=UTF-8**

10. Gestión de la seguridad
**http://www.rediris.es/cert/doc/unixsec/node31.html**

11. Modelo OSI
**http://www.monografias.com/trabajos13/modosi/modosi.shtml**

12. Modelo OSI
**http://www.ilustrados.com/publicaciones/EpyFyuVkZZfOjDVDQL.php**

13. El Modelo de referencia OSI de telecomunicaciones
**http://www.geocities.com/txmetsb/el_modelo_de_referencia_osi.htm**

14. El modelo OSI
**http://www.pchardware.org/redes/redes_osi.php**

15. Introducción a IPv6
**http://216.239.39.104/search?q=cache:lpSaRlJ24alJ:web.frm.utn.edu.ar/codarec/ipv6/Filminas/ipv6-UNLP.PDF+introduccion+ipv4+ipv6+&hl=es&lr=lang_es&ie=UTF-8**

16. Introducción a TCP/IP Direccionamiento y ruteo
**http://216.239.39.104/search?q=cache:yvCscB6xJjEJ:www.galeon.com/jorhack/JL-Picard/JL-Books/IntroTCP-IP.pdf+introduccion+ipv4+ipv6+&hl=es&lr=lang_es&ie=UTF-8**

17. Introducción al Protocolo IPv6
**http://216.239.39.104/search?q=cache:Uq_MtTMdVlMJ:internetng.dit.upm.es/ponencias-jing/2001/david-fernandez.PDF+introduccion+ipv4+ipv6+&hl=es&lr=lang_es&ie=UTF-8**

18. IPv6, descubriendo el protocolo
**http://ranty.pantax.net/~ghe_rivero/documentos/ipv6/node1.html**

19. Verdejo Alvarez, Gabriel. **El protocolo IPv6 y sus extensiones de seguridad IPSec.**

20. IPv6: El protocolo del *Internet* de la nueva generación
**http://www.eveliux.com/articulos/ipv6.html**

21. PROCEDIMIENTOS DE SEGURIDAD POR CAPAS PARA INCORPORAR REDES LAN INALÁMBRICAS A INTRANETS
**http://64.233.161.104/search?q=cache:XoAmm5CKM-YJ:www.ajoomal.com/Securizar%2520en%2520una%2520red%2520Wireless.pdf+seguridad+por+capas+de+red&hl=es&ie=UTF-8**

22. Enrique de la Hoz de la Hoz. **Autenticación.**

23. Protocolos de Red: Protocolo TCP/IP
**http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml**

24. SECURE SOCKET LAYER (SSL)
**http://www.geocities.com/CapeCanaveral/2566/ssl/ssl.html**

25. PROTOCOLO SSL
**http://www.geocities.com/CapeCanaveral/2566/ssl/ssl1.html**

26. RSA y PGP : Sistemas para la Seguridad en la Red
**http://cipres.cec.uchile.cl/~domorale/**

27. Criptoanálisis
**http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node310.html**

28. Criptosistemas de clave pública
**http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node309.html**

29. IP Sec
**http://216.239.41.104/search?q=cache:DGFGuuT6-GAJ:www.uniboyaca.edu.co/facingenieria/ipsec.pdf+Authentication+Header+Encapsulating+Security+Payload+&hl=es&lr=lang_es&ie=UTF-8**

30. IPv6
**http://216.239.41.104/search?q=cache:SGyKDNcKejlJ:people.ac.upc.es/joseb/std_t2_f_01.pdf+Authentication+Header+Encapsulating+Security+Payload+&hl=es&lr=lang_es&ie=UTF-8**

31. IPsec: IP segura sobre *Internet*
**http://www.gulic.org/comos/LARTC/html/c440.html**

32. Perez Iglesis, Santiago. **El estándar de seguridad IP.**

33. *Internet* 2 en México. **Protocolos de Seguridad e Instrumentación de IPSec en Escenarios Experimentales de *Internet* 2 en México.**

34. Aliaga Calderón, Fco Javier. **IPSec y firewalls en IPv6.** Área de Ingeniería Telemática Universidad CARLOS III de Madrid.

35. Protocolos Seguros
**http://64.233.161.104/search?q=cache:lohrcdzk6r8J:www.redes.upv.es/irc/transpas01-02/Protocolos%2520Seguros.pdf+Protocolos+Authentication+Header&hl=es&lr=lang_es&ie=UTF-8**

36. Documentación de Windows 2000 Server
**www.microsoft.com/windows2000/**

37. Seguros desde la cripta
**http://www.iec.csic.es/criptonomicon/susurros/susurros11.html**

38. Infraestructura de clave pública (PKI)
**http://www-106.ibm.com/developerworks/patterns/es_es/glossary/public-key-infrastructure.html**

39. Santiago María Concepción Mendoza Díaz. **Protocolos de seguridad e Instrumentación de IPSec**. Centro de investigación científica y de educación superior de ensenada.