"ESTUDIO, ANALISIS E INVESTIGACION DE LOS METODOS Y PROTOCOLOS PARA LA NEGOCIACION DE CLAVES DE SEGURIDAD EN EL INTERNET"

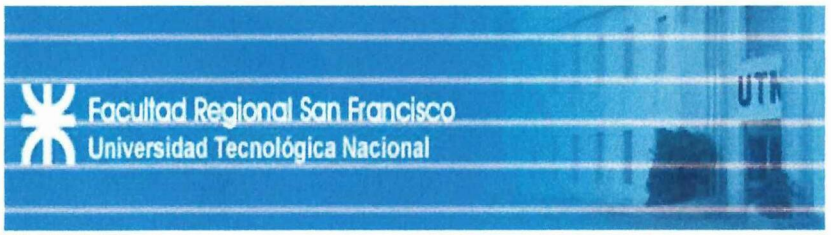
Postulante:

- **Chusin Cayo Mayra Narcisa**

TESIS DE GRADO PARA LA OBTENCIÓN DEL TITULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

CONVENIO:

UNIVERSIDAD TECNOLOGICA NACIONAL
FACULTAD REGIONAL "SAN FRANCISCO"
(San Francisco-Argentina)



UNIVERSIDAD TÉCNICA DE COTOPAXI
(Latacunga - Ecuador)

SAN FRANCISCO – ARGENTINA

2009

CERTIFICACIÓN

En calidad de Tutor de Tesis yo Ing. Gabriel Cerutti certifico que el presente trabajo de Investigación fue realizado en su totalidad bajo mi dirección Proyecto desarrollado por la Srta. Mayra Narcisa Chusin Cayo con el siguiente Tema: "ESTUDIO, ANALISIS E INVESTIGACION DE LOS METODOS Y PROTOCOLOS PARA LA NEGOCIACION DE CLAVES DE SEGURIDAD EN EL INTERNET".

Es todo cuanto puedo certificar en honor a la verdad.

Ing. Gabriel Cerutti.

Córdoba – San Francisco

Argentina Noviembre – 2009

PAGINA DE APROBACIÓN DEL TUTOR

Tesis de Grado para la obtención del Título de Ingeniero en Informática Y Sistemas Computacionales

Especialidad:

Ingeniería en Sistemas

ASESOR DEL TRABAJO

Ing. Gabriel Cerutti.

.....

Calificación: ---------- ----------

Numero Letras

Córdoba – San Francisco

Argentina Noviembre - 2009

PAGINA DE APROBACIÓN DEL TRIBUNAL DE GRADO

"ESTUDIO Y ANALISIS DE LOS METODOS Y PROTOCOLOS PARA LA NEGOCIACION SEGURA DE CLAVES DE SEGURIDAD EN EL INTERNET"

APROBADO POR LOS MIEMBROS DEL TRIBUNAL DE GRADO:

FECHA:.....

Ing.

Ing.

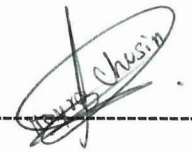
Ing.

Córdoba – San Francisco
Argentina Noviembre - 2009

PAGINA DE AUDITORÍA

El presente trabajo es responsabilidad de los autores que han sido realizados de acuerdo al cronograma de actividades y trabajo presentado y cumple con los requisitos y exigencias de la investigación científica.

Postulante:

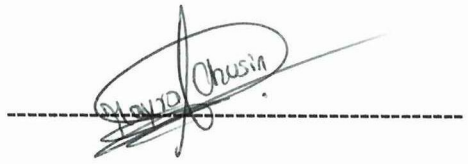


Mayra Narcisa Chusín Cayo
C.I. 050295902-6

Córdoba – San Francisco
Argentina Noviembre - 2009

PAGINA DE AUTORÍA

El presente trabajo de investigación, es original, auténtica y personal. En tal virtud expongo que el contenido es de mi absoluta responsabilidad legal y académica.



Mayra Narcisa Chusín Cayo
C.I. 050295902-6

Córdoba – San Francisco
Argentina Noviembre – 2009

AGRADECIMIENTO

En el presente trabajo agradezco a todas las personas quienes me apoyaron en los momentos más difíciles de mi estadía fuera del país y que hicieron posible la culminación del proyecto de tesis. De la misma manera al Ing. Gabriel Cerutti, quien fue mi tutor de tesis en el transcurso de estos largos 6 meses.

De igual manera a las Autoridades de la Universidad Técnica de Cotopaxi y de la Universidad Tecnológica Regional de San Francisco quienes me dieron apertura para la culminación de mi trabajo de investigación.

Agradezco a todos mis familiares, amigos (as) y demás que de una u otra manera aportaron con un granito de arena para que el trabajo de investigación se lo realice de la mejor forma posible, también agradezco a una persona muy especial quien fue mi guía a la distancia; a usted Ing. Fabián Masapanta gracias por ese apoyo incondicional y esto se lo recalco muy en alto, por todo lo brindado en el transcurso de todos estos meses de educación para llegar a ser lo que se anhelo, gracias a los consejos y a esa mano amiga que jamás desmayo en todo este tiempo.

En fin gracias Dios por permitirme culminar mi carrera profesional con muchos éxitos, y ayudándome a derrotar cualquier obstáculo que pudiese obstruir mi camino dándome la oportunidad de progresar cada día más.

Mayra Chusin.

Córdoba – San Francisco
Argentina Noviembre – 2009

DEDICATORIA

Primero le doy gracias a DIOS por darme la vida y concederme el regalo más grande y valioso mi MADRE que es un ejemplo para seguir su camino, por medio de ese esfuerzo se ha llegado a cumplir las metas y los objetivos propuestos en el transcurso de la carrera profesional, por tal motivo se lo dedico a mi Mamita Sra. María Cayo por apoyarme, brindándome paciencia, comprensión, fuerzas, para luchar y conseguir el fin buscado en lo que se desea, proporcionándome mucho valor en los momentos de nostalgia al no poder estar junto a ella y lejos de mi familia.

Gracias Mamita a usted por darme mucho amor, cariño y por estar en las buenas y en las malas junto a mi siendo padre y madre a la vez, ya que sin usted no sería lo que soy, ahora ya como una profesional, yo velare por el bienestar de nosotras para luchar adelante juntas, a mi hermanita María Fernanda que es el ser más bello que papito dios me lo pudo dar, a ti preciosa porque en mi ausencia tú cuidaste de mi madre y eres la parte fundamental en mi vida siendo mi guía, mi luz, mi alegría para salir adelante en estos largos meses, no saben cuánto las amo.

A mi Padre, a mis primos(as), mis tíos Efra, Piedy, Fabi y a mi preciosa Kelly que a la distancia me han hecho sonreír cuando me encontraba triste, a mis Abuelitos Papi Agustín, Mami Rosa y a toda mi familia quien supo darme consejos en los momentos de soledad, gracias a todos ustedes por encaminar este triunfo alcanzado con empeñó y dedicación para llegar a ser una Ing. Sistemas.

Mayra Chusin.

Córdoba – San Francisco
Argentina Noviembre – 2009

RESUMEN

La presente investigación se ha desarrollado en Instituciones de Ecuador y Argentina, su objetivo principal es facilitar un método adecuado para ofrecer garantías sobre el manejo de información en Internet o cualquier red de datos, así como también la aprobación de herramientas de control de claves de validación de usuarios que utilizan esta característica.

En vista que en el siglo XXI la revolución y el avance científico tecnológico nos lleva a conocer y desarrollar conocimientos desconocidos e ir insertándonos en la actualización del desarrollo y buen desempeño de la función o cargo a una persona encomendada, según su profesión y actitud personal.
El desarrollo de esta investigación aporta con nuevos avances tecnológicos, de manera especial en el área tecnológica y sistemas de información, porque es la ciencia que presenta muchas ventajas y es necesario e importante conocer sobre el material de apoyo con el cual laboramos, estudiamos, etc., facilitando de esta manera optimizar recursos.

Se profundizo en la utilización de herramientas de encriptación de actualidad por lo que la estructura del algoritmo se baso en un estudio a profundidad de seguridad, bajo una red de área extensa (WAN), utilizando métodos alternos con el mismo objetivo y prioridad.

El aporte científico está enmarcado en permitir que estudios posteriores den cuenta de que la seguridad de la información es un campo muy amplio y sujeto de vulnerabilidades por cualquier intruso, esto requiere de una atención mediante el uso de algoritmos seguros y confiables.

SUMMARY

This research has been developed in institutions of Ecuador and Argentina, its main goal is to provide a suitable method to provide assurance about the management of information on the Internet or data network, as well as validation of key control tools for validation Users who use this feature.

Since the technological advancements ant the revolution of the XXI have lead us to know and to develop new knowlege and the take part in this process of development a good performance of the position or charge for any person, according to their profession and personal attitude.

The development of this research provides new technological advancements are found, especially in the technological area and information systems, because it is the science that has many advantages, and it is necessary and important to know about the supporting material with which we work, study, etc., making easy the optimization of resources.

Elaborated on the use of current encryption tools so that the structure of the algorithm was based on a depth study of security in a wide area network (WAN), using alternate methods for the same purpose and priority.

The scientific contribution is framed to allow further studies to realize that information security is a very broad field and subject of vulnerability for any intruder, this requires attention through the use of safe and reliable algorithms.

CONTENIDO

CAPÍTULO 1 17

1.1 JUSTIFICACION TEORICA 17
1.2 INTRODUCCION 17
1.2.1 ALCANCES Y LIMITES DE LA INVESTIGACIÓN 19
1.3 UBICACIÓN GEOGRAFICA 20
1.4 JUSTIFICACIÓN 20
1.5 OBJETIVOS 21
1.5.1 OBJETIVO GENERAL 21
1.5.2 OBJETIVO ESPECIFICOS 21

CAPÍTULO 2 23

2.1 Tema: ESTUDIO Y ANALISIS DE LOS METODOS Y PROTOCOLOS PARA LA NEGOCIACION SEGURA DE CLAVES DE SEGURIDAD EN EL INTERNET 23
2.2 PRESENTACIÓN 23
2.3 ANTECEDENTES 23
2.3.1 HISTORIA DEL INTERNET 23
2.3.1.1 ¿QUÉ ES EL INTERNET? 24
2.3.1.2 QUE ES UNA RED GLOBAL? 25
2.3.2 NIVELES DE SEGURIDAD Y APLICACIÓN 26
2.3.2.1 PORQUE ES TAN IMPORTANTE LA SEGURIDAD? 27
2.3.3 AMENAZAS Y VULNERABILIDADES 28
2.4 IMPACTO 31
2.5 DESARROLLO TECNICO Y/O TECNOLOGICO 31
2.5.1 METODOS EXISTENTES 31
2.6 MÉTODOS DE ENCRIPTACIÓN 33
2.6.1 Encriptación de Datos 33
2.6.1.1 Algoritmo HASH 33

2.6.1.2 Algoritmos Simétricos 35

2.6.1.3 Algoritmos Asimétricos (RSA) 36

2.7 HERRAMIENTAS DE SEGURIDAD 37

2.7.1 PROTOCOLOS DE SEGURIDAD 38

2.7.1.1 Protocolo FTP 38

2.7.2 Protocolo DHCP 38

2.7.3 Protocolo SNMP 40

2.7.4 Protocolo TCP 41

2.7.5 Protocolo HTTP 43

2.7.6 Protocolo TELNET 45

2.7.7 Protocolo IP 46

2.8 ESTANDARES DE SEGURIDAD 47

2.8.1 Seguridad para aplicaciones del web: S-HTTP y SSL. 48

2.8.2 Seguridad para correo electrónico: PEM, S/MIME y PGP. 49

2.8.3 PGP es un estándar para asegurar el correo electrónico en Internet. 50

2.8.4 Seguridad para redes: firewalls 50

2.8.4.1 Los firewalls proporcionan un punto único de control para la seguridad de la red. 51

2.8.4.2 Los firewalls no preservan el carácter privado ni autentifican los datos, ni pueden proteger una red contra los virus. 51

2.8.4.3 Los protocolos S/WAN. 52

CAPÍTULO 3 53

3.1 INTRODUCCIÓN A IPSEC 53

3.1.1 Análisis del protocolo IPSec y estándar de seguridad en IP 54

3.1.1.1 Características de seguridad de IPsec 55

3.1.1.2 Beneficios que aporta IPSec 57

3.2 Protocolos del IPSec 58
3.2.1 El protocolo AH 59
3.2.2 El Protocolo ESP 61
3.2.2.1 Firma y cifrado de paquetes ESP 65
3.2.2.2 El modo túnel. 66
3.2.2.3 Modo de túnel ESP 66
3.2.3 Los modos transporte y túnel en AH y ESP 68
3.2.3.1 El modo transporte. 68
3.2.3.2 Modo de transporte Encabezado de autenticación 69
3.2.3.3 Encabezado 70
3.2.3.4 Índice de parámetros de seguridad (SPI) 70
3.2.3.5 Número de secuencia 70
3.2.3.6 Datos de autenticación 71
3.2.3.7 Firma de paquetes con el encabezado AH 71
3.3 IKE el protocolo de control 71
3.3.1 El primer método de autenticación 73
3.3.2 En la segunda fase el canal seguro IKE 74
3.3.3 Integración de IPSec con una PKI 75
3.3.4 Integridad y autenticación del origen de los datos 78
3.3.5 Confidencialidad 78
3.3.6 Detección de repeticiones 79
3.3.7 Control de acceso: autenticación y autorización 79
3.3.8 No repudio 80
3.4 Aplicaciones prácticas de IPsec 80
3.4.1 La interconexión segura de redes locales (intranet) 81
3.4.2 El acceso seguro de usuarios remotos 83

CAPÍTULO 4 86

4.1 RECOLECCIÓN Y PROCESAMIENTO DE LA INFORMACIÓN 86
4.1.1 Recolección 86
4.2 Procesamiento de la información 86
4.3 Análisis e Interpretación de los resultados 87
4.3.1 Aplicación de Técnicas de Investigación 87
4.3.2 Encuestas 87
4.3.3 Entrevista 87
4.3.4 Observaciones 88
4.3.5 Población 88
4.3.6 Muestra 88

CAPÍTULO 5 108

5.1 CONCLUSIONES Y RECOMENDACIONES DE LOS METODOS DE SEGURIDAD 108
5.1.1 CONCLUSIONES: 108
5.1.2 RECOMENDACIONES 110
5.2 BIBLIOGRAFIA: 111
5.3 GLOSARIO DE TERMINOS 112

LISTA DE TABLAS

CAPÍTULO 1

Tabla 2. 1 CLASES DE DIRECCION IP 32
Tabla 2. 2 Estándar de Seguridad 47
Tabla 2. 3 Métodos 48

CAPITULO 4

Tabla 4. 1 89
Tabla 4. 2 90
Tabla 4. 3 91

Tabla 4. 4 92
Tabla 4. 5 93
Tabla 4. 6 94
Tabla 4. 7 95
Tabla 4. 8 96
Tabla 4. 9 97
Tabla 4. 10 98
Tabla 4. 11 99
Tabla 4. 12 100
Tabla 4. 13 101
Tabla 4. 14 102

LISTA DE FIGURAS

CAPÍTULO 2

Figura 2. 1 24
Figura 2. 2 25
Figura 2. 3 26
Figura 2. 4 27
Figura 2. 5 29
Figura 2. 6 30
Figura 2. 7 Encriptación 33
Figura 2. 8 Algoritmos Simétricos 35
Figura 2. 9 Cifrado y descifrado 35
Figura 2. 10 Emisor Receptor 37
Figura 2. 11 La función multiplexión 43
Figura 2. 12 Protocolo TCP/ IP 44

CAPÍTULO 3

Figura 3. 1 Estructura de un datagrama AH 59
Figura 3. 2 Modo Túnel para IPv4 e IPv6 60
Figura 3. 3 Funcionamiento del protocolo AH 61
Figura 3. 4 Estructura de un datagrama ESP 62
Figura 3. 5 Funcionamiento para IPv4 e IPv6 63
Figura 3. 6 Funcionamiento del protocolo ESP 64
Figura 3. 7 Funcionamiento IPv4 e IPv6 para ESP 65
Figura 3. 8 Los modos de funcionamiento transporte y túnel de IPSec 67
Figura 3. 9 Funcionamiento del protocolo IKE 74

Figura 3. 10 Integración de una PKI en IPSec 77
Figura 3. 11 Interconexión de redes locales en entorno financiero..... 82
Figura 3. 12 Acceso seguro de usuarios remotos a una corporación 84

CAPÍTULO 4

Figura 4. 1 89
Figura 4. 2 90
Figura 4. 3 91
Figura 4. 4 92
Figura 4. 5 93
Figura 4. 6 94
Figura 4. 7 95
Figura 4. 8 96
Figura 4. 9 97
Figura 4. 10 98
Figura 4. 11 99
Figura 4. 12 100
Figura 4. 13 101
Figura 4. 14 103
Figura 4. 15 104
Figura 4. 16 105
Figura 4. 17 106

CAPÍTULO 1

1.1 JUSTIFICACION TEORICA

La conversión de los distintos medios de comunicación, con el manejo de información ya no como medio alternativo sino como medio permanente que está influyendo en las actividades cotidianas y de servicios en los campos de producción de todas las organizaciones tanto local, nacional e internacional, ha levantado el interés de personas con buenas pretensiones y de personas fuera del contexto moral, atacando a la información desde todos los ámbitos, provocando alteraciones de tipo económico, de tiempo y de manejo de procesos que conllevan a pérdidas considerables y perjuicios que en muchos de los casos lleva mucho tiempo el recuperar el status normal.

Esto ha permitido que personal técnico preocupado busque e investigue formas, métodos que ayuden a evitar y detectar infiltraciones de cualquier naturaleza de personas y equipos identificados como "INDESEABLES" que ayudará a mantener en perfectas condiciones integral y segura hacia su destino, los mismos han tenido su grado de complejidad pero se ha logrado frenar esta infiltración, pero no es suficiente por lo tanto se hace necesario incursionar en la búsqueda de métodos más eficientes que cubran y generen campos de bloque efectivos y permitan un alto grado de confianza por parte de los usuarios de la red local o global como es el INTERNET.

1.2 INTRODUCCION

Actualmente el campo de las comunicaciones ha tenido cambios relevantes, hace un tiempo atrás los estándares aplicados no eran eficientes respecto a facilitar una fluidez adecuada de información entre los actores que conforman una Red de Datos Mundial (INTERNET).

A Nivel Global el riesgo de manejar información a través de la Internet, tiene sus puntos vulnerables cuando no están bien definidos los niveles de seguridades sobre dicha información, y se encuentran a merced de personas con destrezas de infringir cualquier tipo de seguridades y acceder sin ningún inconveniente, es por eso que se ha visto en la necesidad de investigar nuevas posibilidades de mantener la información con un mejor nivel de protección.

La aplicación de nuevas tecnologías en el campo de manejo de claves o llaves de autenticación, envío – recepción de información entre dos usuarios de una Red (Manejo de IP´s, IPSEc en versiones 4 y 6), permiten implementar un método de integridad de información.

Por lo anteriormente expuesto se propone el ESTUDIO, ANALISIS E INVESTIGACION DE LOS MÉTODOS Y PROTOCOLOS PARA LA NEGOCIACION SEGURA DE CLAVES DE SEGURIDAD EN EL INTERNET, que permitirá mejorar la seguridad en la manipulación de los datos, lo cual beneficiara y ayudará al usuario en el manejo adecuado y seguro en la manipulación de claves o llaves de confidencialidad.

El envío y la recepción de información a través de la Red se encuentran vulnerables ante usuarios (intrusos) que pueden acceder a información considerada en algunos casos muy confidenciales, y constituye un riesgo que la misma pueda ser utilizada de manera indebida, ocasionando un perjuicio hacia los usuarios u organización participante.

Para obtener una mejor seguridad en el manejo de información, se ha visto en la necesidad de poner mayor énfasis en aspectos de seguridad sobre IP (IPSec) específicamente en el Internet.

1.2.1 ALCANCES Y LIMITES DE LA INVESTIGACIÓN

Nuestra investigación estará enfocada al campo funcional en general, sin especificar áreas de interés particular. Y lo apropiado es enfocar el tema en general ya que al internet como medio de comunicación se lo mantiene activo para cualquier tipo de actividad.
Al ser la información el medio por el cual se fusionan todo tipo de actividades y se comparte información entre dos ámbitos: punto a punto o multipunto (punto a varios puntos), es decir en términos técnicos redes dedicadas, y multiusuario, se hace necesario cubrir todo tipo de comunicación intranet o extranet en todas las áreas.

De ahí se desprende el punto vulnerable que posee el acceso indebido a información, por varias formas, métodos, procesos, etc. Pero los autores confidenciales de estas actividades indebidas son usuarios expertos en violar seguridades de acceso a la información. A pesar de los beneficios que este ofrece. A nivel educativo, si bien Internet contiene todo un mundo de información en pro del desarrollo del conocimiento y las habilidades sociales, el uso inadecuado de este recurso ha permitido la difusión al interior de la comunidad estudiantil de esta manera ayuda de la cultura de la piratería, el copy – paste y el atentado a los derechos de autor; además de ser foco de distracción al momento de hacer consultas dado que simultáneamente llevan a cabo otras actividades de diferente índole afectando la productividad del estudiante.

A través del tiempo con la evolución de la tecnología, las comunicaciones han tenido un avance sustancial, sus procesos y sus niveles de seguridades se han visto en la necesidad de tener una robustez con éxitos en brindar información segura desde y hacia los usuarios de la red.

El definir los niveles de importancia de información es muy serio, cuando de tomar decisiones se trata, el logro de estos niveles de seguridad deben estar en todos las plataformas de software existentes, y deben ser compatibles entre sí, logrando una globalidad no solo de manejo de información sino también en hablar el mismo lenguaje entre los distintos puntos del mundo y sus Sistemas Operativos como elemento central.

1.3 UBICACIÓN GEOGRAFICA

La presente investigación está dirigido para la comunidad en general que depende mucho del uso del internet, asociados en organizaciones e instituciones que giran la mayor parte de sus actividades e incluso con la toma de decisiones bajo el procesamiento de datos e información en los equipos tecnológicos.
Por lo tanto la investigación se orientará en una área de cobertura comparativa tanto en Ecuador como en Argentina, sitios en los cuales se pueden definir elementos de estudio sobre el manejo de seguridades de información en una red, los mismos que delimitarán el área de estudio, para lo cual se toma como muestra instituciones afines del uso de manejo de información en una red de datos.

1.4 JUSTIFICACIÓN

La evolución en el proceso de comunicaciones en los últimos tiempos ha sido muy acelerada, a tal punto que no existe espacio ni distancia que pueda superarlo, referente a las tecnologías y estándares sobre conectividad ya que estas ofrecen alternativas que dependen del protocolo y no de la estructura (topología) de una Ethernet.

El aporte que brinde esta investigación pretende dar a conocer nuevas alternativas de solución al problema más común que se da en una Intranet (el plagio y el

acceso no permitido), de tal manera que los servicios de las redes de datos en cada organización sean considerados de alta calidad y con mayor confiabilidad en el envío y recepción de datos.

Podremos ver como las Tecnologías de Comunicación han venido a ocupar una parte medular en cualquier medio que pretenda brindar un principio de calidad y seguridad. Para ello es necesario implementar estos algoritmos de cifrado sobre IPv4 e IPv6, no sólo en los procesos de distribución sino en mantener la fiabilidad y la manera más segura del intercambio de claves entre dos partes que no conocen previamente.

El factor importante que nos motiva realizar esta investigación fue debido a que no existe la suficiente garantía en el manejo de información por medio de la Internet al momento de enviar datos que pueden ser muy privados para el usuario.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

- ✓ Estudiar los Métodos y Protocolos para la negociación segura de claves de seguridad en la internet.

1.5.2 OBJETIVO ESPECIFICOS

1. Analizar y establecer los principales problemas de la transferencia de claves de cifrado sobre IPSec.
2. Conocer los distintos protocolos y su vinculación con procesos de cifrado para evitar el plagio de claves y su acceso a la información.

3. Investigar el funcionamiento y la confiabilidad de este proceso mediante el análisis de los distintos métodos, llegando a una solución de propuesta eficiente y eficaz para el fin buscado.

4. Conocer el nivel de utilización de los diferentes protocolos y métodos en empresas de Argentina y Ecuador

CAPÍTULO 2

PROPUESTA

2.1 Tema: ESTUDIO Y ANALISIS DE LOS METODOS Y PROTOCOLOS PARA LA NEGOCIACION SEGURA DE CLAVES DE SEGURIDAD EN EL INTERNET

2.2 PRESENTACIÓN

Esta sección incluye una introducción detallada a los protocolos que se incluyen en TCP/IP. Aunque la información es conceptual, debe conocer los nombres de los protocolos. También aprenderá las acciones que lleva a cabo cada protocolo. "TCP/IP" es el acrónimo que se utiliza comúnmente para el conjunto de protocolos de red que componen en el Internet. Muchos textos utilizan el término "Internet" para describir tanto el conjunto de protocolos como la red de área global. El "TCP/IP" hace referencia específicamente al conjunto de protocolos de Internet.

2.3 ANTECEDENTES

2.3.1 HISTORIA DEL INTERNET

Esta red se creó en 1969 y se llamó ARPANET. En principios, la red contaba con 4 ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos 40 ordenadores conectados. Tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Entonces dos investigadores crearon el protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo).

ARPANET siguió creciendo y abriéndose al mundo, y cualquier persona con fines académicos o de investigación podía tener acceso a la red. Las funciones militares

se desligaron de ARPANET y fueron a pasar a MILNET, una nueva red creada por los EE.UU.

La NSF (National Science Fundation) crea su propia red informática llamada NSFNET, que mas tarde absorbe a ARPANET, creando así una gran red con propósitos científicos y académicos. El desarrollo de las redes fue abismal, y se crean nuevas redes de libre acceso que más tarde se unen a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET.

Con el tiempo la palabra "ciberespacio" termino por ser sinónimo de Internet. El desarrollo de NSFNET fue tal que hacia el año de 1990 ya contaba con alrededor de 100.000 servidores.

En el centro Europeo de Investigadores Nucleares (CERN), Tim Berners Lee dirigía la búsqueda de un sistema de almacenamiento y recuperación de datos. Berners retomó la idea de Ted Nelson (un proyecto llamado "Xanadú") de usar hipervínculos. Robert Caillau quien cooperó con el proyecto, cuenta que en 1990 deciden ponerle un nombre al sistema y lo llamarón World Wide Web (WWW) o telaraña mundial.

2.3.1.1 ¿QUÉ ES EL INTERNET?

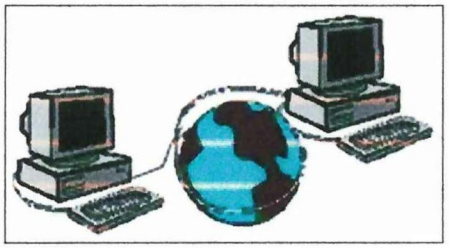


Figura 2. 1

Podemos definir a Internet como una "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí.

Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos.
De esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "red global".

2.3.1.2 QUE ES UNA RED GLOBAL?

Garantiza la intercomunicación de los diferentes participantes esta red global tiene la característica de que utiliza un lenguaje o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP. Así pues, Internet es la "red de redes" que utiliza TCP/IP como su protocolo de comunicación.

Figura 2. 2

En informática, la capa de aplicación es el nivel 7 del modelo OSI. Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y protocolos de transferencia de archivos (FTP)

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml. O cuando chateamos con el Messenger, no es necesario que codifiquemos la información y los datos del destinatario para entregarla a la capa de Presentación (capa 6) para que realice el envío del paquete.

2.3.2 NIVELES DE SEGURIDAD Y APLICACIÓN

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

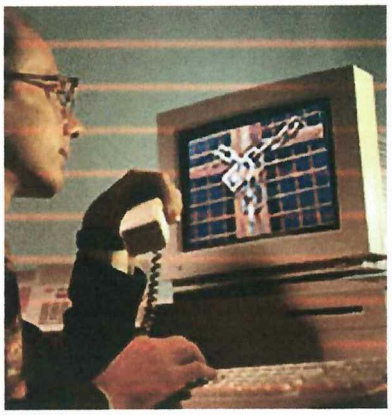


Figura 2. 3

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

2.3.2.1 PORQUE ES TAN IMPORTANTE LA SEGURIDAD?

Por la existencia de personas ajenas a la información, también conocidas como piratas informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos.

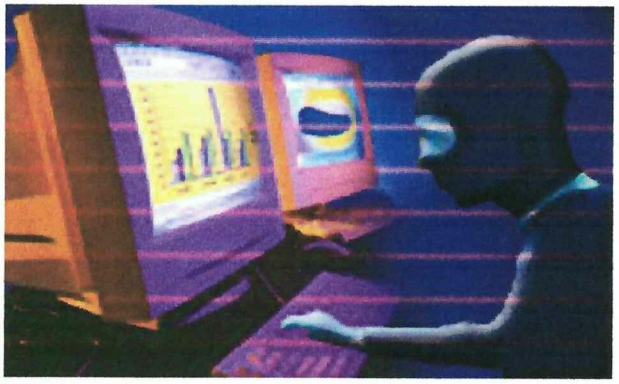


Figura 2. 4

Tales personajes pueden, incluso, formar parte del personal administrativo o de sistemas, de cualquier compañía; de acuerdo con expertos en el área, más de 70% de las Violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.
Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe

conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.
El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.
Por esta razón se hace necesario realizar un análisis e investigación del presente tema de investigación, que permitirá elevar los niveles de seguridad en el manejo de información.

2.3.3 AMENAZAS Y VULNERABILIDADES

Por vulnerabilidad entendemos la exposición latente a un riesgo. En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.
Específicamente, en los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, es el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el Web Site de la compañía. Con ello, es evidente que los riesgos están en la red, no en la PC.
Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Cortesía de la Revista Red

Figura 2. 5

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible)
- Establecer niveles de prioridad e importancia sobre esta información
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red.
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- Implementar respuesta a incidentes y recuperación para disminuir el impacto.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el

manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Figura 2. 6

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional (firewalls, autenticación, \ antivirus, controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros), y no únicamente tecnología.

Un esquema de seguridad empresarial contempla la seguridad física y lógica de una compañía. La primera se refiere a la protección contra robo o daño al personal, equipo e instalaciones de la empresa; y la segunda está relacionada con el tema que hoy nos preocupa: la protección a la información, a través de una arquitectura de seguridad eficiente.

Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos para generar una cultura de seguridad dentro de la organización.

2.4 IMPACTO

Las áreas que serán beneficiadas directa o indirectamente están en el ámbito general, es decir no existe organización que no esté inmersa en el trabajo informático mucho menos en el campo de uso del Internet, herramienta que se ha vuelto indispensable como parte inclusive de su estructura funcional de labores usuales, en vista de aquello, se hace indispensable enfocar un sistema central llamado información en internet, que es el medio por el cual trabajan todas las áreas y especialidades de todo tipo, por lo tanto el área de impacto estarán en todas las tareas de toda institución, en toda persona al cual denominaremos usuarios informáticos o internautas, usuarios 90% dependientes de la red de redes (Internet).

2.5 DESARROLLO TECNICO Y/O TECNOLOGICO

2.5.1 METODOS EXISTENTES

Un protocolo de intercambio de hardware es por tanto similar a dos personas que físicamente estrechan sus manos, mientras que uno de software es más parecido a dos grupos que deciden conversar en un lenguaje particular.
El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC (Centro de Información de Red) asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro).

CLASE	Dirección más baja	Dirección más alta
CLASE A	0.1.0.0	126.0.0.0
CLASE B	128.0.0.0	191.255.0.0
CLASE C	192.0.1.0	223.255.255.0
CLASE D	224.0.0.0	239.255.255.255
CLASE E	240.0.0.0	247.255.255.255

Tabla 2. 1 Clases de dirección IP

Clase A Corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

Clase B Sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.

Clase C Tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Clase D Se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Clase E Cabe decir que, las direcciones de clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

2.6 MÉTODOS DE ENCRIPTACIÓN

Figura 2. 7 Encriptación

2.6.1 Encriptación de Datos

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticación, integridad, confidencialidad y el no repudio (Servicio de Seguridad) de la misma entre otros aspectos.

Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos.

Para poder Encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes:

- Los algoritmos HASH
- Los simétricos
- Los asimétricos

2.6.1.1 Algoritmo HASH

Un HASH no es más que un número, hexadecimal generalmente, que es un compendio de bits que dependen bit a bit de un conjunto de bits original. Dicho

conjunto de bits original puede ser un fichero, cadena de texto (archivos adjuntos) etc.

Para ilustrarlo de forma sencilla, podemos realizar un resumen de un texto que cumpliera las siguientes características:

- Todos los resúmenes generados utilizando el mismo método, tienen la misma longitud
- Es sencillo realizar el resumen.
- A partir del resumen es imposible recuperar el texto original.
- Es imposible que dos textos tengan el mismo resumen.

Además, este número cumple las características antes mencionadas:

- Todos los códigos HASH son diferentes para entradas diferentes
- Calcular un HASH es sencillo para un computador
- Lo realmente complejo, desde el punto de vista computacional, es revertir el HASH, es decir, obtener el conjunto de bits original de entrada a partir del HASH.
- Cada entrada al algoritmo de HASH tiene una salida distinta.

Por tanto, un Algoritmo de HASH no es un algoritmo de cifrado. Es decir, no se usan claves, ni códigos ni nada similar para realizar un HASH. Sin embargo estos si tienen aplicación en algoritmos de cifrado y seguridad.

Ejemplo:

Ana envía un mensaje a Benito. Al final del mensaje le añade el valor HASH del texto según una función en la que se han puesto previamente de acuerdo.
Benito recibe el mensaje y calcula el valor HASH. Si coincide con el que ha dicho Ana puede estar seguro de que el mensaje no ha sido modificado.

2.6.1.2 Algoritmos Simétricos

Estos algoritmos presentan la particularidad de presentar una sola llave, que se usa tanto para cifrar como para descifrar. Este principio se muestra en la siguiente figura.

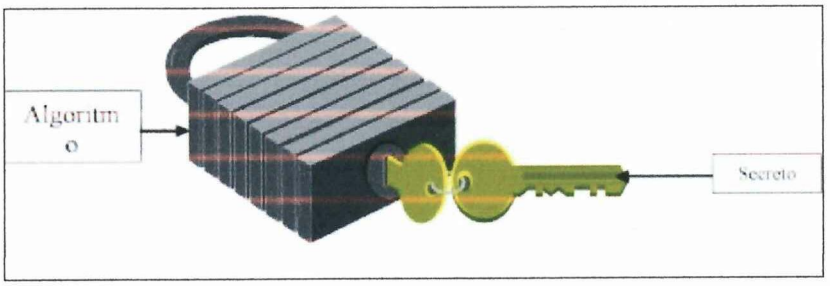


Figura 2. 8 Algoritmos Simétricos

Como dijimos, el algoritmo es ampliamente conocido, como nuestro candado del dibujo, pero sólo quien posea la llave (que es el secreto), en este caso amarilla, podrá operarlo. Como se ve en la figura siguiente, la misma llave se usa a ambos extremos.

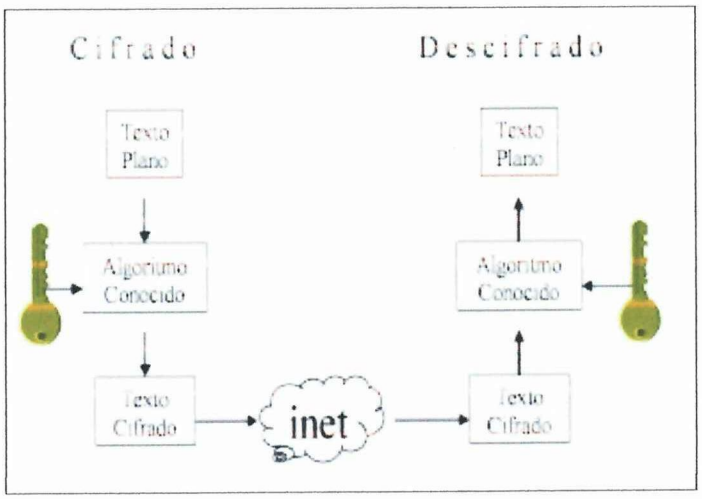


Figura 2. 9 Cifrado y descifrado

La fortaleza de los algoritmos simétricos está dada por la longitud de sus llaves. Imaginemos el caso de la llave de un candado. Si una persona tuviese que adivinar la forma de la llave sin saber ningún dato, cuanto más larga sea, presentará más variabilidad de dientes y hendiduras, haciéndola más segura. El concepto informático es el mismo, a llaves más grandes (más bits), mayor seguridad.

Los algoritmos simétricos son muy rápidos para cifrar y descifrar gran cantidad de datos, lo que los hace apropiados para cifrar un archivo completo, un ejecutable de un programa, o una imagen.

La gran limitación de los algoritmos simétricos se da en los casos en que trabajar con la misma llave se vuelve un problema. Justamente la distribución de la llave entre las personas que deseen operar entre sí supone que se encuentren en algún lugar, o tengan otro medio confiable para la distribución de la llave. Generalmente se dice que encuentran mayor aplicación en casos 1 a 1, donde solo dos individuos deben conocer la misma llave.

2.6.1.3 Algoritmos Asimétricos (RSA)

- Son aquellos que emplean una doble clave es decir, una clave denominada pública y otra clave privada.
- La clave privada sólo la posee el receptor y la utiliza para desencriptar.
- La clave pública la posee el receptor, pero se la pasa al emisor para que la utilice a la hora de encriptar su mensaje.
- Son más seguros, ya que aunque un intruso consiga la clave pública, no será capaz de encontrar la clave privada a través de la clave pública para poder desencriptar el mensaje.

- El principal inconveniente es que resulta computacionalmente muy costoso su implementación.
- A la hora de encriptar, son mucho más lentos que los algoritmos simétrico

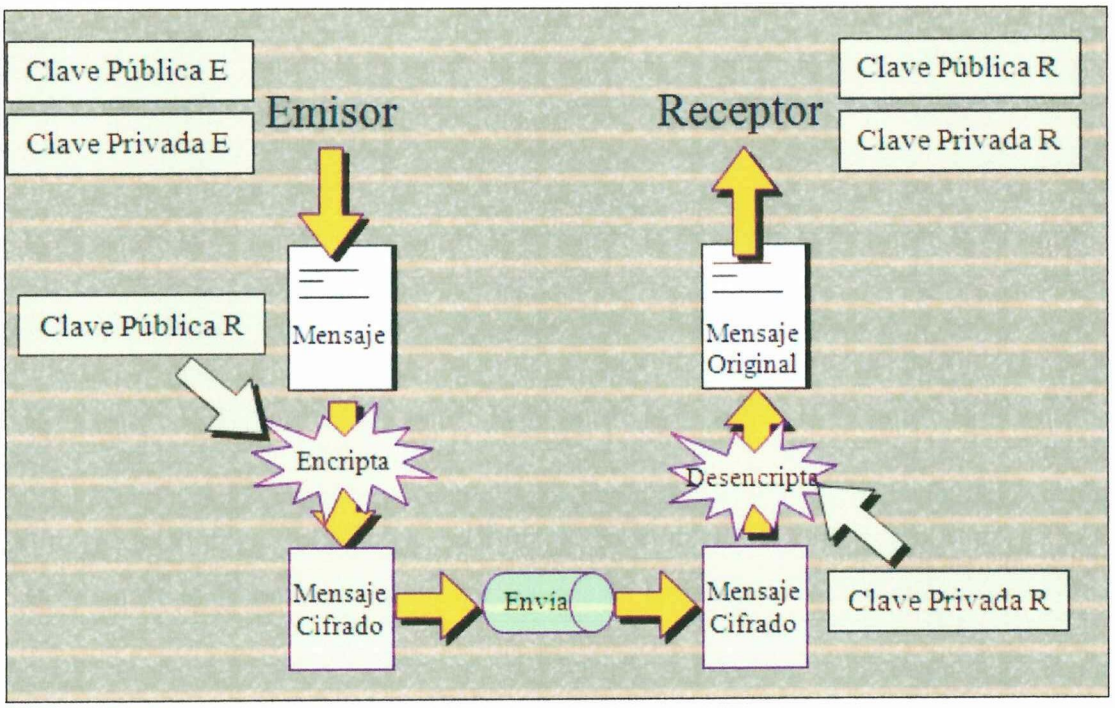


Figura 2. 10 Emisor Receptor

2.7 HERRAMIENTAS DE SEGURIDAD

Existen muchos tipos diferentes de amenazas que pueden comprometer la seguridad de la información electrónica. Para contrarrestar estas amenazas se han desarrollado varios protocolos y aplicaciones usando las técnicas criptográficas descritas anteriormente.

Desde hace mucho tiempo se sabe que Internet depende de estándares abiertos. Este apoyo a los estándares abiertos, junto con el intercambio abierto de información en Internet, puede hacer que usted piense que seguridad e Internet son términos mutuamente excluyentes. Nada menos cierto. Aunque en el pasado

Internet instrumentó menos seguridad que las redes privadas de valor agregado (VANs), o las redes corporativas, los esfuerzos por proporcionar una variedad de mecanismos de seguridad al tráfico en Internet han progresado a toda velocidad.

2.7.1 PROTOCOLOS DE SEGURIDAD

2.7.1.1 Protocolo FTP

El protocolo FTP (Protocolo de transferencia de archivos). La implementación del FTP se remonta a 1971 cuando se desarrolló un sistema de transferencia de archivos (descrito en RFC141) entre equipos del Instituto Tecnológico de Massachusetts (MIT). Desde entonces, diversos documentos de RFC (petición de comentarios) han mejorado el protocolo básico, pero las innovaciones más importantes se llevaron a cabo en julio de 1973.

La función del protocolo FTP

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

El objetivo del protocolo FTP es:

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

2.7.2 Protocolo DHCP

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración

(principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

Funcionamiento del protocolo DHCP

Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base tanto, en una red puede tener sólo un equipo con una dirección IP fija: el servidor DHCP.

El sistema básico de comunicación es BOOTP (con la trama UDP). Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP.

Para esto, la técnica que se usa es la transmisión para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en 255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local.

Cuando el DHCP recibe el paquete de transmisión contestará con otro paquete de transmisión (no olvide que el cliente no tiene una dirección IP y por lo tanto no es posible conectar directamente con él) que contiene toda la información solicitada por el cliente.

Se podría suponer que un único paquete es suficiente para que el protocolo funcione. En realidad hay varios tipos de paquetes DHCP que pueden emitirse tanto desde el cliente hacia el servidor o viceversa.

2.7.3 Protocolo SNMP

SNMP significa Protocolo simple de administración de red. Es un protocolo que les permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red.

Principio operativo de SNMP

El sistema de administración de red se basa en dos elementos principales en un supervisor y agentes.
El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

Los conmutadores concentradores (hubs), routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión.

Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB ("Base de datos de información de administración"). SNMP permite el diálogo entre el supervisor y los agentes para recolectar los objetos requeridos en la MIB.
La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

- Los dispositivos administrados son los elementos de red (puentes, concentradores, routers o servidores) que contienen "objetos

administrados" que pueden ser información de hardware, elementos de configuración o información estadística.

- Los agentes es decir una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP.
- El sistema de administración de red (NMS), es un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

2.7.4 Protocolo TCP

TCP (que significa Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo o van hacia él Protocolo IP. Cuando se proporcionan los datos al protocolo IP los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Las principales características del protocolo TCP son las siguientes:

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

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

El objetivo de TCP

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).
Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Es por eso que estamos en un entorno Cliente-Servidor.

Las máquinas de dicho entorno se comunican en modo en línea es decir que la comunicación se realiza en ambas direcciones.
Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

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

La función multiplexión

TCP posibilita la realización de una tarea importante: multiplexar/demultiplexar; es decir transmitir datos desde diversas aplicaciones en la misma línea o, en otras palabras ordenar la información que llega en paralelo.

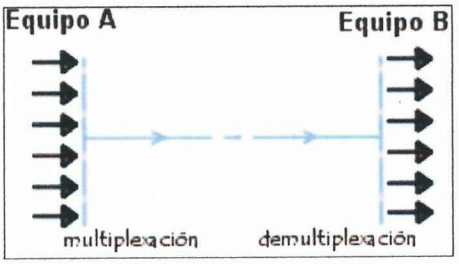


Figura 2. 11 La función multiplexión

Estas operaciones se realizan empleando el concepto de puertos (o conexiones), es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

2.7.5 Protocolo HTTP

Desde 1990, el protocolo HTTP (Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. La versión 0.9 sólo tenía la finalidad de transferir los datos a través de Internet (en particular páginas Web escritas en HTML).

La versión 1.0 del protocolo (la más utilizada) permite la transferencia de mensajes con encabezados que describen el contenido de los mensajes mediante la codificación MIME.

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML). Entre un navegador (el cliente) y un servidor web (denominado, entre otros, http en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL.

Comunicación entre el navegador y el servidor

La comunicación entre el navegador y el servidor se lleva a cabo en dos etapas:

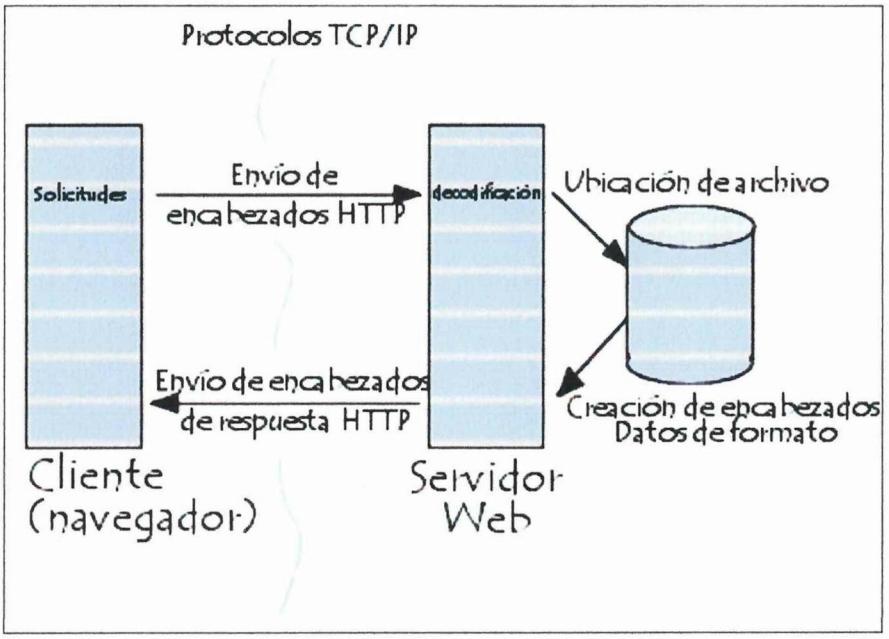


Figura 2. 12 Protocolo TCP/ IP

- El navegador realiza una solicitud HTTP
- El servidor procesa la solicitud y después envía una respuesta HTTP

2.7.6 Protocolo TELNET

El protocolo Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos (del lado del servidor).
El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma Terminal virtual de red (NVT);
- El principio de opciones negociadas;
- Las reglas de negociación.

Éste es un protocolo base, al que se le aplican otros protocolos del conjunto TCP/IP (FTP, SMTP, POP3, etc.). Las especificaciones Telnet no mencionan la autenticación porque Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet). Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada).

Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

Excepto por las opciones asociadas y las reglas de negociación, las especificaciones del protocolo Telnet son básicas. La transmisión de datos a

través de Telnet consiste sólo en transmitir bytes en el flujo TCP (el protocolo Telnet específica, que los datos deben agruparse de manera predeterminada. Específicamente, esto significa que de manera predeterminada los datos se envían línea por línea). Cuando se transmite el byte 255, el byte siguiente debe interpretarse como un comando. Por lo tanto, el byte 255 se denomina IAC (Interpretar como comando). Los comandos se describen más adelante en este documento.

Las especificaciones básicas del protocolo Telnet se encuentran disponibles en la RFC (petición de comentarios) 854, mientras que las distintas opciones están descriptas en la RFC 855 hasta la RFC 861.

2.7.7 Protocolo IP

El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su "entrega". En realidad, el protocolo IP procesa datagramas de IP de manera independiente al definir su representación, ruta y envío.

El protocolo IP determina el destinatario del mensaje mediante 3 campos:

- El campo de dirección IP: Dirección del equipo;
- El campo de máscara de subred: una máscara de subred le permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red;
- El campo de pasarela predeterminada: le permite al protocolo de Internet saber a qué equipo enviar un datagrama, si el equipo de destino no se encuentra en la red de área local.

2.8 ESTANDARES DE SEGURIDAD

Algunos de los estándares de seguridad para Internet:

Estándar	Función	Aplicación
Secure HTTP (S-HTTP).	Asegura las transacciones en la web.	Exploradores, servidores web, aplicaciones para Internet.
Secure Sockets Layer (SSL).	Asegura los paquetes de datos en la capa de la red.	Exploradores, servidores web, aplicaciones para Internet.
Secure MIME (S/MIME).	Asegura los anexos de correo electrónico en plataformas múltiples.	Paquetes de correo electrónico con encriptamiento y firma digital.
Secure Wide-Area Nets (S/WAN).	Encriptamiento punto a punto entre cortafuegos y enrutadores.	Redes virtuales privadas.
Secure Electronic Transaction (SET).	Asegura las transacciones con tarjeta de crédito.	Tarjetas inteligentes, servidores de transacción, comercio electrónico.

Tabla 2. 2 Estándar de Seguridad

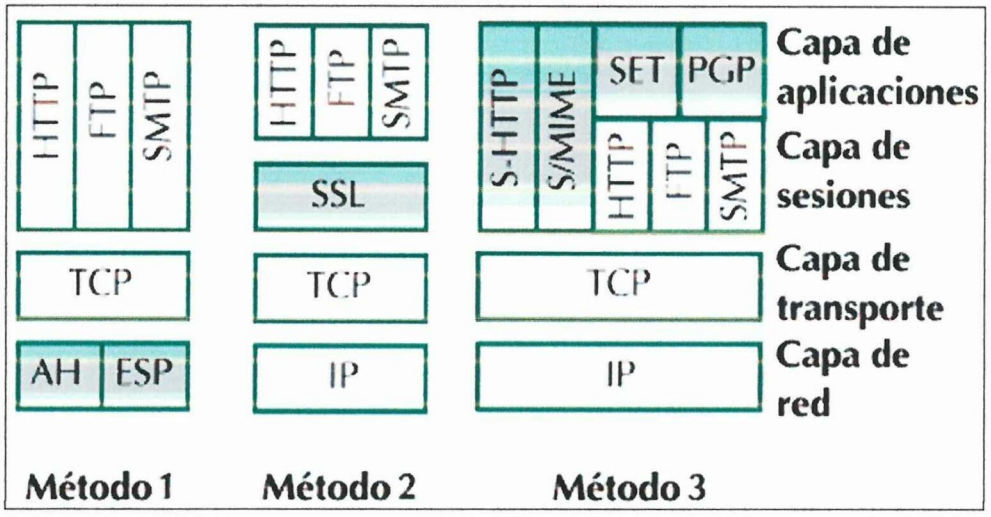


Tabla 2. 3 Métodos

Tres maneras en que los estándares de seguridad se usan en las redes.

Los estándares cubiertos aquí se pueden clasificar de acuerdo a si proporcionan seguridad de conexión o de aplicación.

2.8.1 Seguridad para aplicaciones del web: S-HTTP y SSL.

La seguridad de las aplicaciones para web gira en entorno a dos protocolos, Secure HTTP y Secure Sockets Layer, que proporcionan autentificación para servidores y navegadores, así como confidencialidad e integridad de los datos para las comunicaciones entre un servidor web y un navegador.

S-HTTP está diseñado específicamente para soportar el protocolo de transferencia de hipertexto (HTTP), proporcionando la autorización y seguridad de los documentos. SSL ofrece métodos de protección similares, pero asegura el canal

de comunicaciones al operar más abajo en la pila de red (entre la capa de la aplicación y las capas de red y transporte TCP/IP).

S-HTTP asegura los datos, mientras SSL asegura el canal de las comunicaciones.

SSL se puede usar para otras transacciones, aparte de las de web, pero no está diseñado para manejar decisiones de seguridad basadas en autentificación a nivel de documento o aplicación. Esto significa que se tendría que usar otros métodos para controlar el acceso a diferentes archivos.

2.8.2 Seguridad para correo electrónico: PEM, S/MIME y PGP.

Se ha propuesto una variedad de protocolos de seguridad para el correo electrónico en Internet, pero sólo uno o dos han recibido cierto uso extendido. El correo enriquecido con carácter privado (PEM-Privacy-enhanced mail) es un estándar de Internet para asegurar al correo electrónico usando llaves públicas o simétricas.

El uso de PEM ha descendido, ya que no está diseñado para manejar el moderno correo electrónico de multipartes soportado por MIME, además de que requiere una jerarquía rígida de autoridades de certificación para emitir llaves. Secure MIME (S/MIME) es un estándar más nuevo que se ha propuesto; usa muchos de los algoritmos criptográficos patentados y cuyas licencias corresponden a RSA Data Security Inc. S/MIME depende de certificados digitales, por ello también depende de algún tipo de autoridad de certificación, ya sea corporativa o global, para asegurar la autentificación.

2.8.3 PGP es un estándar para asegurar el correo electrónico en Internet.

PGP es una aplicación popular desarrollada para asegurar los mensajes y archivos, también se le conoce como Pretty Good Privacy. Probablemente sea la aplicación de seguridad para correo electrónico en Internet más usada; emplea una variedad de estándares de encriptamiento.

Las aplicaciones para encriptamiento/desencriptamiento PGP están disponibles de manera gratuita para la mayoría de los sistemas operativos importantes; así, los mensajes se pueden encriptar antes de usar un programa de correo electrónico.

Algunos programas de correo, como Eudora Pro, Qualcomm y OnNET, de FTP Software, pueden usar módulos conectores especiales de PGP para manejar correo encriptado. PGP se diseñó alrededor del concepto de una red de confianza que permitía a los usuarios compartir sus llaves, sin requerir una jerarquía de autoridades de certificación.

2.8.4 Seguridad para redes: firewalls

Cuando usted conecta recursos en su red corporativa a una red pública, como Internet, pone en riesgo sus datos y los sistemas de cómputo. Sin un firewall, el carácter secreto de los datos y la integridad de la información misma están sujetos a un ataque.

Al igual que sus contrapartes físicas en las casas y demás construcciones, los firewalls están diseñados para controlar el daño, en este caso, a sus datos y sistemas de cómputo.

2.8.4.1 Los firewalls proporcionan un punto único de control para la seguridad de la red.

Una de las ventajas más importantes de un firewall es que proporciona un punto de control único para la seguridad en una red. Aunque claro, esto puede revertirse contra usted, ya que el cortafuego también puede ser un punto único de falla y, por lo tanto, recibir la atención concentrada de los intrusos.

2.8.4.2 Los firewalls no preservan el carácter privado ni autentifican los datos, ni pueden proteger una red contra los virus.

Recuerde que los firewalls no son la reparación para los problemas de seguridad en Internet. Por ejemplo, no verifican la presencia de virus, así que no pueden garantizar la integridad de los datos. Por otra parte, no autentifican la fuente de los datos, y en la mayoría de los casos, no garantizan la confidencialidad de los datos tampoco. Sin embargo, se están desarrollando nuevos protocolos que manejen la autentificación y confidencialidad de los paquetes de datos en Internet.

Aunque los firewalls pueden ayudar a proteger sus datos y sistemas, las redes corporativas a menudo dependen de oficinas enlazadas dispersas por una ciudad, condado, estado o el mundo entero. Hoy en día se realizan trabajos para asegurar las redes basadas en IP6, por ejemplo, aquellas que forman Internet, al nivel de red, cosa que posibilitará que los negocios creen sus propias redes virtuales privadas (VPNs), usando Internet como una alternativa a las costosas líneas arrendadas.

2.8.4.3 Los protocolos S/WAN para autentificar y encriptar paquetes ayudarán a asegurar la compatibilidad entre los distintos vendedores de enrutador y firewalls.

Un grupo de vendedores de firewalls y enrutadores han formado una iniciativa llamada "S/WAN" (Secure Wide Area Networks-Redes de área grande seguras). Se han dado a la tarea de instrumentar y probar los protocolos sugeridos por la IETF-Internet Engineering Task Force (Fuerza de tareas de ingeniería en Internet) para asegurar los paquetes IP. Estos protocolos incluyen métodos para autentificar y encriptar paquetes, así como un método para intercambiar y manejar las llaves requeridas para los procesos de autentificación y encriptamiento. Los protocolos S/WAN ayudarán a asegurar la interoperabilidad entre los vendedores de enrutadores y firewalls, haciendo más fácil que las oficinas corporativas separadas geográficamente, así como los socios que formen una corporación virtual, se comuniquen con seguridad por Internet.

CAPÍTULO 3

3.1 INTRODUCCIÓN A IPSEC

IPSec es la tendencia a largo plazo para las redes seguras. Proporciona una línea de defensa clave frente a ataques en redes privadas e Internet.

IPSec tiene dos objetivos:

1. Proteger el contenido de los paquetes IP.
2. Defender contra los ataques de red mediante el filtrado de paquetes y la exigencia de comunicaciones de confianza.

Ambos objetivos se alcanzan gracias al uso de servicios de protección criptográfica, protocolos de seguridad y administración dinámica de claves.

Estos fundamentos proporcionan al mismo tiempo la capacidad y la flexibilidad para proteger las comunicaciones entre equipos de redes privadas, dominios, sitios remotos, extranets y clientes de acceso telefónico. Incluso pueden utilizarse para bloquear la recepción o la transmisión de determinados tipos de tráfico.

IPSec se basa en un modelo de seguridad completo, y establece la confianza y la seguridad desde una dirección IP de origen hasta una dirección IP de destino. La dirección IP en sí no se considera necesariamente una identidad, sino que el sistema que hay tras la dirección IP tiene una identidad que se valida a través de un proceso de autenticación. Los únicos equipos que deben conocer que el tráfico está protegido son los equipos remitente y receptor.

Cada equipo trata la seguridad en su extremo respectivo y supone que el medio a través del cual tiene lugar la comunicación no es seguro. Los equipos que se limitan a enrutar datos desde el origen hasta el destino no necesitan ser

compatibles con IPSec, salvo en el caso de que se filtren paquetes de tipo servidor de seguridad o se traduzcan direcciones de red entre los dos equipos.

Este modelo permite implementar correctamente IPSec en los siguientes casos:

- Red de área local (LAN): cliente-servidor y entre homólogos
- Red de área extensa (WAN): entre enrutadores y entre puertas de enlace
- Acceso remoto: clientes de acceso telefónico y acceso a Internet desde redes privadas

Normalmente, ambas partes requieren una configuración de IPSec (denominada directiva IPSec) para establecer las opciones y los parámetros de seguridad que permitirán que ambos sistemas acuerden el modo de proteger el tráfico entre ellos.

Las implementaciones de IPSec se basan en estándares del sector desarrollados por el grupo de trabajo de ingeniería de Internet (IETF). Algunas partes de los servicios relacionados con IPSec han sido desarrollados conjuntamente por Microsoft y Cisco Systems, Inc

3.1.1 Análisis del protocolo IPSec y estándar de seguridad en IP

IPSec es un conjunto de estándares del IETF para incorporar servicios de seguridad en IP y que responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas y comercio electrónico.

Está implementado por un conjunto de protocolos criptográficos.

1. Para asegurar el flujo de paquetes
2. Para garantizar la autenticación mutua y

3. Para establecer parámetros criptográficos

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). Es un estándar que aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP.

Todas las soluciones anteriores se basaban en soluciones propietarias que dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispusiesen de una misma plataforma.
La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Entre las de IPSec enfatizan que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogénea para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

3.1.1.1 Características de seguridad de IPsec

Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable ya que todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios.

El IPSec es un carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI y aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Las siguientes características de IPSec afrontan todos estos métodos de ataque:

- **Protocolo Carga de seguridad de encapsulación.**

El proceso de encapsulación lo realiza el AH y ESP proporciona privacidad a los datos mediante el cifrado de los paquetes IP

- **Claves basadas en criptografía.**

Se comparten entre los sistemas que se comunican, crean una suma de comprobación digital para cada paquete IP. Cualquier modificación del paquete altera la suma de comprobación, mostrando al destinatario que el paquete ha sido cambiado en su tránsito. Se utiliza material de claves diferente para cada segmento del esquema de protección global y se puede generar nuevo material de claves con la frecuencia especificada en la directiva de IPSec.

- **Administración automática de claves.**

Las claves largas y el cambio dinámico de claves durante las comunicaciones ya establecidas protegen contra los ataques. IPSec usa el protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP, Internet Security Association and Key Management Protocol) para intercambiar y administrar dinámicamente claves cifradas entre los equipos que se comunican.

- **Seguridad a nivel de red.**

IPSec existe en el nivel de red, proporcionando seguridad automática a todas las aplicaciones.

- **Autenticación mutua.**

IPSec permite el intercambio y la comprobación de identidades sin exponer la información a la interpretación de un atacante. La comprobación mutua (autenticación) se utiliza para establecer la confianza entre los sistemas que se comunican.

Sólo los sistemas de confianza se pueden comunicarse entre sí. Los usuarios no tienen que estar en el mismo dominio para comunicarse con la protección de IPSec. Pueden estar en cualquier dominio de confianza de la empresa. La comunicación se cifra, lo que dificulta la identificación e interpretación de la información.

- **Filtrado de paquetes IP.**

Este proceso de filtrado habilita, permite o bloquea las comunicaciones según sea necesario mediante la especificación de intervalos de direcciones, protocolos o, incluso, puertos de protocolo específicos.

3.1.1.2 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 realizan 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 que 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.

3.2 Protocolos del IPSec

Dentro de IPSec se distinguen los siguientes protocolos:

- IP (AH) Authentication Header
- IP (ESP) Encapsulating Security Payload
- IP (IKE) Internet key Exchange

Que proporcionan mecanismos de seguridad para proteger tráfico IP. Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

3.2.1 El protocolo AH

Protege la cabecera del paquete IP de interferencias de terceros así como contra la falsificación, calculando una suma de comprobación criptográfica y aplicando a los campos de cabecera IP una función hash segura. Detrás de todo esto va una cabecera adicional que contiene el hash para permitir la validación de la información que contiene el paquete.

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver la Figura 3.1).

Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP.

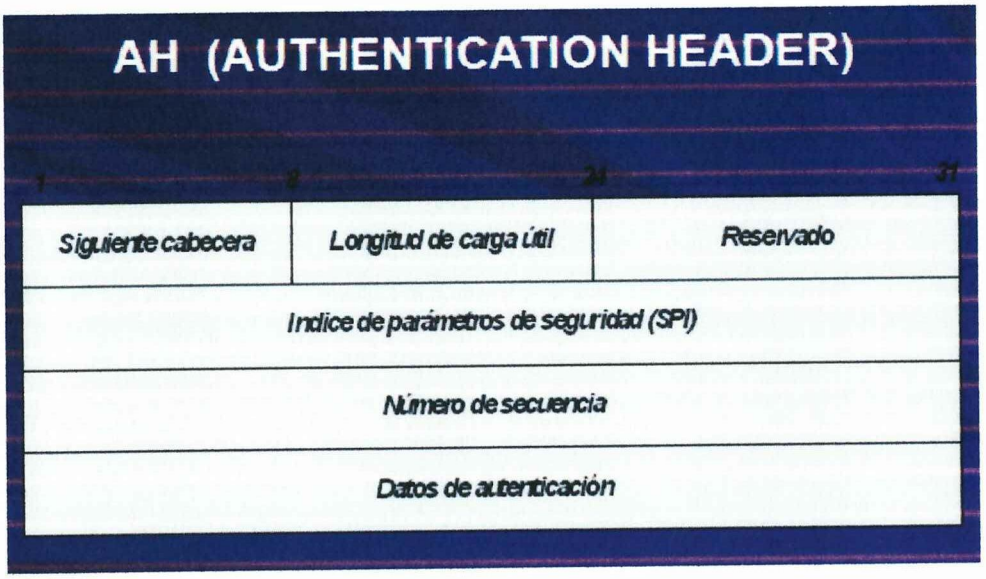
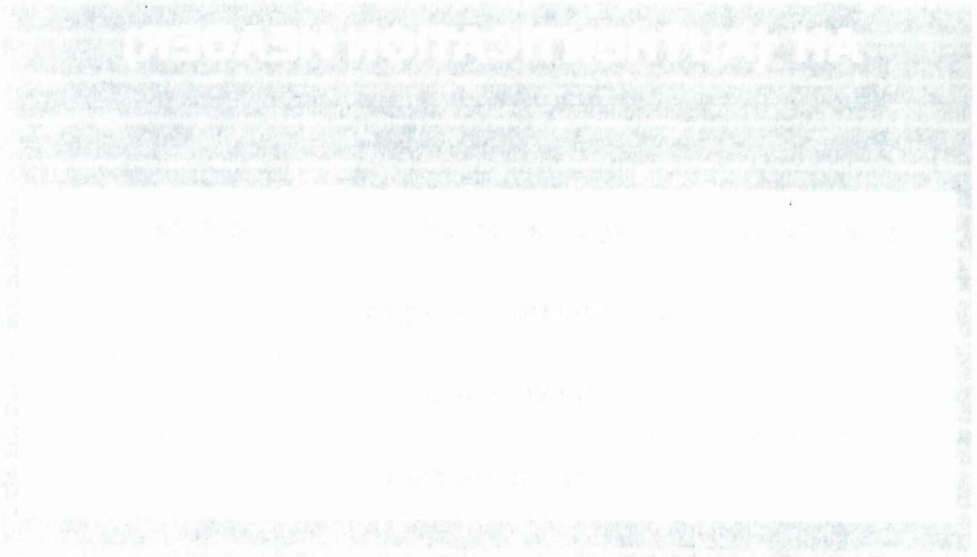


Figura 3. 1 Estructura de un datagrama AH



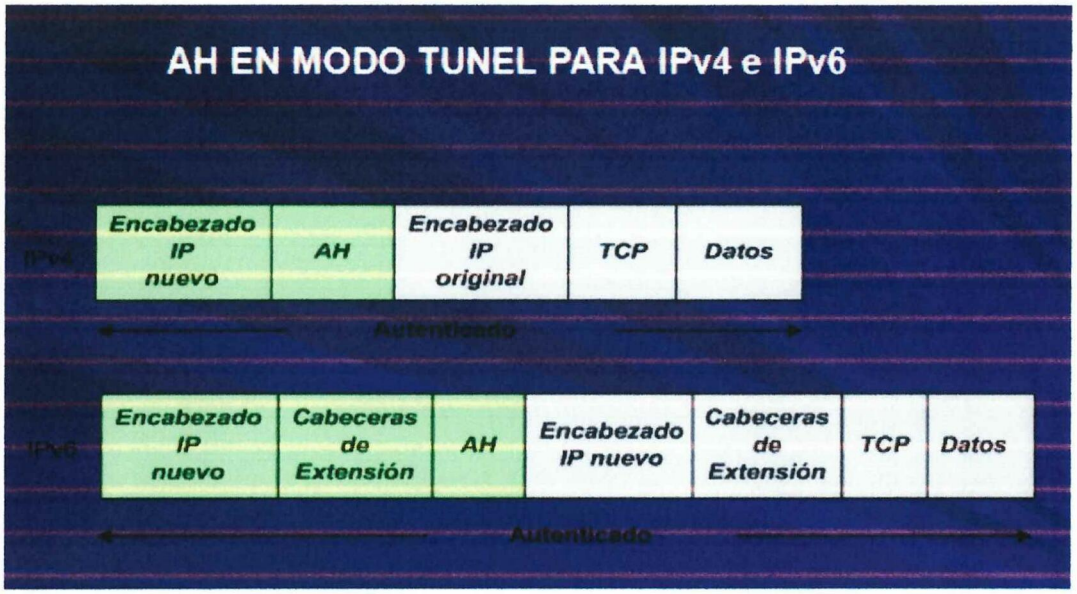


Figura 3. 2 Modo Túnel para IPv4 e IPv6

El funcionamiento de AH se basa en un algoritmo HMAC esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

En la Figura 3.3 se muestra el modo en que funciona el protocolo AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH.

El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave, y que dicha clave sólo la conocen el emisor y el receptor.

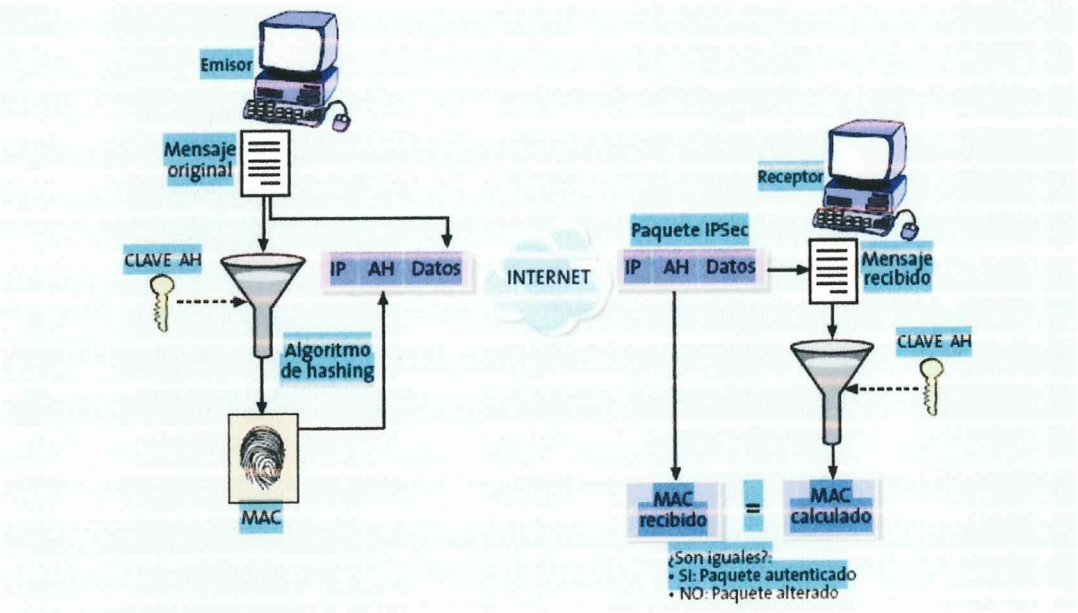


Figura 3. 3 Funcionamiento del protocolo AH

3.2.2 El Protocolo ESP

Protege los datos del paquete IP de interferencias de terceros, cifrando el contenido utilizando algoritmos de criptografía simétrica.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo).

En la Figura 3.4 se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

Esto implica que el campo Protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos.

Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

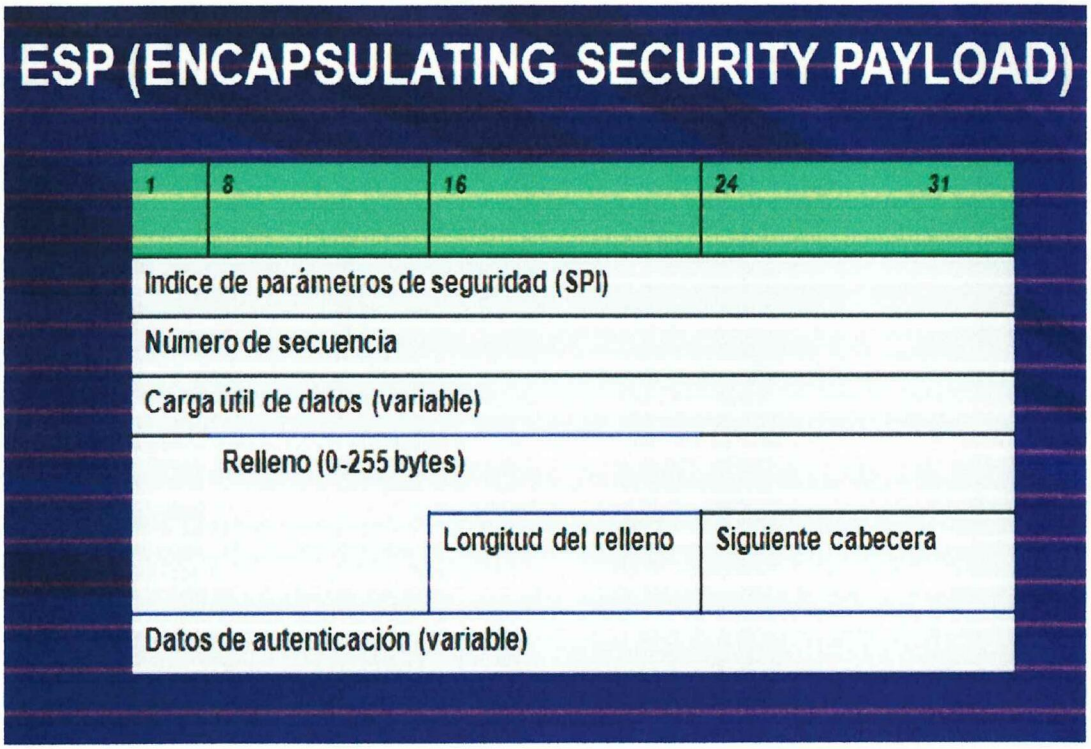


Figura 3. 4 Estructura de un datagrama ESP

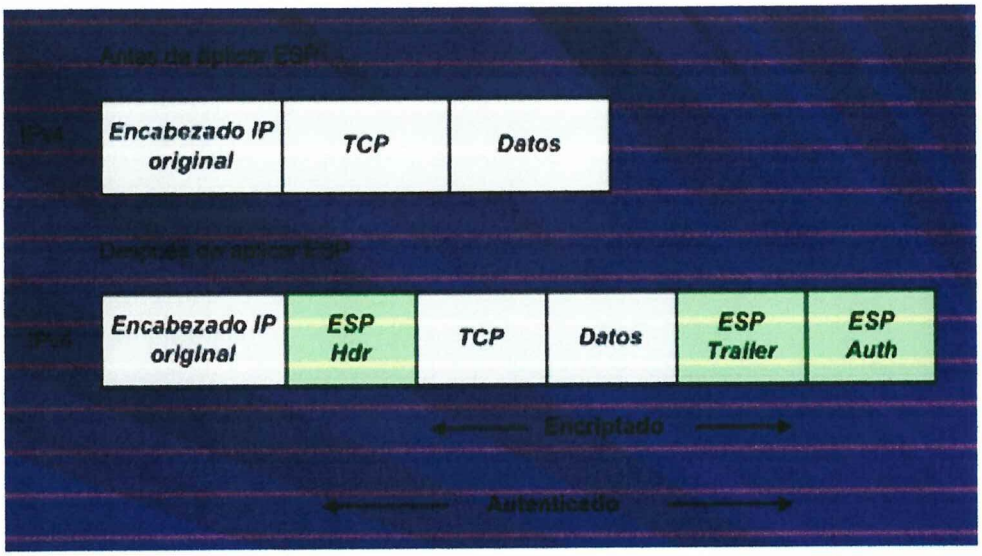


Figura 3. 5 Funcionamiento para IPv4 e IPv6

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica.

Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte, en la mayoría de los casos).

Por esta razón existe un campo de relleno, tal como se observa en la Figura 3.5 , el cual tiene una función adicional es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y por tanto las características del tráfico.

Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

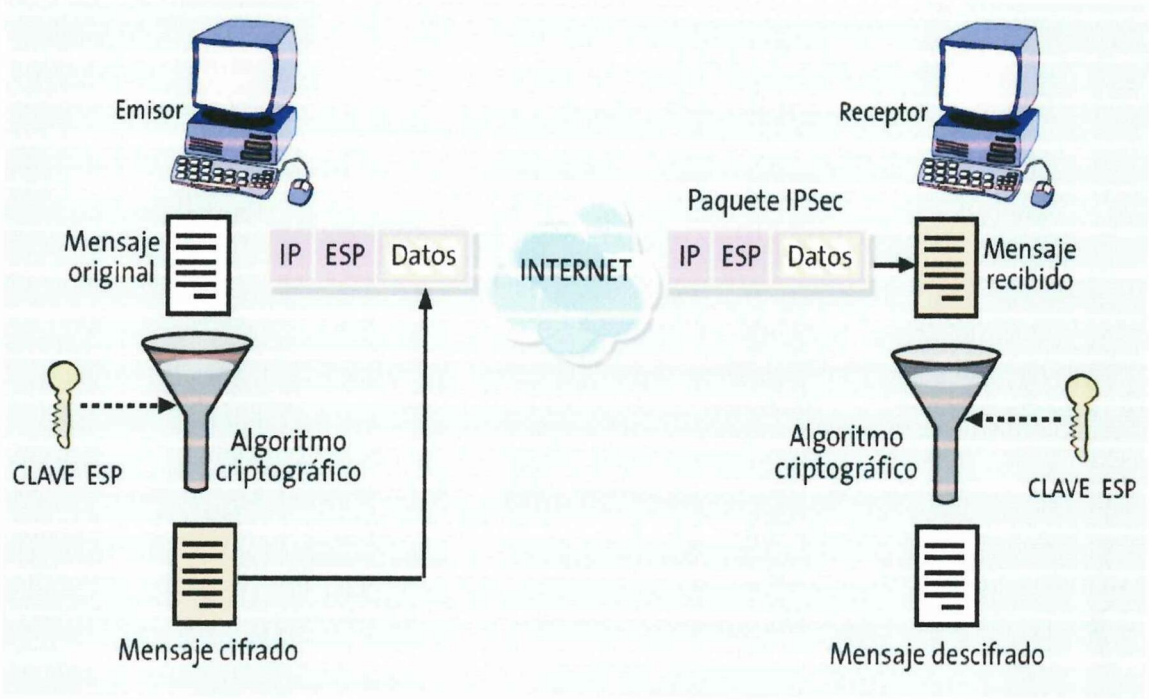


Figura 3. 6 Funcionamiento del protocolo ESP

En la Figura 3.6 se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles.

En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

La distribución de claves de forma segura es por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de

acuerdo tanto en el algoritmo de cifrado o de hash y como en el resto de parámetros comunes que utilizan.

Estos dos protocolos (AH y ESP), sirven para asegurar la autenticación, integridad y confidencialidad de la comunicación.

Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte.

3.2.2.1 Firma y cifrado de paquetes ESP

ESP proporciona protección a las cargas IP. La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué la información está protegida por confidencialidad.

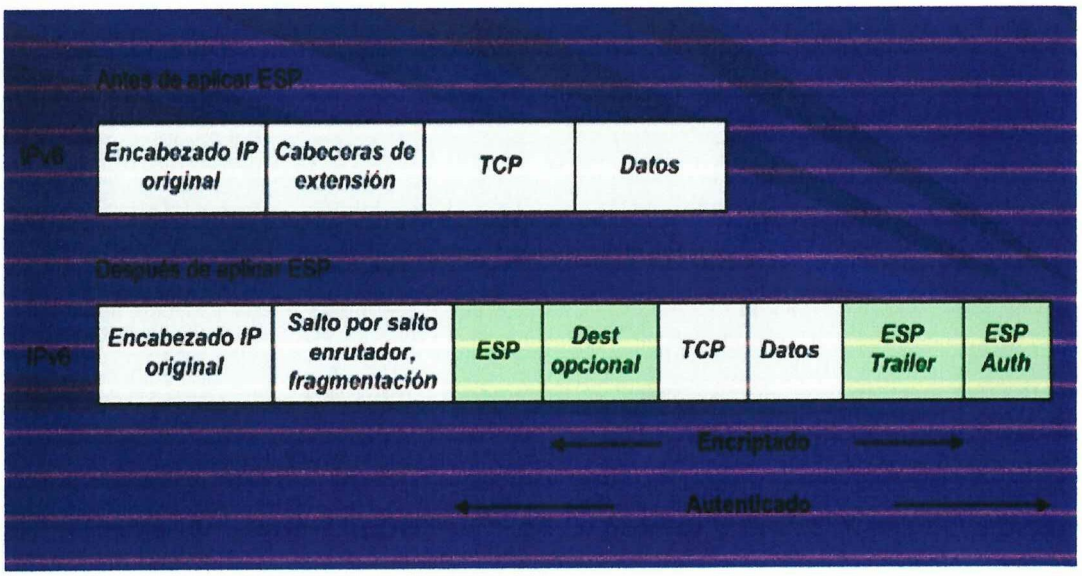
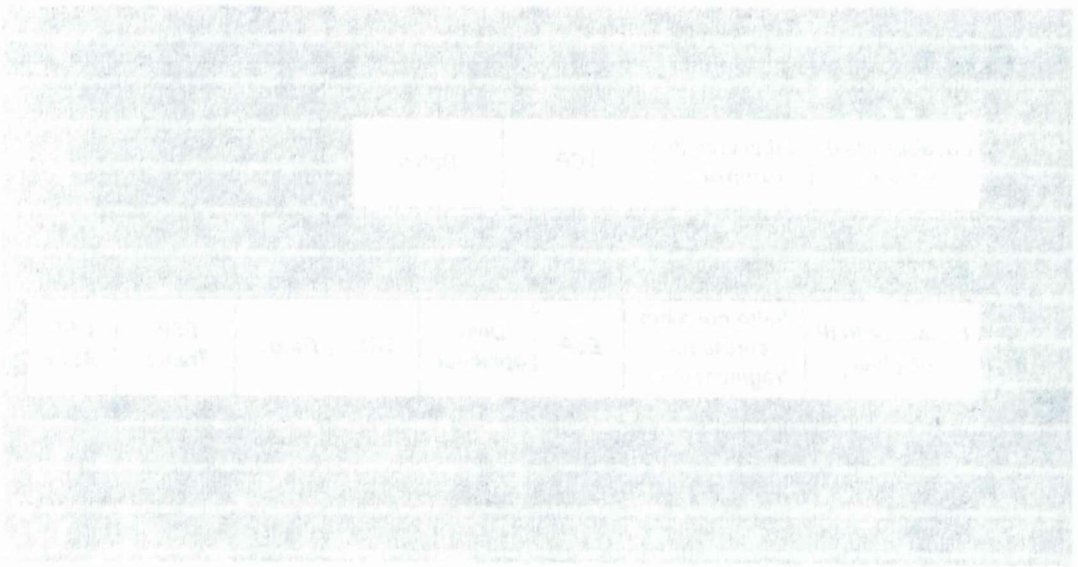


Figura 3. 7 Funcionamiento IPv4 e IPv6 para ESP



3.2.2.2 El modo túnel.

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.

3.2.2.3 Modo de túnel ESP

Todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento.

El modo túnel se utiliza para comunicaciones red a red (puerta a puerta, Gateway a Gateway) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

El modo túnel es empleado principalmente por los Gateway 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. El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando.

Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtual (VPN) 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.

IPSec puede ser implementado bien en un host o bien en un equipo dedicado, tal como un router o un firewall, que cuando realiza estas funciones se denomina gateway IPSec.

La grafica muestra los dos modos de funcionamiento del protocolo IPSec, donde:

- En la Figura 6a se representan dos hosts que entienden IPSec y que se comunican de forma segura.

  Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.
- En la Figura 6b se muestran dos redes que utilizan para conectarse dos gateways IPSec y, por tanto, utilizan una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los gateways IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales.

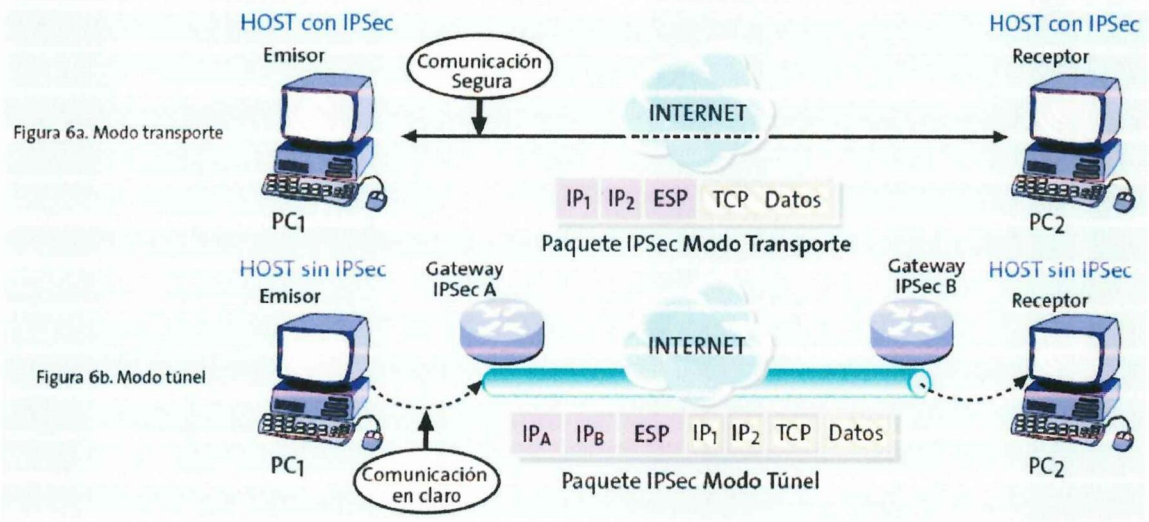


Figura 3. 8 Los modos de funcionamiento transporte y túnel de IPSec

Sin embargo ambos PCs envían y reciben el tráfico como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo las funciones de seguridad en un único punto facilitando así las labores de administración.

Toda la carga ESP se encapsula dentro del nuevo encabezado de túnel, el cual no se cifra. La información del nuevo encabezado de túnel sólo se utiliza para enrutar el paquete desde el origen hasta el punto final del túnel.

Si el paquete se envía a través de una red pública, se enrutará hacia la dirección IP de la puerta de enlace de la intranet receptora. La puerta de enlace descifra el paquete, descarta el encabezado ESP y utiliza el encabezado IP original para enrutar el paquete hacia el equipo de la intranet.

ESP y AH pueden combinarse al utilizar túneles para lograr tanto la confidencialidad del paquete IP enviado por el túnel como la integridad y la autenticación de todo el paquete.

3.2.3 Los modos transporte y túnel en AH y ESP

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionando modos de uso:

3.2.3.1 El modo transporte.

En 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.

El modo de transporte es el predeterminado para IPSec y se utiliza para comunicaciones entre cliente y servidor, proporcionando seguridad de (extremo a extremo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el proceso de seguridad, sólo se transfieren los datos del paquete IP entonces este es cifrada y autenticada.
El modo de transporte proporciona la protección de una carga IP mediante un encabezado AH o ESP. Las cargas IP típicas son segmentos TCP, un mensaje UDP y un mensaje ICMP.

3.2.3.2 Modo de transporte Encabezado de autenticación

El Encabezado de autenticación (AH) proporciona autenticación, integridad y protección para todo el paquete (el encabezado IP y la carga de datos transportados en el paquete).

No proporciona confidencialidad, ya que no cifra los datos. La información es legible, pero está protegida contra modificaciones. AH utiliza algoritmos hash con claves para firmar el paquete y asegurar su integridad.

La integridad y la autenticación se consiguen al situar el encabezado AH entre el encabezado y la carga de IP.

AH se identifica en el encabezado IP con el Id. de protocolo este puede utilizarse por sí solo o combinado con el protocolo de Carga de seguridad de encapsulación (ESP).

3.2.3.3 Encabezado

Identifica la carga IP mediante el Id. de protocolo IP. Por ejemplo, el valor 6 representa TCP.

3.2.3.4 Índice de parámetros de seguridad (SPI)

La dirección de destino y el protocolo de seguridad (AH o ESP), permiten identificar la asociación de seguridad correcta para la comunicación. El receptor utiliza este valor para determinar con qué asociación de seguridad se identifica el paquete. El número de secuencia se usa para impedir ataques de repetición, al impedir el procesamiento múltiple de un paquete.

3.2.3.5 Número de secuencia

Proporciona protección para el paquete. El número de secuencia es un número de 32 bits que aumenta de forma incremental (a partir de 1) e indica el número de paquetes enviados a través de la asociación de seguridad para una comunicación dada.

El número de secuencia no se puede repetir mientras se mantenga la seguridad de modo rápido. El receptor comprueba este campo para asegurarse de que no ha recibido ya un paquete para una asociación de seguridad con este número. Si se recibió alguno, se rechazará este paquete.

3.2.3.6 Datos de autenticación

Contiene el valor de comprobación de integridad, también conocido como código de autenticación de mensaje, que se utiliza para comprobar la autenticación del mensaje y su integridad. El receptor calcula el valor de integración y lo compara con este valor (calculado por el remitente) para comprobar la integridad. El ICV se calcula para el encabezado IP, el encabezado AH y la carga IP.

3.2.3.7 Firma de paquetes con el encabezado AH

AH firma todo el paquete para garantizar su integridad, a excepción de algunos campos del encabezado IP que pueden cambiar durante el trayecto (por ejemplo, los campos Tiempo de vida y Tipo de servicio). Si se utilizan otros encabezados de IPSec además de AH, el encabezado AH se inserta delante de todos ellos.

3.3 IKE el protocolo de control

Un concepto esencial en IPSec es el de asociación de seguridad (SA) es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos Asociaciones Seguras, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la

información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

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

- 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:

3.3.1 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. 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.

3.3.2 En la segunda fase el canal seguro IKE

Negocia los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado.

El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

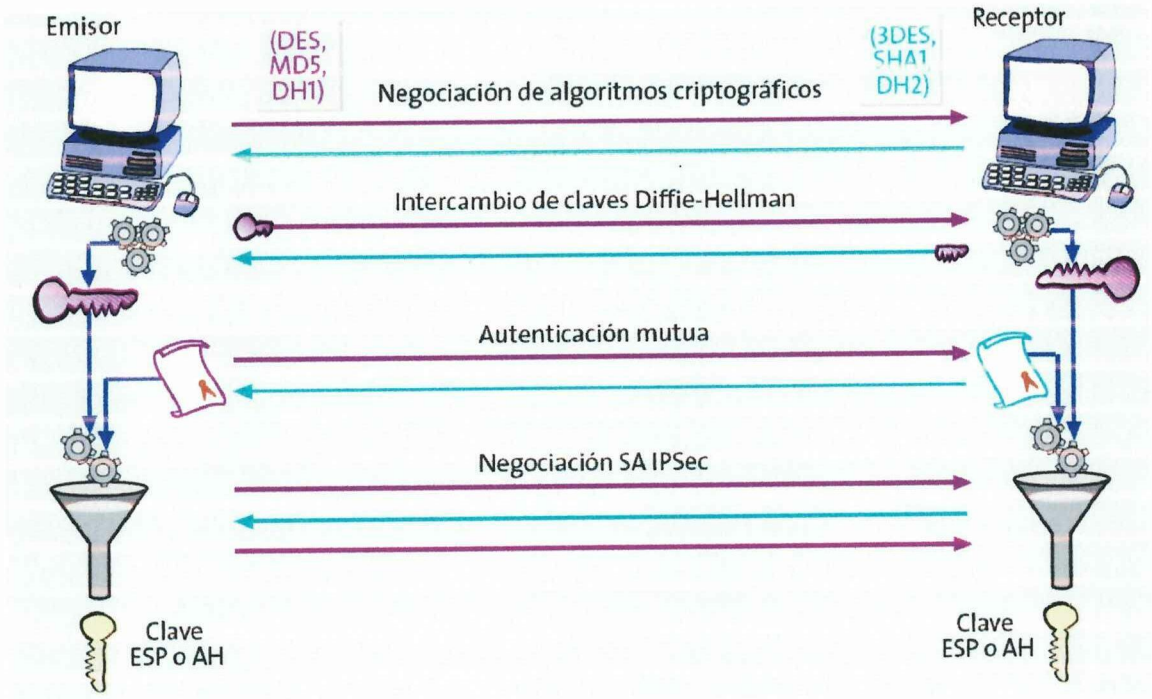


Figura 3. 9 Funcionamiento del protocolo IKE

Se representa de forma representativa 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.

3.3.3 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. 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 usuarios móviles.

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.

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 como formato común de los 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.

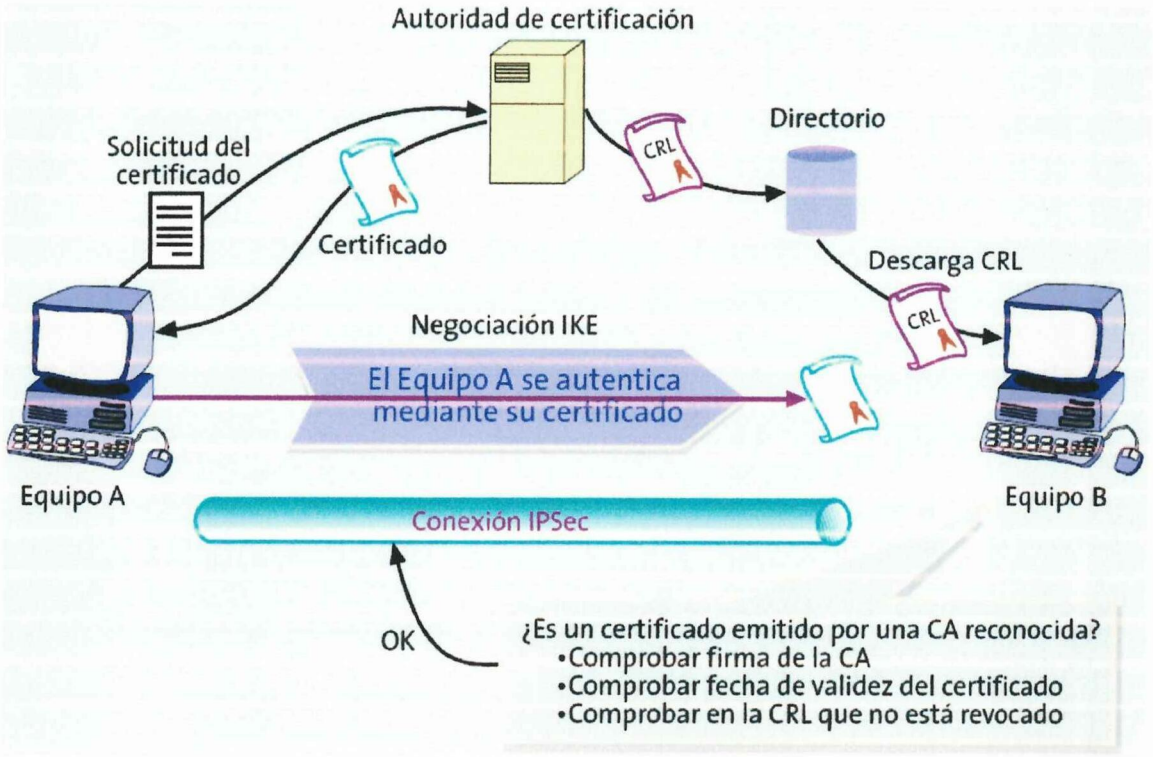


Figura 3. 10 Integración de una PKI en IPSec

En la Figura 3.10 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.

3.3.4 Integridad y autenticación del 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.

3.3.5 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 prudentemente, ya que recién 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 hagan más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.

3.3.6 Detección de repeticiones

La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante 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.

3.3.7 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.

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.

3.3.8 No repudio

El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante.

Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

3.4 Aplicaciones prácticas de IPsec

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cuál 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.

En este apartado veremos como el protocolo IPSec proporciona una solución viable para tres escenarios:

- Interconexión segura de redes locales.

- Acceso seguro de usuarios remotos.
- Extranet o conexión de una corporación con sus partners y proveedores.

Para cada uno de los escenarios mencionados se desarrolla una aplicación práctica concreta y se presentan las ventajas de utilizar IPSec.

3.4.1 La interconexión segura de redes locales (intranet)

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. Por 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.

En la Figura 3.11 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.

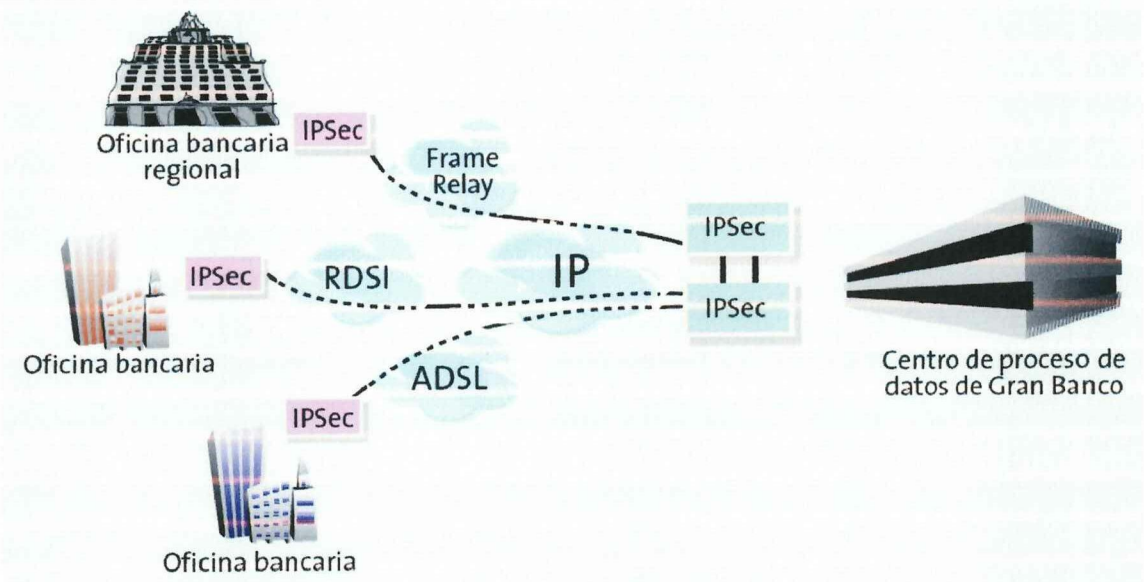


Figura 3. 11 Interconexión de redes locales en entorno financiero

Como puede observarse en la Figura 9, 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.

3.4.2 El acceso seguro de usuarios remotos

La gran 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.

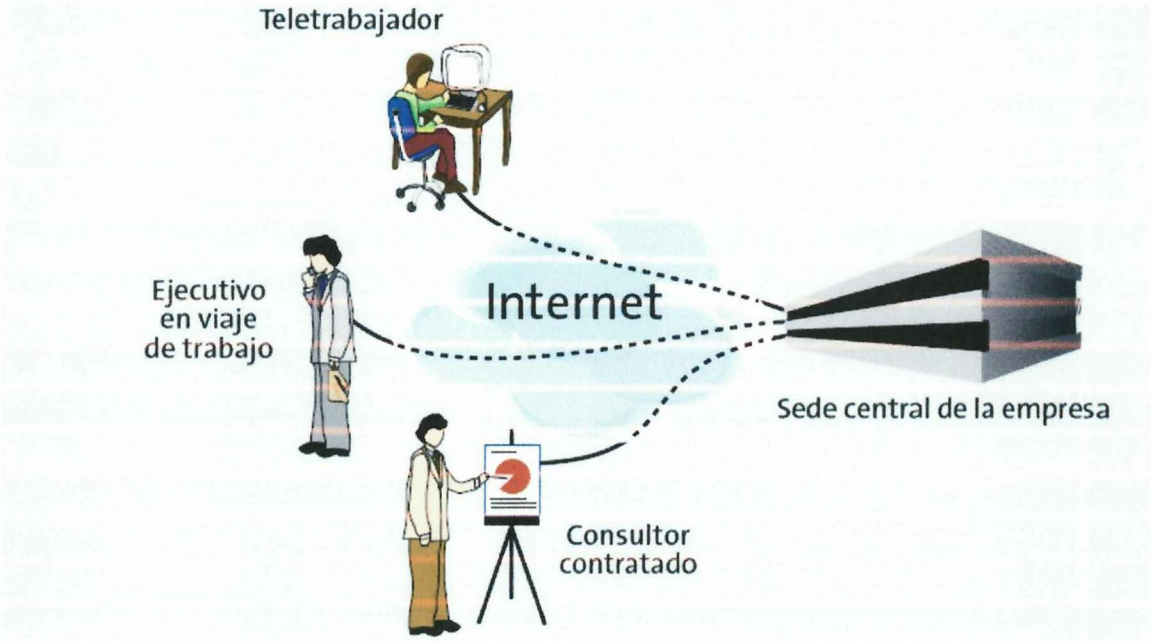


Figura 3. 12 Acceso seguro de usuarios remotos a una corporación

En la Figura 3.12 se presenta un escenario típico de acceso remoto seguro a una corporación. 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 2000 o Solaris 8 incluyen un cliente IPSec.

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.

CAPÍTULO 4

Encuestas realizada para el levantamiento de información sobre la seguridad en el internet de la misma manera verificar el alto o bajo grado de conocimiento sobre las vulnerabilidades que hoy en día es un tema muy importante tanto para las empresas de Argentina y Ecuador.

4.1 RECOLECCIÓN Y PROCESAMIENTO DE LA INFORMACIÓN

4.1.1 Recolección

Para realizar la recolección de datos tenemos que usar una gran diversidad de técnicas y herramientas que pueden ser utilizadas por el analista para desarrollar los sistemas de información, los cuales pueden ser la entrevistas, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos.
Todos estos instrumentos se aplicarán en un momento en particular, con la finalidad de buscar información que será útil a una investigación en común. En la presente investigación trata con detalle los pasos que se debe seguir en el proceso de recolección de datos, con las técnicas ya antes nombradas.

4.2 Procesamiento de la información

Mediante está capacidad el Sistema de Información efectúa cálculos de acuerdo con una secuencia de instrucciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera o técnica a partir de los datos que contiene un estado de resultados o un balance general.

4.3 Análisis e Interpretación de los resultados

Identifica las necesidades de información precisas para el levantamiento de información, por lo que es necesario seleccionar los instrumentos de medición y/o técnicas de recolección de información, permitiéndonos de esta forma optimizar el tiempo en la recolección de información para ello utilizamos las siguientes fuentes y técnicas de recolección de información.

4.3.1 Aplicación de Técnicas de Investigación

Se identificó las necesidades de los usuarios de internet para realizar la investigación, por lo que fue necesario seleccionar las técnicas de recolección de información, para de esta manera optimizar recursos económicos y de tiempo empleados en esta actividad.

Consecuentemente se decidió utilizar las siguientes fuentes y técnicas de recolección de información.

4.3.2 Encuestas

Se realizó las respectivas encuestas al personal técnico de las Empresas Akros del Ecuador, CONAMU (Consejo Nacional de Mujeres) y Instituto de Seguridad Social de Latacunga, el cual conformó un total de 47 personas y esto permitió la recopilación de la información necesaria para encontrar el sustento del desarrollo de la investigación.

4.3.3 Entrevista

Se realizaron entrevistas a los Jefes Departamentales de Sistemas de cada Institución involucrada para conocer sus opiniones y recomendaciones, ya que

tienen mayor experiencia sobre lo que es el Manejo de Seguridades en Información de sus actividades por Internet y las necesidades que el usuario tiene.

4.3.4 Observaciones

Al realizar las entrevistas se observó la prioridad en el manejo y cuidado de información indicándome la operatividad e instalación del sistema de registro de datos desde un Nodo (usuarios de internet), cabe mencionar que no toda la información está disponible ya que existe documentación que se considera de uso exclusivo para las empresas.

De igual manera se percibió la preocupación del personal que no tienen conocimientos seguridad a excepción del IESS, que si posee un método de encriptamiento de datos para transacciones de sus afiliados, por lo que la idea más adecuada fue la sociabilización en aplicar un método de control y seguridad de datos en la red.

4.3.5 Población

La población seleccionada para la realización del presente proyecto de tesis la constituyó el personal técnico de los departamentos de Sistemas, que conformo un total de 47 personas.

4.3.6 Muestra

Debido a que el número de involucrados en la presente investigación es un total de 47 personas, el mismo que es un grupo pequeño, se procederá a tomarlos como muestra en su totalidad.

ENCUESTA DIRIGIDA A LOS DEPARTAMENTOS DE SISTEMAS DE AKROS DEL ECUADOR, IESS-LATACUNGA, CONAMU

PREGUNTA N.- 1

1. ¿Existe en la empresa un área de seguridad informática?

Si ☐ No ☐

Tabla 4. 1

Opinión	Frecuencia	Porcentaje (%)
Si	5	11%
No	42	89%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

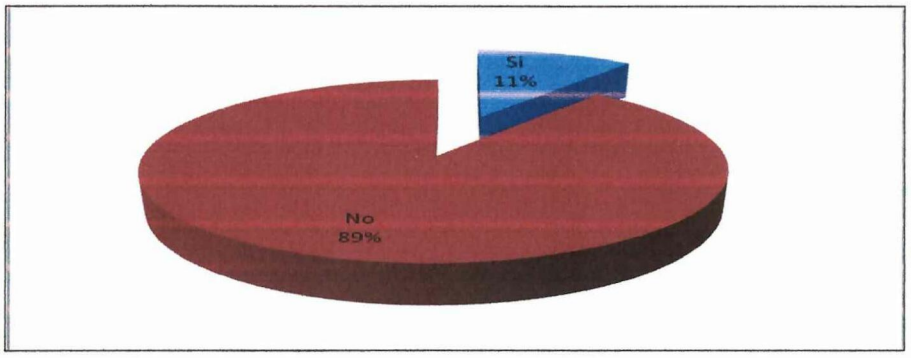


Figura 4. 1

ANÁLISIS:

El 89% de los encuestados responden que no existe un área de seguridad informática, mientras que el 11% responden que si, lo cual refleja la poca actividad de seguridad en las instituciones en general, esto se da por falta de conocimiento o el uso indebido de herramientas de seguridad.

PREGUNTA N.- 2

2. ¿Ha realizado usted en el último año capacitación referida a seguridad informática vinculada con internet?

Si ☐ No ☐

Tabla 4. 2

Opinión	Frecuencia	Porcentaje (%)
Si	11	23%
No	36	77%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

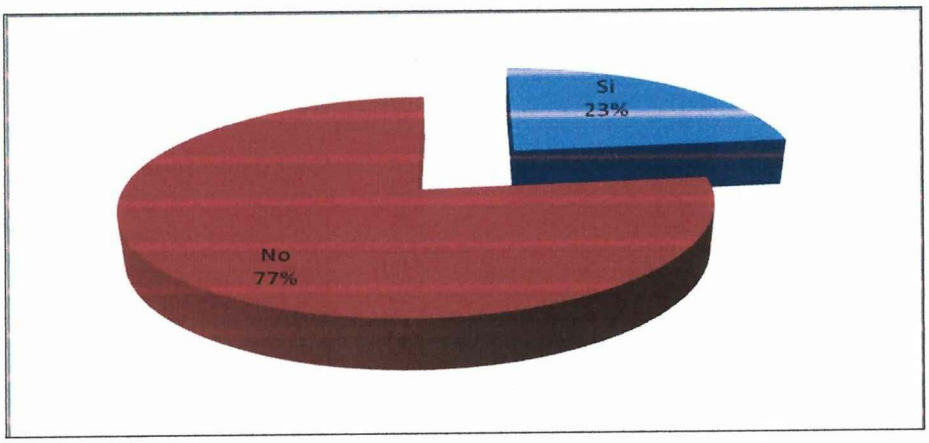


Figura 4. 2

Si responde afirmativamente sobre ¿qué aspectos?

Descargas y actualizaciones .....

Navegadores Web .....

Servicios de mensajería electrónica .....

Redes .....

Otros (escriba el nombre) .....

Tabla 4. 3

Opinión	Frecuencia	Porcentaje (%)
Descargas y actualizaciones	2	18%
Navegadores Web	5	46%
Servicios de mensajería electrónica	2	18%
Redes	2	18%
Otros (escriba el nombre)	0	0%
Total	11	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

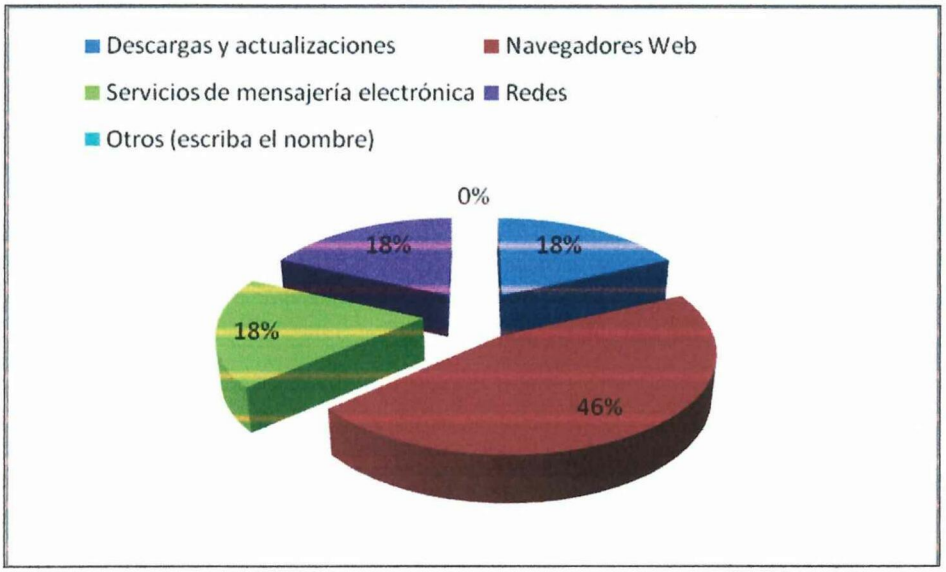


Figura 4. 3

ANÁLISIS.

Respecto al grado de conocimientos del personal técnico de los departamentos de sistemas sobre seguridades en internet, solo conocen los típicos, el tema de

seguridades es un campo no conocido por la gran parte de personal técnico responsable del manejo de comunicaciones vía internet.

PREGUNTA N.- 3

3. ¿Utilizan en la empresa protocolos de seguridad para controlar el acceso a información sensible (IPSec, https, SSL, etc.)?

Si ☐ No ☐

¿Cuáles?.....

Tabla 4. 4

Opinión	Frecuencia	Porcentaje (%)
Si	2	4%
No	45	96%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

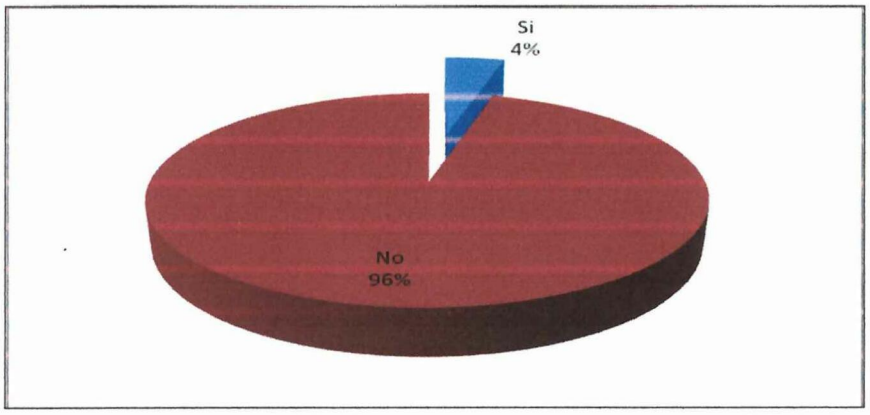


Figura 4. 4

ANÁLISIS:

El 96% de los encuestados son evidencia, de que no conocen ningún método de los mencionados en la encuesta, mientras que el 4% los conoce pero no se

utilizan, esto significa que falta mucho por investigar el tema de seguridades en internet.

PREGUNTA N.- 4

4. ¿Hay en la empresa un presupuesto específico para seguridad informática?

Si ☐ No ☐

Tabla 4. 5

Opinión	Frecuencia	Porcentaje (%)
Si	2	4%
No	45	96%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

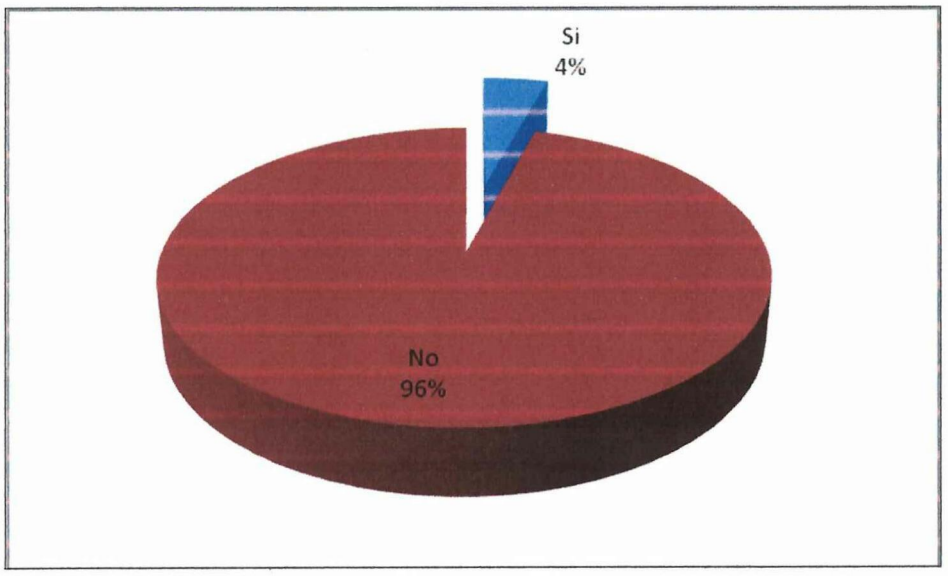


Figura 4. 5

ANÁLISIS:

El 96% de los encuestados mencionan que no existe un presupuesto para seguridad en información, mientras que el 4% cita que si existe este presupuesto, esto quiere decir que muy pocas empresas toman en serio la seguridad en Internet.

PREGUNTA N.- 5

5. ¿Ha crecido en el último año, la inversión en seguridad informática (hardware, software, capacitación, etc) para el uso de aplicaciones vinculadas con internet?

Si ☐ No ☐

Tabla 4. 6

Opinión	Frecuencia	Porcentaje (%)
Si	15	26%
No	42	74%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

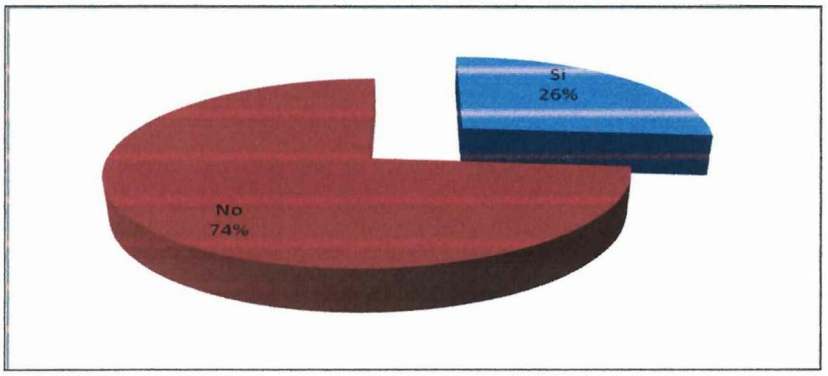


Figura 4. 6

ANÁLISIS:

Si hablamos de desconocer métodos de seguridades basados en encriptamiento, el 74% menciona que no existe una inversión en este campo, mientras que el 26% dice que si, lo cual refleja el poco uso e investigación de seguridad en el manejo de información.

PREGUNTA N.- 6

6. ¿Cree Ud. que han mejorado en el último año las medidas de seguridad para controlar el acceso a la información en internet por parte de los usuarios?

Si ☐ No ☐

Porque?.....

Tabla 4. 7

Opinión	Frecuencia	Porcentaje (%)
Si	15	32%
No	32	68%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

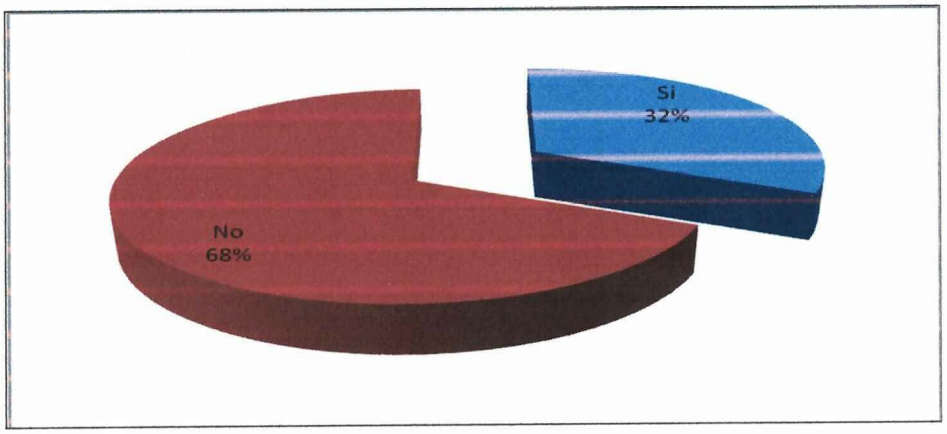


Figura 4. 7

ANÁLISIS:

El 68% menciona que no se ha incrementado las seguridades en el manejo de información en el internet, mientras que el 32% afirma que si, esto significa que la poca actividad de métodos en el internet para proteger la información, esta desechada en la mayoría de empresas, por su complejidad o dificultad de uso.

PREGUNTA N.- 7

7. ¿En base a la pregunta anterior, cuales aspectos cree usted que deberían mejorarse actualmente?

.....

Tabla 4. 8

Opinión	Frecuencia	Porcentaje (%)
Correo electrónico	6	13%
Ftp	16	34%
Http	11	23%
Internet	8	17%
No Opina, No Sabe	6	13%
Total	26	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

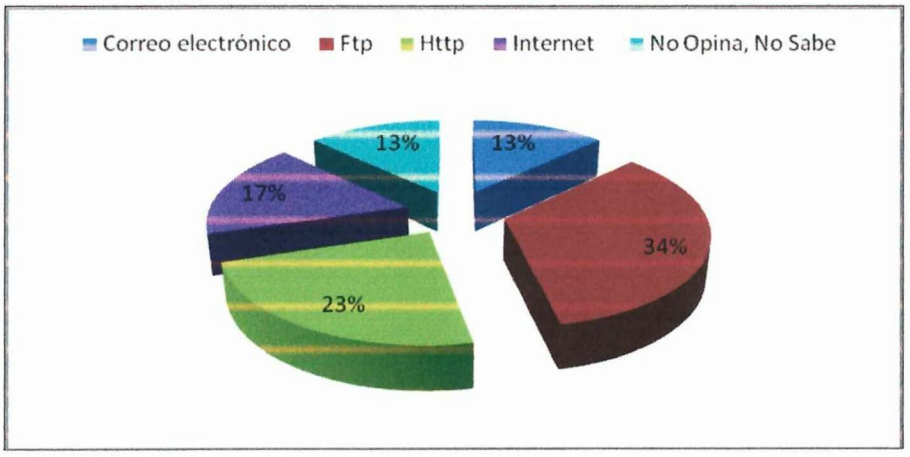


Figura 4. 8

ANÁLISIS:

La mayoría coinciden en que los medios que mas seguridad deberían brindar son los de transporte de información sobre internet, es decir los medios vulnerables.

PREGUNTA N.- 8

8. ¿Cuál es el aporte del personal técnico al momento de trabajar con información confidencial para gestionar su buen uso y evitar el plagio de la misma?

.....

Tabla 4. 9

Opinión	Frecuencia	Porcentaje (%)
Muy Bueno	1	2%
Bueno	5	11%
Regular	6	13%
Malo	28	59%
No Opina, No Sabe	7	15%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

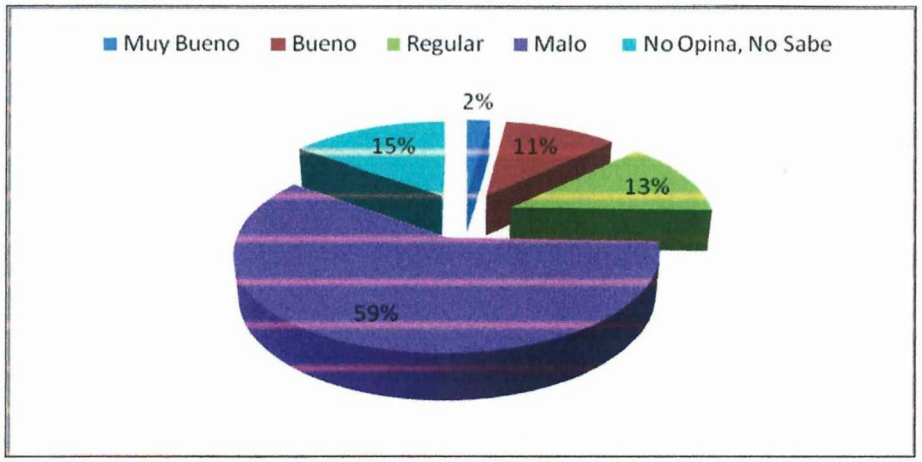


Figura 4. 9

ANÁLISIS:

El 59% de los encuestados opina que percibe como mala la gestión de personal técnico en cuestión de seguridades en el uso del internet y sus medios, el 11% indica que es bueno, mientras que el 13% indica que a medias se cubre un rango de seguridad, y el 2% indica desconocer este tipo de herramientas o normas para una adecuada seguridad.

PREGUNTA N.- 9

9. ¿Cuál de estas herramientas con acceso a internet utilizan en su empresa?

1 ☐ email 2 ☐ Messenger 3 ☐ ftp 4 ☐ browser 5 ☐ otros

Tabla 4. 10

Opinión	Frecuencia	Porcentaje (%)
Email	18	38%
Messenger	8	17%
Ftp	6	13%
Browser	13	28%
Otros	2	4%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

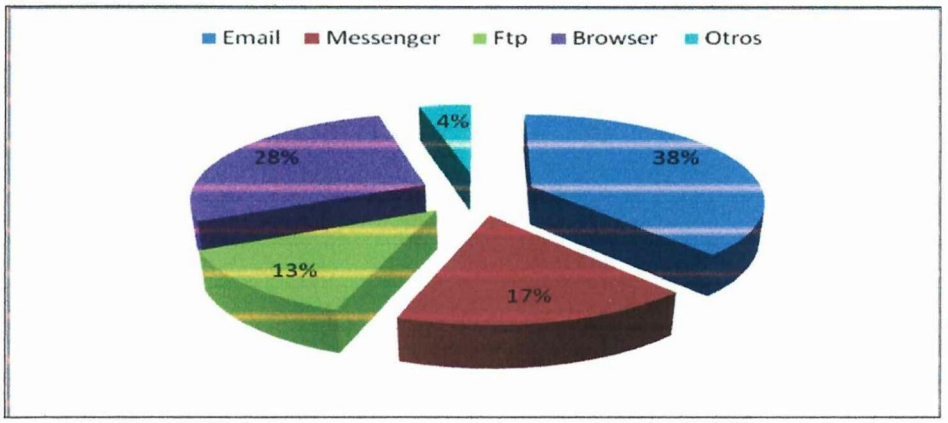


Figura 4. 10

ANÁLISIS:

En total de los encuestados, la mayoría cita herramientas de internet como medio de sus actividades diarias, esto denota una mayor responsabilidad en su uso, por lo tanto la seguridad también debería estar en el mismo nivel o mejorado en todo caso.

PREGUNTA N.- 10

10. ¿Han tenido incidentes en el último año con el uso de estas herramientas? En caso afirmativo, mencione cuales (ej: virus, pérdida de información, acceso no autorizado, spam, etc.)

.....

Tabla 4. 11

Opinión	Frecuencia	Porcentaje (%)
Virus	17	36%
Perdida de información	15	32%
Acceso no autorizado	10	21%
Spam	0	0%
No Opina, No sabe	5	11%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

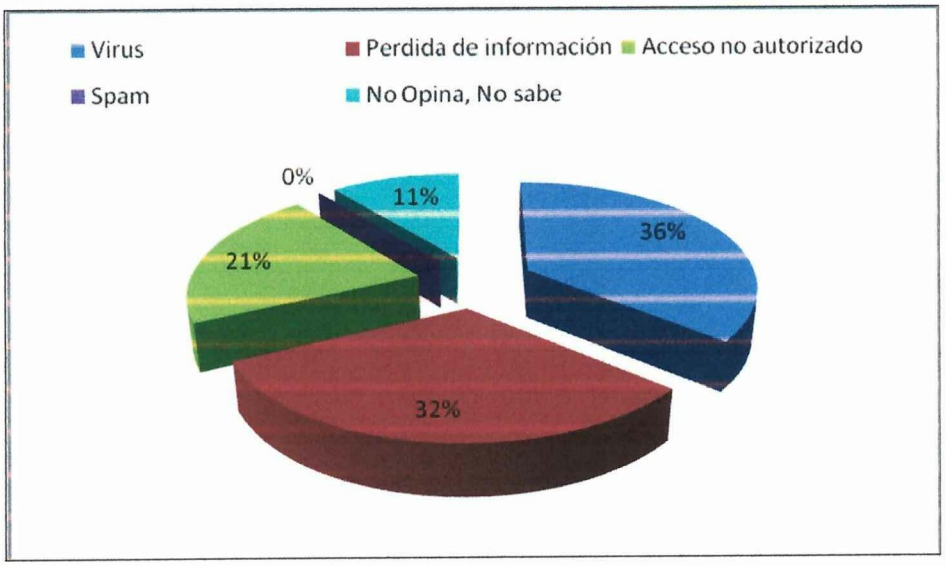


Figura 4. 11

ANÁLISIS:

En relación a las actividades la mayor vulnerabilidad es el traslado de información, esto conlleva a que en mayor proporción los daños y perdidas de información se dan por factores externos: como virus, plagio, acceso indebido, etc. Lo cual permite la ineficiencia de los servicios en la comunicación.

PREGUNTA N.- 11

11. ¿Existen controles en relación a los sitios accedidos por los usuarios?

Si ☐ No ☐

Tabla 4. 12

Opinión	Frecuencia	Porcentaje (%)
Si	10	21%
No	37	79%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

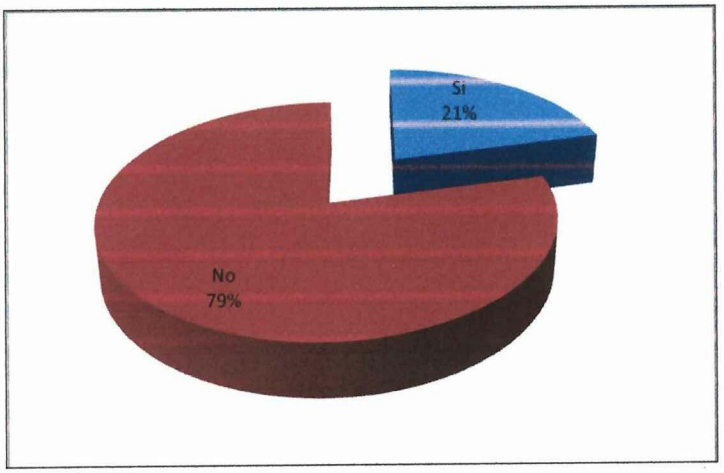


Figura 4. 12

ANALISIS:

El 79% responde que no existen controles o no son suficientes para el buen desempeño, y el 21% responde que si poseen seguridades, lo cual indica que la mayoría de usuarios no tiene un control adecuado incluso con ciertos métodos alternos de seguridades estos no son implementados con eficiencia.

PREGUNTA N.- 12

12. ¿Se plantean sanciones para el personal que utilice indebidamente herramientas con acceso a internet?

Si ☐ No ☐

Tabla 4. 13

Opinión	Frecuencia	Porcentaje (%)
Si	8	17%
No	39	83%
Total	47	100%

Fuente: Personal técnico de los departamentos de sistemas de Akros del Ecuador, IESS, CONAMU

Elaboración: Investigadora

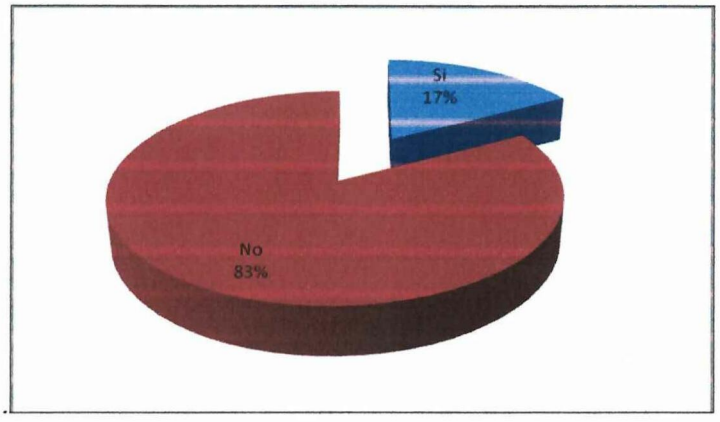


Figura 4. 13

ANÁLISIS:

El 83% de los encuestados responde que no se aplican sanciones a las personas o usuarios que den mal uso al internet en general, mientras que el 17% responde que si, se dan sanciones, esto es mas imprescindible cuando existen normas o políticas de uso en el medio laboral.

PREGUNTA N.- 13

13. Le pido contestar las siguientes preguntas consignando una X en el casillero de su preferencia, utilizando la siguiente escala de valoración:

Tabla 4. 14

4	3	2	1	0
Totalmente de Acuerdo	Parcialmente de Acuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo	No Opina, No Sabe
Muy Satisfecho	Satisfecho	Parcialmente Satisfecho	Insatisfecho	No Opina, No Sabe
Muy Bueno	Bueno	Regular	Malo	No Opina, No Sabe

Nº	CUESTIONARIO	VALORACIÓN (de 0 a 4)				
		0	1	2	3	4
a)	¿Cree conveniente limitar el acceso a internet según la necesidad del usuario?	0	13	11	15	8

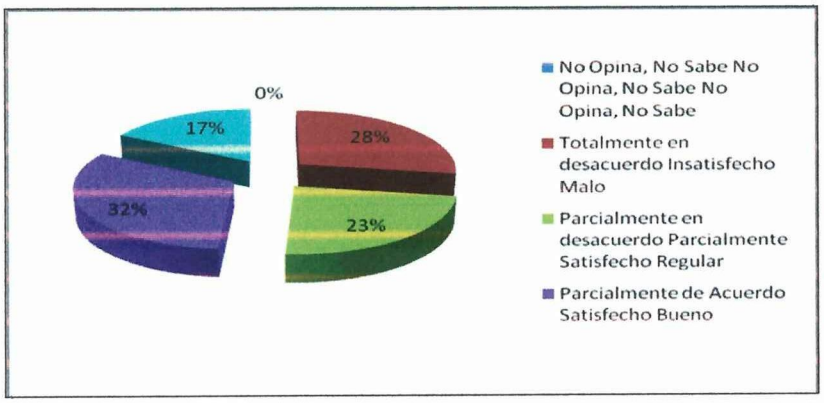


Figura 4. 14

ANÁLISIS.

Es imprescindible que se emitan normas o que en algunos casos se cumplan con las mismas, esto según las encuestas la mayoría afirma el deseo de contar con herramientas que brinden el buen uso del internet.

Nº	CUESTIONARIO	VALORACIÓN (de 0 a 4)				
		0	1	2	3	4
b)	¿Están conformes los usuarios en cuanto a las medidas de seguridad de información que la empresa adopta para la utilización de internet al manejar sus aplicaciones?	2	22	13	8	2

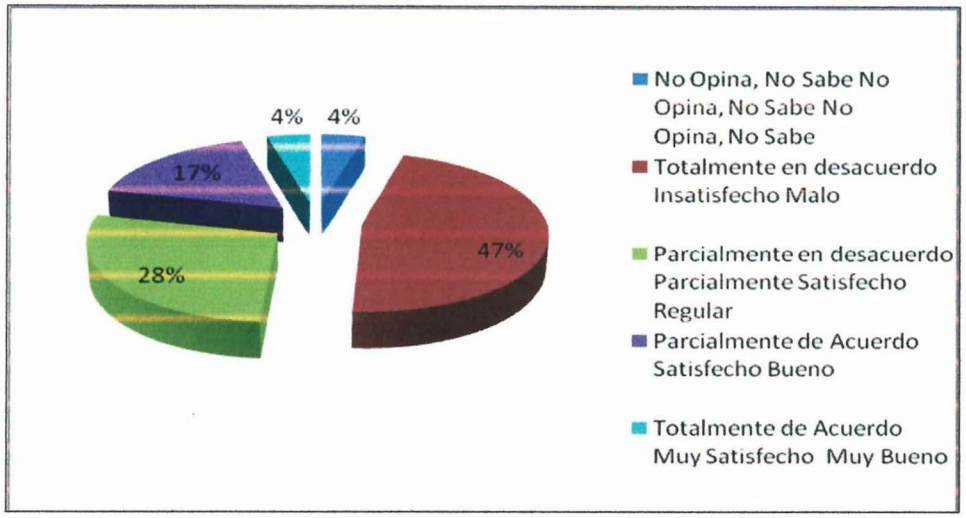


Figura 4. 15

ANÁLISIS.

Anteriormente se tiene una pregunta que indica la inconformidad de los usuarios y personal técnico con las medidas de seguridad que tiene una empresa, lo cual implica en esta pregunta el alto número de personas en desacuerdo con la falta de medios de control y seguridad en el manejo de información en el internet.

Nº	CUESTIONARIO	VALORACIÓN (de 0 a 4)				
		0	1	2	3	4
c)	¿Qué valoración le daría a la seguridad que cuenta su institución para mantener segura la información entrante y saliente que implica interactuar en internet? (navegación en internet, webmail, etc.)	2	12	8	17	8

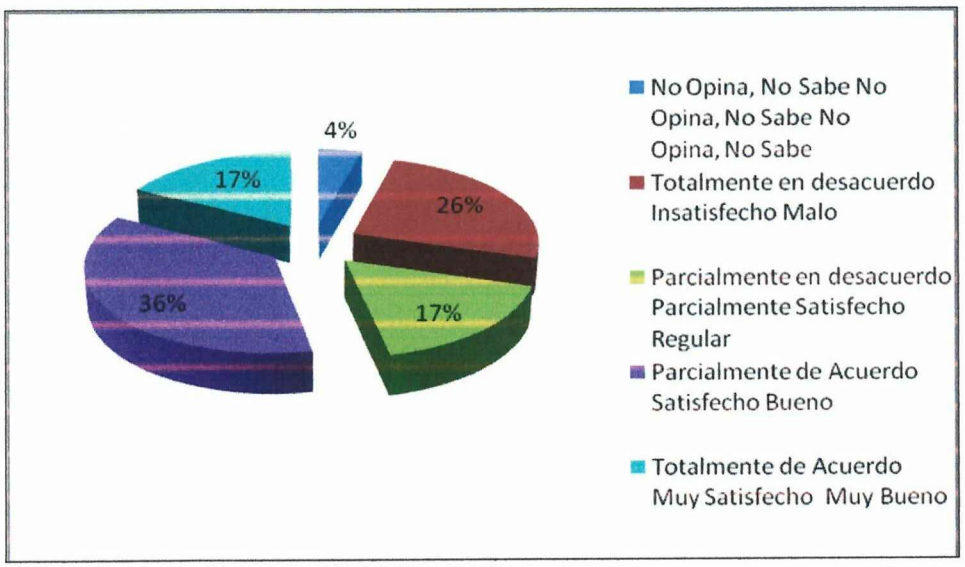


Figura 4. 16

ANÁLISIS:

La valoración de seguridades en la mayoría de empresas es muy baja con respecto al uso de seguridades, esto se refleja en los continuos problemas en el uso y la desconfianza para trasladar información relevante por internet.

Nº	CUESTIONARIO	VALORACIÓN (de 0 a 4)				
		0	1	2	3	4
d)	¿Cómo percibe la seguridad con la que cuenta el internet a nivel global?	2	35	5	3	2

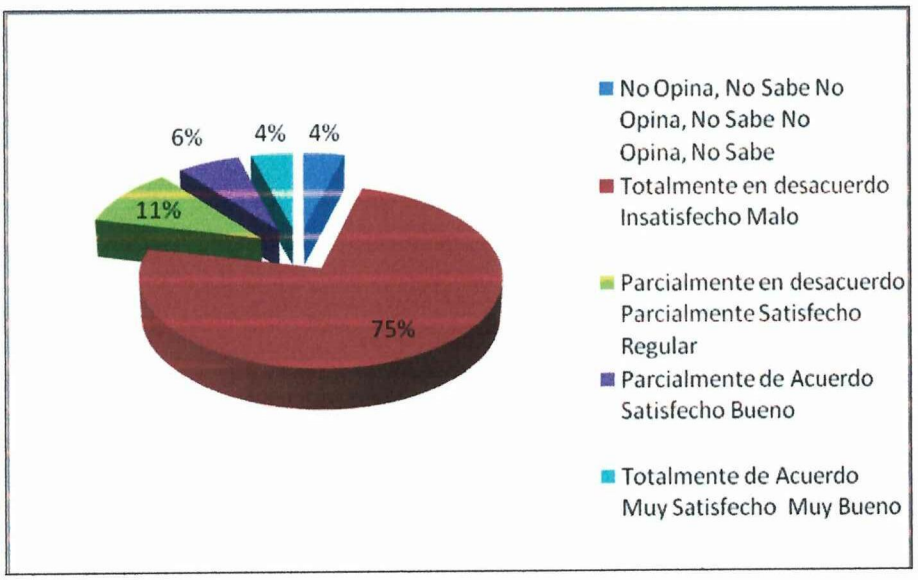


Figura 4. 17

ANÁLISIS:

El 75% de las opciones presentadas, indica que a nivel general la seguridad en el internet es mala, en vista de que las herramientas por su complejidad no son sencillas de implementarse en los sitios de trabajo, aunque este debería ser el motivo de investigar y utilizar estos métodos.

4.1. CONCLUSIONES Y RECOMENDACIONES DE LAS ENCUESTAS REALIZADAS

4.1.1. Conclusiones

- ✓ Luego de haber realizado las diferentes encuestas y enmarcándome en el punto sobre la necesidad de investigar y analizar el mejor método de seguridad, la mayoría del personal técnico está de acuerdo con el desarrollo de la presente investigación que cubra las necesidades de realizar los análisis de situaciones de daños de información en el medio.

- ✓ La decisión de seleccionar del método estará orientado a satisfacer la mayor parte de necesidades de seguridad de información en el internet, por lo cual esto dará la pauta o el camino para futuras investigaciones e implementaciones de este tipo.

4.1.2. Recomendaciones

- ✓ En vista de que la mayoría de empresas hoy por hoy cuentan con una buena infraestructura tecnológica en sus áreas de apoyo y toma de decisiones, es factible que sean de uso común un método de solución a las vulnerabilidades de acceso hacia la información, por lo cual se recomienda continuar con la presente investigación con estudiantes que tomen la posta de seguir en búsqueda de posibles mejores alternativas de solución, y den continuidad a la misma.

- ✓ El apoyo institucional es importante y su apertura a permitir la confianza de que el personal técnico mediante la capacitación y conocimientos de esta investigación se motiven y acoplen un medio de seguridad en la empresa pública como privada.

CAPÍTULO 5

5.1 CONCLUSIONES Y RECOMENDACIONES DE LOS METODOS DE SEGURIDAD.

5.1.1 CONCLUSIONES:

- Con la masificación de internet, la demanda de servicios sobre esta plataforma por parte de las empresas ha crecido sustancialmente. Sin embargo, esto ha generado también nuevos y potencialmente mayores riesgos que atentan contra la integridad de la información y la seguridad en las empresas.

- Actualmente existen un importante número de herramientas (protocolos, etc) que permiten reducir el impacto de potenciales riesgos. Sin embargo, el aumento de vulnerabilidades exige una actualización casi permanente de estas herramientas, implicando una capacitación similar por parte de los profesionales en sistemas.

- Es imprescindible, el aplicar un método de seguridad sobre los estándares basados en intercambio de información en el Internet, por lo tanto la presente investigación ha permitido tener una justificación valedera haciendo del IPSec una alternativa confiable en el manejo de información en áreas vulnerables como Comercio Electrónico y Empresas que intercambian información en su toma de decisiones.

- El IPSec al ser un método basado en plataformas Point to Point (punto a punto), permiten mayor fiabilidad y protección de terceros en el envió –

recepción de información en la red, por lo tanto su alcance es amplio de acuerdo a los equipos que realicen intercambio de información.

- Uno de los aspectos importantes en el trabajo de investigación, estuvo orientado a conocer la realidad de las empresas en cuanto al grado de conocimiento y aplicación de métodos de seguridad. En este sentido, se ha podido observar una reticencia de parte de los responsables de sistemas, por brindar información acerca del funcionamiento interno de las empresas.

- Si bien un porcentaje muy elevado de los cuestionarios recibidos dan cuenta de la importancia que le asignan a los aspectos de seguridad, un porcentaje muy reducido investiga al respecto o se ha capacitado durante el último año, lo cual representa un enorme riesgo para las empresas.

- Otro aspecto común es la ausencia en general de áreas de seguridad específicamente conformadas, lo cual dificulta la definición de presupuestos e inversión correspondiente.

- Cerca del 60% de los entrevistados mencionan que su actividad es mal vista o considerada por los usuarios cotidianos en las empresas, dándole escasa valoración a las tareas que diariamente realizan en pos de mejorar los aspectos de seguridad.

- Un elevado porcentaje (83%) comenta que no aplican sanciones a los usuarios que no respetan las políticas de seguridad en la empresa. Esto incide para que los mismos puedan tomar mayor conciencia acerca de los verdaderos riesgos que esta implica.

- Se observa una marcada oposición entre la manera que perciben la seguridad los usuarios cotidianos y el personal técnico.

- Un aspecto donde los futuros profesionales en sistemas de información deberán colocar mayor énfasis es en concientizar en mayor medida a los usuarios de las empresas, respecto de la importancia de adoptar criterios y mecanismos de seguridad y los beneficios que brinda el aplicar los mismos. Esto resulta valido también para que las empresas entiendan que la inversión en herramientas de seguridad y capacitación al personal de sistemas debe ser considerado como tal y no visto simplemente como un gasto.

5.1.2 RECOMENDACIONES

- Se hace factible la sociabilización de los métodos existentes en todos sus ámbitos de aplicación, tomando en cuenta que existe muy poco conocimiento de parte del personal técnico de las Instituciones vinculadas con las comunicaciones, además de ser imprescindible el aplicarlos en todos sus niveles.

- Además se hace necesario, el profundizar su estudio con la capacitación y la búsqueda de instituciones basadas en sus experiencias en el manejo de información, y cuál fue la forma de solucionar estas vulnerabilidades.

- Es recomendable, que estudiantes de nuestra especialidad tomen la posta del presente estudio para poder describir y ofrecer a la comunidad informática la solución a los problemas de violación y daño hacia los datos en una red.

- Tomando en cuenta las falencias descritas en el traslado de paquetes sobre IP en la identificación de los problemas, y contando con las bondades del

IPSec como Algoritmo de seguridad sobre información, describen elementos que favorecen a la confianza de parte de los usuarios en una red de datos.

5.2 BIBLIOGRAFIA:

Consultada:

- http://www.unav.es/SI/servicios/seguridad/faq.html#13
- http://es.wikipedia.org/wiki/Transport_Layer_Security
- http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml#OSI
- http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm
- http://personales.mundivia.es/lapi/pgp/pgp.htm
- http://www.eumed.net/cursecon/ecoinet/seguridad/autentificacion.htm
- http://www.reduy.com/computacion/ms-com-electronico/technet-8.htm
- http://es.tech-faq.com/tls-transport-layer-security.shtml&prev=hp&rurl=translate.google.com
- http://www.2.dc.uba.ar/materias/tc/downloads/apuntes/smtp_pop_imap.pdf
- http://www.terra.es/personal6/morenocerro2/seguridad/ssl/ssl_8.html
- http://developersdotnet.com/blogs/marcos/archive/2007/05/22/criptograf-a-algoritmos-sim-tricos.aspx
- http://developersdotnet.com/blogs/marcos/archive/2007/05/22/criptograf-a-algoritmos-sim-tricos.aspx
- http://www.scribd.com/doc/12882085/Manual-IPsec-Terminado(manual)

5.3 GLOSARIO DE TERMINOS

A

Autenticación: También se utiliza como una firma electrónica de documentos que de esta manera se encuentran refrendados en forma legal (código numérico único).

Autenticación codificada: Es una forma de encriptar la contraseña, antes de enviarla por Internet, distinta a la autenticación básica.

ADSL: Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales. Con la apropiada actualización por parte de las compañías telefónicas, éstas pueden suministrar 6 Mbps de transmisión de datos.

Algoritmo: Descripción exacta de la secuencia en que se ha de realizar un conjunto de actividades tendientes a resolver un determinado tipo de problema o procedimiento.

Algoritmos standard: Son aquellos que permiten la comunicación entre sistemas standard de distintos fabricantes.

ATM (Modo de Transmisión Asíncrona) Sistema de transmisión de datos usado en banda ancha para aprovechar al máximo la capacidad de una línea. Se trata de un sistema de conmutación de paquetes que soporta velocidades de hasta 1,2 Gbps.

B

Bit (Dígito binario). Unida básica de información 0-1, usada por las computadoras para la entrada de información, almacenamiento y transmisión.

Browser: Programa que provee una manera de acceder a la información en la World Wide Web. ejem: el Netscape y el Explorer.

C

Clave privada: Es conocida solamente por un usuario y es utilizada para desencriptar datos encriptados con la clave pública de usuarios. La clave pública es conocida por todos los usuarios y es utilizada de tal manera que solamente un usuario puede desencriptarla.

Cliente-servidor: Programa cuya misión es obtener datos de otro programa denominado servidor, sin que ambos tengan que estar ejecutándose en el mismo ordenador. La mayoría de aplicaciones que se utilizan para acceder a Internet utilizan la tecnología cliente-servidor.

Cookies: Pequeño segmento de datos que entrega el programa servidor de HTTP al navegador WWW para que éste lo guarde. Normalmente se trata de información sobre la conexión o los datos requeridos, de esta manera puede saber qué hizo el usuario en la última visita.

Cracker: Individuo con amplios conocimientos informáticos que desprotege/piratea programas o produce daños en sistemas o redes.

D

Datagrama: Es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes.

DDL: Lenguaje de descripción de documento o de datos.

DSL: Tecnología que provee información en un gran ancho de banda a una empresa sobre líneas telefónica convencionales. xDSL se refiere a diferentes modalidades de DSL, tal como ADSL.

DES: (Algoritmo de Encriptación Estándar). Algoritmo desarrollado por IBM, utiliza bloques de datos de 64 bits y una clave de 56 bits.

DTE: (Equipo Terminal de Datos). Se refiere al ordenador conectado a un modem que recibe datos de este.

E

Encriptar: Es una medida de seguridad que permite que solamente las partes a participar en una videoconferencia o transferencia de datos estén habilitadas para hacerlo.

F

FTP (Protocolo de transferencia de Archivos): Permite la transferencia de archivos entre ordenadores y requiere de la identificación del usuario que realiza la transferencia.

Firewall: Enlace de una red que vincula solo paquetes de datos con un destino claro y autorizado para llegar a un determinado usuario protegiendo contra los "piratas".

Firma: Mensaje de correo electrónico enviado a través de internet, que indica quién ha enviado dicho mensaje y desde donde.

G

Gateway: Puerta de enlace, acceso, pasarela. Nodo en una red informática que sirve de punto de acceso a otra red. Dispositivo dedicado a intercomunicar sistemas con protocolos incompatibles. Se trata de un intermediario entre ambos para poder comunicarlos.

H

Hacker: Experto en informática capaz de de entrar en un sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

HDSL: Sistema de transmisión de datos de alta velocidad que utiliza dos pares trenzados. Se consiguen velocidades superiores al Megabit en ambos sentidos.

HPFS: Sistema de Archivos de Alto Rendimiento. Sistema que utiliza el OS/2 opcionalmente para organizar el disco duro en lugar del habitual de FAT.

HTML: Lenguaje para elaborar páginas Web.

Host name: Un conjunto de caracteres alfanuméricos que identifica de manera única una computadora dentro del domino DNS.

Hub: Provee a las workstation y otros dispositivos, un solo punto de conexión a la red.

I

ICMP: Protocolo Internet de Control de Mensajes.

Internet: Soporte de comunicación entre computadoras (net = red). Red internacional que conecta miles de redes enlazadas que utiliza protocolos TCP/IP.

IP: Protocolo de Internet. Bajo este se agrupan los protocolos de internet. También se refiere a las direcciones de red Internet.

IRTF. Internet Research Task Force. Grupo de investigadores Internet. Consta de un grupo de voluntarios que proyectan resultados y problemas a largo plazo en internet, y propone soluciones y nuevas direcciones.

ISS: Internet Security Scanner. Rastreador de Seguridad de Internet. Programa que busca puntos vulnerables de la red con relación a la seguridad.

IEEE: (Institute of Electrical and Electronics Engineers). Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana

IETF: Internet Engineering Task Force. Grupo de Tareas de Ingeniería de Internet. Asociación de técnicos que organizan las tareas de ingeniería principalmente de telecomunicaciones en Internet. Por ejemplo: mejorar protocolos o declarar obsoletos a ortos protocolos.

IPV6: En IPv6 el método propuesto se basa primordialmente en la coexistencia de ambos protocolos. Los nuevos sistemas que vayan incorporando IPv6

(computadores y routers) deberán mantener asimismo la plena capacidad de procesar paquetes IPv4.

IPV4: Utiliza un modelo de direccionamiento, de forma que a cada interface de cada dispositivo se le asigna una dirección independientemente de su dirección MAC.

K

Key(Clave): Es utilizado para encriptar datos. Un par de claves (clave pública y clave privada) están asociadas con un usuario cuando es usada en la encriptación de claves.

L

Linux: Sistema operativo Unix. Es un sistema multitarea multiusuario de 32 bits para PC.

M

MAN: (Metropolitan Área Network). Red de Área Metropolitana.

Mega: En el sistema decimal, el prefijo mega quiere decir un millón, pero en el sistema binario, el cual utilizan las computadoras, mega significa dos elevado a la veinteava potencia, o sea, la cantidad de 1.048.576. (ACR Estándard).

MIME: (Extensiones multiusos de correo de Internet). Especificaciones de Internet que permite a los usuarios enviar partes múltiples y mensajes multimedia en vez de simples mensajes de texto en Código Estándard Americano para Intercambio de Información. Una aplicación de correo electrónico compatible con MIME puede enviar imágenes PostScript, archivos binarios, mensajes de audio y video digitales a través de Internet.

Multicast: Envío de un mismo paquete a un grupo de receptores.

Multiplexar: Proceso consistente en recibir mensajes de diferentes fuentes y enviarlas a un destino común. A la inversa, la técnica de multiplexado permite enviar a puntos de destino diversos datos que proceden de una fuente común.

N

NSF: Fundación Nacional de Ciencia. Fundación americana que gestiona gran parte de los recursos de Internet.

Nodo: Punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de unión en una red.

O

OSI: Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO Divide las tareas de la red en siete niveles.

P

Password: palabra clave de acceso a un servicio u opción.

PGP: (Pretty Good Privacity). Paquete de encriptación basado en clave pública, escrito por Phil Zimmerman.

PPP: (Point to Point Protocol) Protocolo Punto a Punto. Protocolo Internet para establecer enlace entre dos puntos.

R

RDSI: Red Digital de Servicios Integrados. Red de telefónica con anchos de banda desde 64Kbps. Similar a la red telefónica de voz en cuanto a necesidades de instalación de cara al abonado, pero digital.

RSA: Rivest, Shamir Algoritmo de encriptación de clave pública desarrollado por Rivest, Shamir y Adelman.

RTC: Red Telefónica Conmutada. Red Telefónica para la transmisión de voz.

S

Secure Sockets Layer (SSL): Norma emergente sobre la seguridad en la transmisión de documentos en hipertextos a través de Internet utilizando HTTP seguro (HTTPS).

S-MIME: Abreviatura de Secure/MIME, una nueva versión del protocolo MIME que soporta codificación de mensajes. Está basado en una tecnología que usa una llave pública para interpretar el mensaje. Se espera que S/MIME sea usado ampliamente, lo cual permitirá que la gente envíe mensajes seguros a través del correo electrónico, aunque ambos usuarios estén utilizando diferente programa de e-mail.

SNMP: (Simple Network Managment Protocol): Protocolo para gestionar grandes redes. Muy utilizado por las grandes redes de Internet.

T

TCP: Por otra parte, el TCP es responsable de verificar la correcta entrega de los datos desde el cliente al servidor. Dado que la información puede perderse en el intermedio del punto de envío al punto destino.