



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería de Mecánica Eléctrica

**PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD EN LAS REDES DE
TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS**

César Augusto Menchú Tumax

Asesorado por el Ing. José Aníbal Silva de los Angeles

Guatemala, febrero de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD EN LAS REDES DE
TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CÉSAR AUGUSTO MENCHÚ TUMAX

ASESORADO POR EL ING. JOSÉ ANÍBAL SILVA DE LOS ANGELES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, FEBRERO DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADOR	Ing. Julio César Solares Pena
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

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

PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha octubre 2012.


César Augusto Menchú Tumax

Universidad De San Carlos
De Guatemala



Facultad De Ingeniería

Guatemala, 24 de octubre de 2013

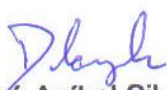
Ing. Carlos Eduardo Guzmán Salazar
Coordinador del Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ingeniero Guzmán:

Por este medio le informo que he revisado el trabajo de graduación titulado: **"Propuesta de Implementación para la Seguridad en las redes de telecomunicaciones aplicada a pequeñas y medianas empresas"**, elaborado por el estudiante César Augusto Menchú Tumax.

El mencionado trabajo llena los requisitos para dar mi aprobación, e indicarle que el autor y mi persona somos responsable por el contenido y conclusiones del mismo.

Atentamente,


Ing. José Aníbal Silva de los Angeles
Asesor

JOSÉ ANÍBAL SILVA DE LOS ANGELES
ELECTRONICO
COLEGIADO No 5067

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERIA

Ref. EIME 88. 2013
Guatemala, 5 de NOVIEMBRE 2013.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

**Me permito dar aprobación al trabajo de Graduación titulado:
PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD
EN LAS REDES DE TELECOMUNICACIONES APLICADA A
PEQUEÑAS Y MEDIANAS EMPRESAS, del estudiante César
Augusto Menchú Tumax, que cumple con los requisitos establecidos
para tal fin.**

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica



STO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERIA

REF. EIME 88. 2013.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; CÉSAR AUGUSTO MENCHÚ TUMAX titulado: PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero



GUATEMALA, 18 DE NOVIEMBRE 2,013.

Universidad de San Carlos
de Guatemala



Facultad de Ingeniería
Decanato

DTG. 046.2014

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **PROPUESTA DE IMPLEMENTACIÓN PARA LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS**, presentado por el estudiante universitario **César Augusto Menchú Tumax**, autoriza la impresión del mismo.

IMPRÍMASE:



Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, 4 de febrero de 2014

/gdech



ACTO QUE DEDICO A:

Dios

Quien es el dador de toda fuerza, inteligencia, sabiduría, gracia y conocimiento, razón principal de mi existir.

Mis padres

José Alejandro Menchú García y María Francisca Tumax Tzoc, por ser la columna de mi formación personal y académica a quienes agradeceré toda mi vida.

Mis hermanos

Apolonia, Victoria, Juan, José, Jerónima, Antonieta, Francisco, Esteban, Rosaura y Daniel Menchú Tumax, con quienes nos hemos apoyado siempre y lo seguiremos haciendo.

Mis sobrinos

Amílcar Ernesto Cua Menchú, María Maricela Cua Menchú y Fernando Alejandro Marroquín Menchú, gracias por su gran ayuda en alcanzar esta meta.

AGRADECIMIENTOS A:

La Universidad de San Carlos de Guatemala	Mi casa de estudios e incluyendo también al pueblo de Guatemala, que contribuyeron con mi desarrollo profesional así como con muchos otros.
Facultad de Ingeniería	Por ser una importante influencia en mi carrera.
Mis amigos de la Facultad	William Teletón, David Ovalle, Edy Aguilar y entre muchos otros con quienes nos apoyamos en los cursos y proyectos.
Mi asesor	Por apoyarme en mi trabajo de graduación y depositar su confianza en mi persona.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	XI
LISTA DE SÍMBOLOS	XIII
GLOSARIO	XV
RESUMEN	XXXVII
OBJETIVOS.....	XXXIX
INTRODUCCIÓN	XLI
1. FUNDAMENTOS DE REDES DE TELECOMUNICACIONES	1
1.1. Definiciones generales de las redes	1
1.1.1. Aplicaciones de las redes	1
1.2. La red y su estructura	2
1.2.1. Topologías de red	2
1.2.2. Topologías en bus y en árbol.....	3
1.2.3. Topología en anillo	4
1.2.4. Topología en estrella	5
1.3. Clasificación de redes.....	5
1.3.1. Por su dispersión	5
1.3.1.1. Redes de área local.....	7
1.3.1.2. Redes de área metropolitana.....	7
1.3.1.3. Redes de área amplia.....	8
1.3.1.4. Red global Internet.....	9
1.3.2. Por la forma de conmutación	9
1.3.2.1. Conmutación de circuitos.....	10
1.3.2.2. Conmutación de mensajes	10
1.3.2.3. Conmutación de paquetes	10

1.3.3.	Por el medio de transmisión	11
1.3.3.1.	Coaxial	11
1.3.3.2.	Par trenzado.....	12
1.3.3.3.	Fibra óptica.....	12
1.3.3.4.	Transmisión inalámbrica.....	15
1.3.4.	Por el tipo de información.....	16
1.3.4.1.	Red de telefonía fija.....	16
1.3.4.2.	Red de telefonía móvil.....	17
1.3.4.3.	Red de datos	18
1.4.	Modelo OSI	18
1.4.1.	Las capas de OSI.....	19
1.4.1.1.	Capa física	19
1.4.1.2.	Capa de enlace de datos.....	20
1.4.1.3.	Capa de red.....	20
1.4.1.4.	Capa de transporte.....	20
1.4.1.5.	Capa de sesión.....	20
1.4.1.6.	Capa de presentación	21
1.4.1.7.	Capa de aplicación	21
1.5.	Protocolos TCP/IP	21
1.5.1.	Arquitectura de protocolos TCP/IP	21
1.5.1.1.	Capa de aplicación	22
1.5.1.2.	Capa de transporte (TCP)	22
1.5.1.3.	Capa de Internet (IP)	22
1.5.1.4.	Capa de acceso a la red.....	23
1.5.1.5.	Capa física	23
1.5.2.	Funcionamiento de TCP e IP	23
1.5.3.	Interfaces de protocolo, las aplicaciones.....	24
1.5.3.1.	Protocolo sencillo de transferencia de correo (SMTP).....	24

1.5.3.2.	Protocolo de transferencia de ficheros (FTP).....	24
2.	DESCRIPCIÓN GENERAL DE SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES	25
2.1.	Planificación de la seguridad	25
2.1.1.	Ciclo de seguridad	25
2.1.2.	Activos	27
2.1.3.	Amenazas.....	28
2.1.3.1.	Amenazas a recursos físicos	29
2.1.3.2.	Amenazas a la utilización de recursos.....	30
2.1.3.3.	Amenazas a la información almacenada	30
2.1.3.4.	Amenazas a la información en tránsito.....	31
2.1.3.5.	Amenazas a la imagen y reputación....	32
2.1.3.6.	Daños a terceros	32
2.1.4.	Vulnerabilidades e impacto.....	33
2.1.5.	Identificación de riesgos	34
2.2.	Políticas generales de seguridad.....	36
2.2.1.	Qué son las políticas de seguridad redes de telecomunicaciones	36
2.2.2.	Elementos de una política de seguridad.....	37
2.2.3.	Parámetros para establecer políticas de seguridad.....	38
2.2.4.	Proposición de una forma de realizar el análisis para llevar a cabo un sistema de redes de telecomunicaciones	39

2.2.5.	La políticas de seguridad generalmente no consiguen implantarse.....	41
2.2.6.	Las políticas de seguridad como base de la administración de la seguridad integral	41
2.2.7.	Riesgos	42
2.2.8.	Niveles de trabajo.....	44
2.2.8.1.	Confidencialidad.....	44
2.2.8.2.	Integridad	44
2.2.8.3.	Autenticidad.....	45
2.2.8.4.	No – repudio.....	45
2.2.8.5.	Disponibilidad de la información.....	45
2.2.8.6.	Consistencia.....	46
2.2.8.7.	Control de acceso a los recursos	46
2.3.	Sistemas de defensa perimetral	46
2.3.1.	Defensa perimetral de sistema	47
2.3.1.1.	Interceptores TCP	47
2.3.1.2.	Interceptores de nivel de red	48
2.3.2.	Defensa perimetral de red	48
2.3.2.1.	Zonas de seguridad.....	50
2.3.2.2.	Tipos de cortafuegos.....	53
2.3.2.2.1.	Filtro de paquete	54
2.3.2.2.2.	Transparentes	55
2.3.2.2.3.	Pasarela de aplicación	57
2.3.2.2.4.	Circuitos	60
2.3.2.3.	Arquitecturas de red con cortafuegos.....	61
2.3.2.3.1.	<i>Dual homed host</i>	62
2.3.2.3.2.	<i>Screened host</i>	63

	2.3.2.3.3.	<i>Screened subnet</i>	64
	2.3.2.4.	Características avanzadas de cortafuegos	66
	2.3.2.4.1.	Traducción automática de direcciones	67
	2.3.2.4.2.	Pasarela de aplicación transparente...	67
	2.3.2.4.3.	Seguridad en los contenidos	68
2.4.		Sistemas de detección de intrusos (IDS)	69
	2.4.1.	Firmas (<i>signatures</i>)	69
	2.4.2.	Eventos de interés (EOI)	71
	2.4.3.	Sistema de prevención de intrusos (IPS)	73
	2.4.4.	<i>Firewalls</i>	77
	2.4.5.	Falsos positivos y falsos negativos	78
	2.4.6.	Limitaciones de los IDS	80
	2.4.7.	Arquitecturas de los NIDS	81
	2.4.7.1.	Marco de detección de intrusión común (<i>Common Intrusion Detection Framework</i>) (CIDF)	83
	2.4.7.2.	Distributed Intrusion Detection System (DIDS)	84
	2.4.8.	Ubicación de los NIDS	86
	2.4.9.	Protocolos de comunicación sensor-consola	88
	2.4.10.	Análisis de los datos obtenidos por sistemas NIDS	90

3.	CRIPTOLOGÍA EN SEGURIDAD DE REDES DE TELECOMUNICACIONES.....	93
3.1.	Historia.....	93
3.2.	Criptografía.....	94
3.3.	Criptoanálisis.....	95
3.4.	Criptosistema	95
3.4.1.	Transposición.....	98
3.4.2.	Cifrados mono alfabéticos.....	99
3.4.2.1.	Algoritmo de César.....	99
3.5.	Algoritmos simétricos modernos o llave privada	100
3.5.1.	Redes de Feistel	102
3.5.2.	Estándar de cifrado de datos (<i>Data Encryption Standard</i> DES).....	102
3.5.3.	<i>International data encryption algorithm</i> (IDEA).....	103
3.5.4.	<i>Blowfish</i>	104
3.5.5.	Criptoanálisis de algoritmos simétricos	104
3.6.	Algoritmos asimétricos o llave privada pública.....	105
3.6.1.	RSA.....	107
3.6.1.1.	Ataques a RSA.....	110
3.6.2.	Protocolo de acuerdo de llaves exponenciales (Diffie – Hellman).....	111
3.7.	Autenticación.....	115
3.7.1.	Funciones de dispersión unidireccionales (hash).....	115
3.7.2.	Firma digital.....	117

4.	SEGURIDAD DE VPN EN LAS REDES DE TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS...	121
4.1.	Definición de red privada virtual (VPN)	121
4.1.1.	Componentes de una VPN	123
4.1.2.	Utilizar Internet para crear una VPN	124
4.2.	Arquitectura de una VPN	126
4.2.1.	VPN de acceso remoto	126
4.2.2.	VPN de sitio a sitio	128
4.3.	Tipos de VPN	130
4.3.1.	VPN de <i>firewall</i>	131
4.3.2.	VPN de router y de concentrador	132
4.3.3.	VPN de sistema operativo	132
4.3.4.	VPN de aplicación	133
4.3.5.	VPN de proveedor de servicios	133
4.4.	Topologías de VPN	134
4.4.1.	Topología radial	135
4.4.2.	Topología de malla completa o parcial	136
4.4.3.	Topología híbrida	136
4.4.4.	Topología de acceso remoto	137
4.5.	Requerimientos de una VPN	137
4.5.1.	Autenticación de usuarios	137
4.5.2.	Control de acceso	138
4.5.3.	Administración de direcciones	139
4.5.4.	Cifrado de datos	140
4.5.5.	Administración de claves	141
4.5.6.	Ancho de banda	142
4.6.	Túnel (<i>Tunneling</i>)	143
4.6.1.	Funcionamiento del <i>tunneling</i>	143

4.6.2.	Protocolo pasajero, encapsulador y portador	145
4.6.3.	Tunneling y VPN	145
4.6.4.	Tipos de túneles	147
4.6.4.1.	Túnel voluntario	148
4.6.4.2.	Túnel obligatorio	149
4.7.	Seguridad en una VPN	151
4.7.1.	Clasificación de las amenazas a redes	153
4.7.2.	Clasificación de los ataques a redes	154
4.8.	Configuración de una VPN en un <i>firewall</i>	156
5.	IMPLEMENTACIÓN DE LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES A PEQUEÑAS Y MEDIANAS EMPRESAS	161
5.1.	Diseño de la gestión de seguridad	161
5.1.1.	Infraestructura	161
5.1.1.1.	Seguridad por capas	164
5.1.1.2.	Acceso remoto	164
5.1.2.	Comunicaciones <i>Networking</i>	165
5.1.2.1.	¿ <i>Switch o Hub</i> ?	165
5.1.2.2.	Segurización de dispositivos de red	168
5.1.3.	Almacenamiento	169
5.1.3.1.	Esquema cliente servidor	169
5.1.3.2.	Políticas de almacenamiento	170
5.1.3.3.	Redundancia	172
5.1.3.4.	Medios extraíbles	173
5.1.4.	Política de <i>Backups</i>	173
5.1.4.1.	<i>Backup</i>	174
5.1.4.2.	Consideraciones	175

5.2.	Mejores prácticas.....	176
5.2.1.	Establecer la política de seguridad de la empresa.....	176
5.2.1.1.	Conciencia a sus empleados.....	177
5.2.2.	Proteja sus equipos de escritorio y portátiles.....	178
5.2.2.1.	Protéjase de los virus y el software espía.....	178
5.2.2.2.	Actualizaciones software	179
5.2.2.3.	Configure un <i>firewall</i> para PyMES	179
5.2.2.4.	Evite el correo electrónico no deseado.....	179
5.2.2.5.	Utilice solamente software legal	180
5.2.2.6.	Navegación segura.....	180
5.2.3.	Proteja su red	181
5.2.3.1.	Utilice contraseñas seguras.....	182
5.2.3.2.	Proteger una red WIFI	182
5.2.3.3.	Configure un <i>firewall</i> a nivel de Red ..	183
5.2.4.	Proteja sus servidores	183
5.2.4.1.	Certificados de servidor	183
5.2.4.2.	Mantenga sus servidores en un lugar seguro.....	184
5.2.4.3.	Práctica de menos privilegios	184
5.2.4.4.	Conozca las opciones de seguridad.....	184
5.2.5.	Proteja sus aplicaciones y recursos.....	185
5.2.5.1.	Valore la instalación del directorio activo	185
5.2.5.2.	Gestione las aplicaciones a través del directorio activo.....	186

5.2.5.3.	Preste atención a la base de datos	186
5.2.5.4.	Cortafuegos de aplicaciones Web.....	186
5.2.5.5.	Auditorias técnicas	187
5.2.5.6.	Gestión de las actualizaciones	187
5.2.5.6.1.	Actualizaciones oportunas	187
5.2.5.6.2.	Configuraciones especiales	187
5.2.5.6.3.	Supervisión	188
CONCLUSIONES.....		189
RECOMENDACIONES.....		191
BIBLIOGRAFÍA.....		193
ANEXOS.....		195

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Topologías de red	3
2.	Ciclo de seguridad.....	26
3.	Diagrama para el análisis de un sistema de seguridad	40
4.	Cortafuegos de red con dos zonas de seguridad	51
5.	Cortafuegos de red con tres zonas de seguridad	52
6.	Tipos de cortafuegos.....	53
7.	Cortafuegos transparente.....	57
8.	Pasarela de aplicación	58
9.	Cortafuegos de circuitos.....	61
10.	Arquitectura <i>dual homed host</i>	62
11.	Arquitectura <i>Screened host</i>	64
12.	Arquitectura <i>Screened subnet</i>	66
13.	Eventos de interés (EOI)	72
14.	Ejemplo de sistema DIDS.....	85
15.	Sensores antes del <i>firewall</i>	87
16.	Sensores en el <i>firewall</i>	87
17.	Sensores antes y en el <i>firewall</i>	88
18.	Criptograma.....	94
19.	Modelo de cifrado simétrico.....	101
20.	Modelo de cifrado de clave pública	106
21.	Firma digital a) Creación b) Validación.....	119
22.	Una red virtual de VPN.....	122
23.	Componentes de una VPN.....	124

24.	El uso de internet para crear una VNP.....	125
25.	Vpn de acceso remoto	127
26.	Vpn intranet.....	129
27.	Vpn extranet.....	130
28.	Topología radial	135
29.	Topología de malla: a) completa b) parcial	136
30.	<i>Tunneling</i> en un VNP	147
31.	Túnel voluntario	149
32.	Túnel obligatorio	151
33.	El <i>firewall</i> pix de Cisco	157
34.	Topologías vpn con el <i>firewall</i> PIX	158
35.	Infraestructura	163
36.	<i>Switch</i> y <i>Hub</i>	166

TABLAS

I.	Tipos de redes por su dispersión	6
II.	Comparación de los medio en comunicaciones guiadas	14
III.	Rangos de frecuencia de la transmisión inalámbrica	15
IV.	Transposición.....	99

LISTA DE SÍMBOLOS

Símbolo	Significado
CA	Autoridad de certificación
VHF	Banda del espectro electromagnético
IC	Circuito Integrado
VC	Circuito virtual
E1	Concentrador de acceso
EFF	<i>Electronic Frontier Foundation</i>
T1	En telecomunicaciones la portadora-T
CPE	Equipo terminal del cliente
E1	Formato de transmisión digital
SHF	Frecuencia súper alta
UHF	Frecuencias Ultra Altas
Hz	Hertz, Frecuencia
hr	Hora
η	Índice de refracción
PKI	Infraestructura de Claves Públicas
IPX	Intercambio de paquetes inter red
API	Interfaces de aplicaciones
SSH	Intérprete de órdenes segura
KHz	Kilo Hertz (1000 Hertz)
k Ω	Kilo Ohmios
MHz	Mega Hertz (10000 Hertz)
mm	Milímetro
min	Minuto

ATM	Modo de Transferencia Asíncrona
NSA	<i>National Security Agency</i>
Ω	Ohm, unidad de resistencia eléctrica
XOR	Operador lógico Disyunción exclusiva
FEP	Procesador cliente
IRC	Protocolo de comunicación en tiempo
HTTP	Protocolo de transferencia de hipertexto
UDP	Protocolo del nivel de transporte
R	Resistencia
s	Segundo
NAS	Servidor de Acceso a Red
UNIX	Sistema operativo
SW	<i>Switch</i>
GND	Tierra (<i>Ground</i>)
NAT	Traducción de Dirección de Red
U	Velocidad de la luz
C	Velocidad de la luz en el vacío
V	Voltios

GLOSARIO

Acceso remoto	Conectarse a una red desde una ubicación distante.
Activos	Se considera un activo todo aquello que usa o posee una PyMES y que es susceptible de ser atacado.
Algoritmo	Es un conjunto de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos para realizar dicha actividad.
Amenaza	Es cualquier evento que puede desencadenar un incidente en las PyMES.
Ancho de banda	Es la cantidad de tráfico que fluya de forma eficiente en una red.
Antivirus	Es un software o programa que examina el contenido de los archivos en su PC en busca de indicios de virus.
Arquitectura	Es el arte de diseñar y proyectar.
Asimétricos	Es una llave pública que utiliza una doble clave conocidas como K_p (clave privada) y K_P (clave pública).

ATM	Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones, el Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM).
Autenticación	Es que un dato demuestre que viene del origen pretendido o que un usuario demuestre que es quien dice ser. Un sistema de autenticación es aquel donde un usuario se identifica ante un servidor remoto.
Autenticidad	La autenticidad garantiza que quien dice ser X es realmente X.
Backup	Se denomina <i>backup</i> o copia de seguridad a la copia de información y su almacenamiento fuera de entornos de producción.
Bastiones	Es una aplicación que se localiza en un server con el fin de ofrecer seguridad a la red interna.
BlowFish	Es algoritmo fue desarrollado para la encriptación bloques de 64 bits y permite claves de encriptación de diversas longitudes hasta 448 bits.
Bridge	Un <i>bridge</i> se utiliza cuando tenemos que conectar dos redes a nivel de capa de enlace, el dispositivo conecta dos o más segmentos de la misma LAN.

CDMA	Norma de transferencia de información por teléfonos inalámbricos, Acceso Múltiple de División de Código (<i>Code division Multiple Access</i>).
Ciclo de seguridad	Es un flujo de procesos destinados a la realización de un análisis de riesgos.
Cifrado	Es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Existen muchos algoritmos de cifrado tales como DES, 3DES, RSA, SHA-1, MD5.
Cifrar de datos	El cifrado es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas.
Confidencialidad	Es proteger la información contra la lectura no autorizada explícitamente.
Conmutación	Es establece entre los nodos de la red un camino dedicado a la interconexión de dos estaciones.
Consistencia	Se trata de asegurar que el sistema siempre se comporte de la forma esperada.
Consola	Es un sistema de detección de intrusos se encarga de recibir toda la información de los sensores de <i>pull</i> o <i>push</i> presentarla de forma entendedora al operador.

Cortafuegos	Es un equipo que se ubica interconectando dos enlaces de red, que se encarga de aplicar la configuración de seguridad al tráfico que pretende atravesarlo en ambos sentidos de la red.
Criptografía Lineal	Se basa en tomar porciones del texto cifrado y porciones de otro texto plano y efectuar operaciones sobre ellos de forma tal de obtener probabilidades de aparición de ciertas claves.
Criptografía	Es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.
Criptografía	Es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es mediante claves que sólo el emisor y el destinatario conocen.
Criptosistema	Se define como la quintupla (m, C, K, E, D) , se tiene un mensaje m , se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m .
Criticidad	Indica que no todos los ordenadores tienen la misma función de esta forma un ataque a un servidor DNS, a un <i>firewall</i> o a un PC Cliente se valoran de distinta forma.

<i>Deceptive applications</i>	Se basa en una aproximación diferente y más proactiva frente a la detección de intrusos.
Defensa perimetral	Es un conjunto de filtros que restringen el acceso de las peticiones entrantes antes de que lleguen en los servicios internos de la organización de Pymes.
DES	Estándar de Cifrado de Datos (<i>Data Encryption Standard</i>) es el algoritmo simétrico más extendido mundialmente.
DIDS	Es el centro del sistema.
Diferencial	Es un Criptoanálisis Diferencial se basa en el estudio de dos textos codificados para estudiar las diferencias entre ambos mientras se los está codificando.
Diffie-Hellman	Es un protocolo que también llamado (protocolo de acuerdo de llaves exponenciales), permite a dos usuarios intercambiar una llave secreta sobre un medio inseguro sin tener acuerdos preestablecidos.
Disponibilidad	Es la disponibilidad de la información, se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

DNS	Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
DOS	Es un <i>disk operating system</i> (sistema operativo de disco).
<i>Dual homed host</i>	Es una arquitectura más simple y barata consiste en incluir los tres elementos en un solo equipo.
Encapsulación	Es un método de diseño modular de protocolos de comunicación en el cual las funciones lógicas de una red son abstraídas ocultando información.
Eventos de interés	Definiremos los eventos de interés (<i>Events Of Onterest, EOI</i>) como el subconjunto mínimo de muestras que debemos analizar para considerar nuestra red segura.
Extranet	Es una intranet orientada a las personas u organizaciones que son externas a su empresa, pero necesitan acceder a alguna información, así se les permite el acceso a este contenido adicional, siempre bajo un sistema de autenticación y control de acceso.
Falso negativo	Es un término que hace referencia a un fallo en el sistema de alerta.

Falso positivo	Es un término aplicado a un fallo de detección en un sistema de alertas usualmente en sistemas antivirus o de detección de intrusos.
Fibra óptica	Es un medio de transmisión empleado habitualmente en redes de datos.
<i>Firewall</i>	Es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes. Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso.
Firma Digital	Una firma digital es utilizada con las claves públicas y se trata de un medio por el que los autores de un mensaje, archivo u otro tipo de información codificada digitalmente enlazan su identidad a la información.
Firma	Una firma (<i>signature</i>) es aquello que define o describe un patrón de interés en el tráfico de nuestra red.
FTP	Protocolo de Transferencia de Ficheros que permite el envío y recepción de ficheros de cualquier tipo de o hacia un usuario.

Fuerza bruta	Consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga un mensaje legible de texto nativo.
<i>full-duplex</i>	Es una transmisión que se propaga a través del medio en ambos sentidos.
<i>Gateway</i>	Es una pasarela o puerta de enlace, que es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.
GSM	Es un sistema de teléfono móvil digital más utilizado y el estándar de facto para teléfonos móviles, con las siglas de <i>Global System for Mobile communications</i> (Sistema Global para las comunicaciones Móviles).
<i>Hacker</i>	Es el que intenta acceder a los sistemas sin permiso, sobre todo para demostrar a sí mismo qué es capaz de superar las barreras de protección que se hayan establecido.
Hardware	Se refiere a todas las partes tangibles de un sistema informático o la parte física de una red.
<i>Hash</i>	Son funciones de dispersión unidireccionales (<i>one-way hash function</i>) son muy utilizadas para la autenticación de datos.

Heterogeneidad	La Heterogeneidad de equipos en un entorno compuesto por múltiples sistemas de red, éstos pueden ser heterogéneos desde el punto de vista de su arquitectura hardware y software con distintos sistemas de red.
https	Es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW generalmente para transacciones de pagos o cada vez que se intercambie información sensible.
Hub	Es un dispositivo de red que permite conectar varios equipos (según su capacidad) y que retransmite los paquetes recibidos en todos sus puestos, menos en el que recibió los datos.
Hybrid switches	Es un sistemas de prevención de intrusos se basan en combinar una parte de software y otra de hardware.
IDEA	El International Data <i>Encryption</i> Algorithm fue desarrollado en Alemania trabaja con bloques de 64 bits de longitud empleando una clave de 128 bits.
IDS	Sistemas de detección de intrusos o IDS (<i>Intrusion Detection System</i>).

IEEE	Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnica profesional mundial dedicada a la estandarización.
<i>Inline IPS</i>	Es sistemas de prevención de intrusos se caracterizan por colocarse entre la red y el ordenador a proteger.
Integridad	Es proteger la información contra la modificación sin el permiso del dueño.
Interceptores	Es un filtro que se ubican entre el nivel de transporte y el nivel de aplicación y que capturan la petición justo antes de ser atendida por el servidor.
IPS	Es un sistema de prevención de intrusos como un dispositivo hardware o software que tiene la habilidad de detectar ataques tanto conocidos como desconocidos y reaccionar a esos para impedir su éxito.
IPSec	Es un conjunto de protocolos (<i>Internet Protocol security</i>), cuya función es asegurar las comunicaciones sobren el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos.

ISP	Internet <i>Service Provider</i> (Proveedor de Servicios de Internet), es una organización que proporciona servicios de Internet a empresas y particulares.
L2F	Es un protocolo L2F (<i>Layer 2 Forwarding</i>) que se creó en las primeras etapas del desarrollo de las red privada virtual.
L2TP	Protocolo de Túnel de Capa 2.
LAN	Una red de área local.
Letalidad	Son los diferentes ataques (<i>exploits</i>) no tienen siempre el mismo objetivo.
Linux	Es un núcleo libre de sistema operativo, es uno de los principales ejemplos de software libre y de código abierto.
Login	Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario.
Mail	Es un servicio de red que permite a los usuarios enviar y recibir mensajes, que es un correo electrónico.

MANs	Las redes de servicio de televisión por cable, en general a cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros.
Mbps	Es una unidad que se usa para cuantificar un caudal de datos.
MBSA	Es una herramienta fácil de usar diseñada para ayuda a las pequeñas y medianas empresas a determinar su estado de seguridad según las recomendaciones de seguridad de Microsoft, (Microsoft <i>Baseline Security Analyzer</i>).
MD5	Es un algoritmo de dispersión que autentica los datos de los paquetes, (MD5, Message Digest version 5).
Microondas	Se denomina las ondas electromagnéticas definidas en un rango de frecuencias determinado.
MP3	Es un formato de compresión de audio digital.
Multiplexado	Consiste en transportar la señal por un mismo medio físico, Una de las técnicas de multiplexado óptico actuales se conoce como WDM (<i>Wavelength Division Multiplexing</i>).

Multiplicidad de equipo	Una solución de cortafuegos personales sólo es viable desde un punto de vista de administración y mantenimiento cuando el número de sistemas a gestionar es pequeño.
<i>Netware de Novell</i>	Es un sistema operativo, es una de las plataformas de servicio para ofrecer acceso a la red y los recursos de información.
NIDS	Sistema de detección de intrusos en una Red, busca detectar anomalías tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador.
OSI	Conjunto de protocolos diseñados por comités ISO con el objetivo de convertirlos en estándares internacionales de arquitectura de redes de ordenadores.
<i>Password</i>	Es una contraseña o clave que se utiliza para la autenticación de acceso hacia algún recurso de una organización.
Permisividad máxima	En los <i>firewalls</i> dónde el uso de filtros es mínimo o inexistente en las redes de telecomunicaciones.
Permisividad mínima	En los <i>firewalls</i> en este caso se deniega acceso a todos los servicios de la red y se van permitiendo accesos a estos a medida que se necesiten.

PPP	Es un protocolo que proporciona conexiones fiables de <i>router a router</i> y de <i>host a red</i> . PPP es el protocolo WAN más utilizado y conocido y funciona en la capa 2 del modelo OSI.
PPTP	Protocolo de Túnel punto a punto.
Protocolo	Es un conjunto de reglas que definen cómo interactúan las entidades de comunicación. Para que una computadora se pueda comunicar con otra se requieren de varios protocolos los cuales van a definir las reglas de la comunicación.
Proxy	Es una pasarela de aplicación la funcionalidad de cortafuegos se realiza a nivel de aplicación en un conjunto de servidores.
Pull	Es cuando almacenan los eventos de interés hasta que la consola pregunta por ellos al sensor.
Push	Es cuando se detecta un evento de interés el sensor crea un paquete de datos que se envía a la consola.
RADIUS	Es un Servicio de Usuario de Marcación para Autenticación Remota es un estándar para un sistema de autenticación de acceso remoto, (<i>RADIUS, Remote Authentication Dial In User Service</i>).

RAID	Es una tecnología que permite almacenar información en múltiples discos duros y disponer de ella de manera redundante. (<i>Redundant Array of Independent Disks</i> , en español Conjunto Redundante de Discos Independientes).
Red privada	Es aquella red exclusiva de una sola compañía u organización en particular, la información no se comparte con otras compañías u organizaciones.
Red pública	Es una red a través de la cual circula información de muchas compañías y organizaciones. Una red pública siempre será menos segura que una red privada, pero resultan ser más económicas.
Redes de bots	Las denominadas redes de bots (<i>botnets</i>) que se esparcen accediendo a sistemas informáticos sin las adecuadas medidas de seguridad y desde ellos realizando diversas acciones.
Redes de feistel	Este algoritmo se basa en dividir un bloque de longitud n (generalmente el texto a cifrar) en dos mitades, L y R .
Router	Es un equipo que direcciona los paquetes de datos de una red a otra. Este dispositivo puede determinar cuál es la ruta más corta de un paquete hacia su destino.

RSA	Es un sistema de cifrado de llaves públicas que se usa tanto para cifrado de datos como para autenticación de llaves públicas.
<i>Screened host</i>	Es la combina las funcionalidades de cortafuegos y de router de acceso, separando los bastiones en máquinas independientes que deberán ser declaradas explícitamente en la configuración de seguridad.
<i>Screened subnet</i>	Es la separación de las tres funcionalidades necesarias en tres máquinas distintas, una para el <i>router</i> , otra para el cortafuegos y otra para el bastión que alberga los servicios.
Seguridad por capas	Es una seguridad que consiste en organizar las medidas de seguridad en diferentes niveles, garantizando que si resultara comprometido un nivel, el intruso o atacante deberá traspasar otra capa de seguridad para vulnerar los sistemas de la red.
Sensores	Son elementos pasivos que examinan todo el tráfico de su segmento de red en búsqueda de eventos de interés.
SHA-1	Es un algoritmo que toma como entrada un mensaje con una longitud máxima de 264 bits y produce un resumen del mensaje (hash) de 160 bits, (<i>SHA-1, Security Hash Algorithm</i>).

Simétricos	Es una clave privada, que se utiliza la misma clave K para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave.
Sistema operativo red	Es un sistema operativo especialmente diseñado para la configuración y administración de redes. Un sistema operativo de red se instala en aquellas computadoras que van a operar como servidores.
SLA	Son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba, (SLA, <i>Service Level Agreements</i>).
SLIP	Es un protocolo SLIP (<i>Serial Line Internet Protocol</i>), que es un estándar de transmisión de datagramas IP.
SMTP	Es un protocolo de servicio de correo electrónico.
SNMP	Es un protocolo que permite a los administradores de red administrar dispositivos de red y diagnosticar problemas en la red, que significa Protocolo simple de administración de red.
Software	Es la parte lógico o soporte lógico de un sistema informático son todos los programas.

<i>Spoofing</i>	Es un ataque que se basa en el uso de las direcciones IP.
SSID	Identificador de redes inalámbricas.
<i>Switch</i>	Es un dispositivo de interconexión de equipos en red que retransmite los paquetes de acuerdo a la dirección de la placa de red (MAC) de destino leída en la trama del paquete de datos.
TCP/IPI	Es un conjunto de protocolos que permiten la comunicación a través de varias redes diferentes y el cual constituye la base del funcionamiento de Internet.
TCPQUAD	Es un formato que realiza una reducción compacta de la información contenida en los paquetes IP que se basa en almacenar una cuádruple tupla que contiene los siguientes campos (Fecha, Dirección origen, Dirección de destino, Tipo de protocolo).
TELNET	Es un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
TETRA	Son unos estándares <i>Tetrapol</i> y <i>Terrestrial Trunked RAdio</i> (TETRA) que se utiliza en la telefónica en el ámbito privado y de servicios de emergencias como policía, bomberos y servicios de ambulancias.

Topología de red	Se una diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico.
Tráfico	Es la cantidad de datos enviados y recibidos que pasa por un red.
Transposición	Son aquellos que alteran el orden de los caracteres dentro del mensaje a cifrar.
<i>Tunneling</i>	Es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Algunos protocolos que usan esta tecnología son PPTP y L2TP.
UMTS	Estándar que se empleará en la llamada tercera generación de telefonía móvil, que permitirá disponer de banda ancha en telefonía móvil y transmitir un volumen de datos importante por la red. (<i>Universal Mobile Telecommunications System</i>).
USB	Universal Serial Bus.
Usmeador o sniffer	Es un programa el cual puede leer todos los paquetes que circulan por una red con lo que se puede tener acceso a información privada.

VPN dial-up	En esta VPN el usuario realiza una llamada local al ISP utilizando un módem.
VPN directa	En esta VPN se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP.
VPN extranet	Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, se pueden implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones.
VPN intranet	Se utilizan para la comunicación interna de una organización, enlazan una oficina central con todas sus sucursales se disfrutan de las mismas normas que en cualquier red privada.
VPN	Es una red privada virtual que utiliza la infraestructura de una red pública para poder transmitir información, (VPN, <i>Virtual Private Network</i>).
Vulnerabilidad	Son puntos débiles de un software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo.

WAN	Es aquella red que está formada por la interconexión de varias LAN. Una WAN abarca una gran área geográfica de varios kilómetros.
wap	<i>Wireless Application Protocol</i> o WAP (protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas.
WAV	Es un formato de audio digital normalmente sin compresión de datos.
Web	Es una red informática mundial que es un sistema de distribución de documentos de hipertexto interconectados y accesibles vía Internet.
WEP	Es un protocolo de encriptación introducido en el primer estándar IEEE 802.11.
WEPSe	Es un cifrado basa en claves de 64 ó 128 bits.
Wi-Fi	Es una forma de conexión a internet por medio del aire sin utilizar cable.
Windows de Microsoft	Es un sistema operativo.
Zonificación	Es la definición de una zona de seguridad interna en todas las redes de una organización de Pymes y el resto de Internet es una zona externo.

RESUMEN

El presente trabajo de graduación es una propuesta de implementación de la seguridad en las redes de telecomunicaciones aplicada a pequeñas y medianas empresas.

El capítulo uno es sobre los fundamentos de redes de telecomunicaciones en su estructura, clasificación de redes, modelo OSI y protocolos TCP/IP.

El capítulo dos es la descripción general de la seguridad en las redes de telecomunicaciones en la planificación de la seguridad, políticas generales de seguridad, sistemas de defensa perimetral y sistemas de detección de intrusos (IDS).

El capítulo tres se describe la criptología en la seguridad redes de telecomunicaciones en el criptoanálisis, algoritmos simétricos modernos o llave privada, algoritmos asimétricos o llave privada pública y la autenticación.

El capítulo cuatro se describe la seguridad de VPN en las redes de telecomunicaciones aplicadas a pequeñas y medianas empresas en la definición de red privada virtual, arquitectura, topologías de VPN, túnel (*Tunneling*) y la seguridad en una VPN.

El capítulo cinco es la implementación de la seguridad en las redes de telecomunicaciones aplicadas pequeñas y medianas empresas en el diseño de la gestión de seguridad, en la infraestructura y mejores prácticas de proteja sus aplicaciones y recursos.

OBJETIVOS

General

Realizar una propuesta de implementación para la seguridad en las redes de telecomunicaciones aplicada a pequeñas y medianas empresas.

Específicos

1. Presentar los fundamentos de las redes de telecomunicaciones.
2. Hacer una descripción general de la seguridad en las redes de telecomunicaciones.
3. Presentar los fundamentos de criptología en la seguridad las redes de telecomunicaciones.
4. Presentar la seguridad de VPN en las redes de telecomunicaciones aplicada a Pequeñas y Medianas Empresas (PyMES).
5. Implementar la seguridad en las redes de telecomunicaciones a Pequeñas y Medianas Empresas (PyMES).

INTRODUCCIÓN

El desarrollo de las redes de telecomunicaciones en las pequeñas y medianas empresas ha pasado a ser la herramienta de mayor importancia para el procesamiento y comunicación de datos compartidos, las redes de las pequeñas y medianas empresas posibilitan al personal a compartir recursos y a comunicarse unos con otros de forma eficiente, la red está diseñado para ser amigable con el usuario y existen muchos componentes muy flexibles en la red desafortunadamente este ha hecho llevar a situaciones donde la red de las pequeñas y medianas empresas están configuradas con control o planeamiento centralizado. Esto usualmente resulta en una pérdida o en algunas instancias la falta total de consideración de la seguridad en la red de las pequeñas y medianas empresas.

La seguridad en las redes de telecomunicaciones de las pequeñas y medianas empresas es una parte integral del sistema de red completo y debe ser importante para todos los usuarios, existen herramientas tales como la planificación de la seguridad, políticas de seguridad, la defensa perimetral, sistemas de detección de intrusos, la red privada virtual, encriptación, firmas digitales y códigos de autenticación de mensajes que son muy útiles para garantizar la confidencialidad, integridad y disponibilidad de la información, de la propias red de las pequeñas y medianas empresas.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE Institute of Electrical and Electronic Engineers) definieron las redes de telecomunicaciones de las pequeñas y medianas empresas como un sistema de comunicación de datos que permite a un número de dispositivos independientes comunicarse

directamente entre ellos, dentro de un área geográfica de un tamaño moderado a través de un canal de comunicación físico con una tasa de transmisión también moderada. Las redes de telecomunicación de las pequeñas y medianas empresas usualmente usan una red común conecta servidores, estaciones de trabajo, impresoras y dispositivos de almacenamiento secundario, permitiendo a los usuarios compartir los recursos y la funcionalidad la red.

1. FUNDAMENTOS DE REDES DE TELECOMUNICACIONES

1.1. Definiciones generales de las redes

Las redes de comunicaciones ha tenido un gran avance en los últimos años, debido a diversos hechos tales como el uso generalizado de los protocolos de internet, lo cual ha posibilitado la difusión de servicios como correo electrónico y acceso a web; la apertura de la industria a nuevas tecnologías que han conducido a un sistema muy flexible de transmisión de información basado en intercambio de paquetes; y la tecnología de comunicaciones ópticas que ha dado lugar a un incremento en los anchos de banda para las comunicaciones.

Otra área de las redes de comunicaciones que también ha tenido avances increíbles son los servicios de voz, principalmente la telefonía móvil, la cual ha tenido un crecimiento global impresionante en nuestro país en los últimos años. La clave del éxito de las redes de las comunicaciones es la necesidad básica de todo ser humano de estar en comunicación con otras personas.

1.1.1. Aplicaciones de las redes

Existe una infinidad de aplicaciones para las redes de comunicaciones dependiendo del servicio que presten. Por ejemplo las aplicaciones de una red de computadores (datos) tiene tres aplicaciones principales: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación de valor añadido.

En redes de telefonía móvil, debida a la amplia cobertura de señal dentro de un área y ser inalámbrica, brindan una variedad de aplicaciones de transmisión de datos sin necesidad de tener una red física instalada y limitada a un área. Esto brinda la posibilidad de transmitir audio, datos e imágenes de una forma segura y práctica. Todas estas aplicaciones operan sobre redes por razones económicas pues resulta mucho más económico el intercambio de un documento digitalmente a través de una red que el intercambio del mismo a través de medios de transporte terrestre, marino o aéreo y al final el contenido de la información es exactamente el mismo.

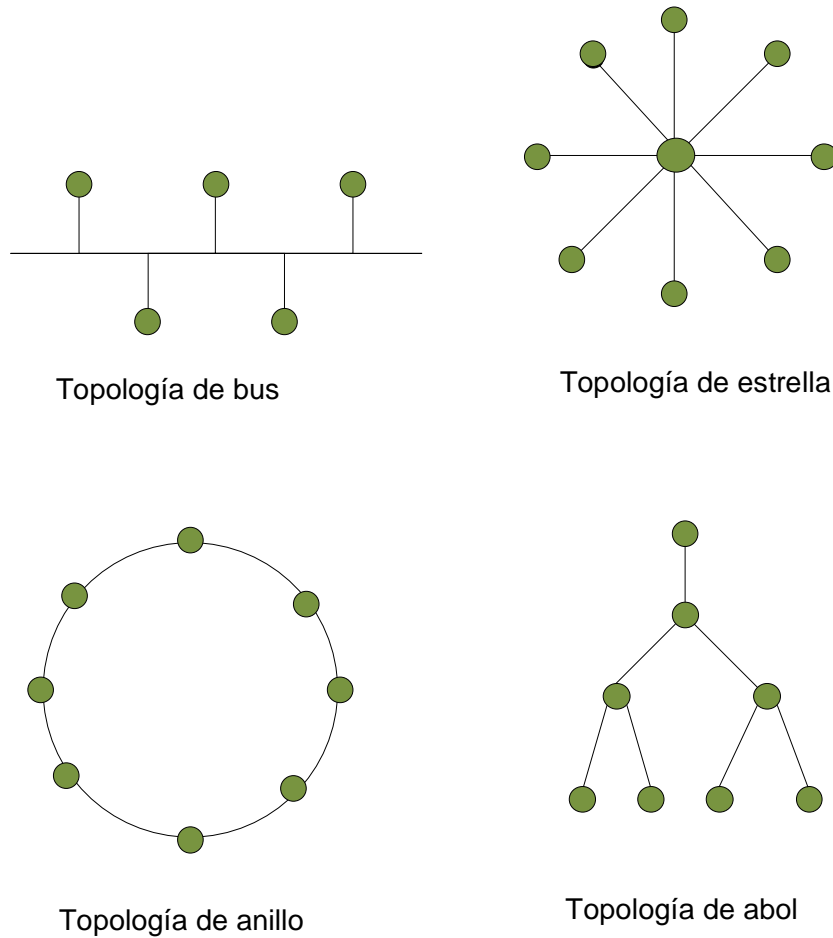
1.2. La red y su estructura

La estructura de una red queda perfectamente definida cuando se conocen la naturaleza de sus elementos, la topología de sus nodos, las reglas de encaminamiento, el dimensionado de sus elementos y el enrutamiento de sus vías.

1.2.1. Topologías de red

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son: bus, árbol, anillo y estrella, como se muestra en la figura 1.

Figura 1. **Topologías de red**



Fuente: elaboración propia en Microsoft Visio.

1.2.2. **Topologías en bus y en árbol**

El bus es un caso especial de la topología en árbol, con un solo tronco y sin ramas. Ambas topologías se caracterizan por el uso de un medio multipunto en el caso de la topología en bus, todas las estaciones se encuentran directamente conectadas, a través de interfaces físicas apropiadas conocidas como tomas de conexión (*taps*), a un medio de transmisión lineal o bus. El

funcionamiento *full-duplex* entre la estación y la toma de conexión permite la transmisión de datos a través del bus y la recepción de éstos desde aquél. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de estaciones.

La topología en árbol es una generalización de la topología en bus. El medio de transmisión es un cable ramificado sin bucles cerrados, que comienza en un punto conocido como raíz o cabecera (*headend*). Uno o más cables comienzan en un punto raíz, y cada uno de ellos puede presentar ramificaciones. Las ramas pueden disponer de ramas adicionales, dando lugar a esquemas más complejos. De nuevo, la transmisión desde una estación se propaga a través del medio y puede alcanzar al resto de estaciones.

1.2.3. Topología en anillo

En la topología en anillo, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un bucle cerrado. El repetidor es un dispositivo relativamente simple, capaz de recibir datos a través del enlace y de transmitirlos, bit a bit, a través del otro enlace tan rápido como son recibidos.

Los enlaces son unidireccionales; es decir, los datos se transmiten sólo en un sentido, de modo que éstos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario. Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él. Como en el caso de las topologías en bus y en árbol, los datos se transmiten en tramas. Una trama que circula por el anillo pasa por las demás estaciones, de modo que la estación de destino reconoce su dirección y copia la trama, mientras ésta la atraviesa, en una memoria temporal local. La trama continúa circulando hasta que alcanza de nuevo la estación origen, donde es eliminada del medio.

1.2.4. Topología en estrella

En redes con topología en estrella cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, una para la transmisión y otro para la recepción. En general existen dos alternativas para el funcionamiento del nodo central. Una es el funcionamiento en modo de difusión, en el que la transmisión de una trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central aunque la disposición física es una estrella, lógicamente funciona como un bus; una transmisión desde cualquier estación es recibida por el resto de estaciones, y sólo puede transmitir una estación en un instante dado.

Otra aproximación es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena en el nodo y se retransmite sobre un enlace de salida hacia la estación destino.

1.3. Clasificación de redes

Las redes se clasifican por su tamaño, es decir la extensión física en que se ubican sus componentes, desde un aula hasta una ciudad, un país o incluso el planeta. Dicha clasificación determinará los medios físicos y protocolos requeridos para su operación.

1.3.1. Por su dispersión

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor se le llama nivel físico y al segundo protocolos.

En el nivel físico generalmente se encuentran señales de voltaje que tienen un significado preconcebido. Esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma como se accedan esos paquetes determina la tecnología de transmisión y se aceptan dos tipos:

- *Broadcast*
- *point-to-point*

Las redes de tipo *broadcast* se caracterizan porque todos los miembros (nodos) pueden acceder todos los paquetes que circulan por el medio de transmisión. Las redes punto a punto sólo permiten que un nodo se conecte a otro en un momento dado.

Por la extensión de las redes *broadcast* o punto a punto, se pueden clasificarlas de acuerdo a la tabla siguiente.

Tabla I. **Tipos de redes por su dispersión**

Distancia/CPU'S	Ubicación de CPU's	Nombre
0,1Mts.	Tarjeta Madre	NODO
1 Mts.	Cluster, Sistema	Multicomputador
10 Mts.	Sala de Computo	LAN
100 Mts.	Edificio	LAN
1 KM.	Campus	LAN
10 Km.	Ciudad	MAN
100 Km.	Estado, País	WAN
1000 Km.	Continente	WAN
10,000 Km	Planeta	INTERNET

Fuente: elaboración propia, con programa Microsoft Excel.

1.3.1.1. Redes de área local

Las redes de área local son el punto de contacto de los usuarios finales. Su finalidad principal es la de intercambiar información entre grupos de trabajo y compartir recursos tales como impresoras y discos duros. Su extensión va de unos cuantos metros hasta algunos kilómetros. Esto permite unir nodos que se encuentran en una misma sala de cómputo, en un edificio, en un campus o una empresa mediana y grande ubicada en una misma locación.

Las redes tradicionales operan con medios de transmisión tales como cable de par trenzado (*Unshielded Twisted Pair*), cable coaxial ya casi obsoleto porque presenta muchos problemas, fibra óptica es inmune a la mayoría de interferencias, portadoras de rayo infrarrojo o láser, radio y microondas en frecuencias no comerciales. Las velocidades en las redes de área local van desde 10 Megabits por segundo (Mbps) hasta 622 Mbps.

1.3.1.2. Redes de área metropolitana

Una red de área metropolitana es una versión más grande de una LAN en cuanto a topología, protocolos y medios de transmisión que abarca tal vez a un conjunto de oficinas corporativas o empresas en una ciudad. Las redes deservicio de televisión por cable se pueden considerar como MANs y, en general, a cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros. El estándar IEEE 802.6 define un tipo de MAN llamado DQDB por sus siglas en inglés *Distributed Queue Dual Bus*. Este estándar usa dos cables half-duplex por los cuales se recibe y transmiten voz y datos entre un conjunto de nodos.

1.3.1.3. Redes de área amplia

Una red de área amplia se expande en una zona geográfica de un país o continente. Los beneficiarios de estas redes son los que se ubican en nodos finales llamados también sistemas finales que corren aplicaciones de usuario. A la infraestructura que une los nodos de usuarios se le llama subred y abarca diversos aparatos de red (denominados en general como routers o enrutadores) y líneas de comunicación que une a las redes de área local.

En la mayoría de las redes de área amplia se utilizan una gran variedad de medios de transmisión para cubrir grandes distancias. La transmisión puede efectuarse por microondas, por cable de cobre, fibra óptica. Sin importar el medio, los datos en algún punto se convierten e interpretan como una secuencia de unos y ceros para formar marcos de información (*frames*), luego estos frames son ensamblados para formar paquetes y los paquetes a su vez construyen archivos o registros específicos de alguna aplicación.

Las redes clásicas se caracterizan porque utilizan routers para unir las diferentes LANs. Como en este caso los paquetes viajan de LAN en LAN a través de ciertas rutas que los *routers* establecen, siendo dichos paquetes almacenados temporalmente en cada *router*, a la subred que usa este principio se le conoce como punto-a-punto, almacena y envía o de enrutado de paquetes (*point to point, store and forward, packet switched*).

Las topologías comunes en una red punto a punto son: de estrella, anillo, árbol, completa, anillo intersecado e irregular. La posibilidad de usar el aire como medio de transmisión da lugar a las redes inalámbricas. Se pueden construir usando estaciones de radio o satélites que envían ondas a diferentes frecuencias para enlazar los correspondientes enrutadores. Como el alcance de

estas ondas no puede ser restringido en un cierto radio, se deben tomar algunas medidas especiales para no entrar en conflicto con otras ondas y para restringir el acceso.

1.3.1.4. Red global Internet

La red Internet es aquella que se ha derivado de un proyecto del departamento de defensa de Estados Unidos y que ahora es accesible en todo el mundo y cuyos servicios típicos son las conexiones con emulación de terminal telnet, la transferencia de archivos ftp, el WWW, el correo electrónico.

Por otro lado, se consideran como internets (con la letra i minúscula) a aquellas redes públicas o privadas que se expanden por todo el mundo. El asunto interesante es que estas internets pueden valerse del Internet en algunos tramos para cubrir el mundo. La restricción mayor para que una red privada se expanda en el mundo usando Internet es que puede verse atacada por usuarios del Internet. Un esquema de seguridad para este caso puede ser que, para las LANs que conforman la internet privada, cada una de ellas encripte su información antes de introducirla a Internet y se decodifique en las LANs destinos, previo intercambio de las claves o llaves de decodificación. Este tipo de esquemas se pueden lograr con el uso de *firewalls*.

1.3.2. Por la forma de conmutación

En las redes de telecomunicaciones, es la forma de establecer un camino entre 2 puntos, un transmisor y un receptor a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

1.3.2.1. Conmutación de circuitos

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino tan rápido como se pueda. En cada nodo, los datos se encaminan o conmutan por el canal apropiado de salida sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red telefónica.

1.3.2.2. Conmutación de mensajes

Método de transmisión de mensajes a través de una red de comunicación, en la que en cualquier tiempo en particular, no es necesaria una conexión completa ya que el mensaje es enviado al centro de conmutación más próximo y es almacenado en su búfer esperando hasta que la línea al siguiente centro de conmutación no esté siendo utilizada o no esté siendo utilizado por mensajes con mayor prioridad, y así sucesivamente hasta llegar a su punto de destino.

1.3.2.3. Conmutación de paquetes

En conmutación de paquetes, no es necesario hacer una reserva por prioridades de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y el destino. En cada nodo, el paquete se recibe completamente, se almacena durante un intervalo breve y posteriormente se transmite al siguiente nodo. Las redes de conmutación de

paquetes se usan fundamentalmente para comunicaciones terminal computador.

1.3.3. Por el medio de transmisión

Los medios de transmisión son el componente básico de toda red de telecomunicaciones. Existen diferentes tipos. La elección de uno respecto a otro depende del ancho de banda necesario, las distancias existentes y el costo, cada medio de transmisión tiene sus ventajas e inconvenientes; no existe un tipo ideal.

Las principales diferencias entre los distintos tipos radican en la anchura de banda permitida y consecuentemente en el rendimiento máximo de transmisión, su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la amortiguación de la señal y la distancia recorrida.

1.3.3.1. Coaxial

Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas. Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive.

1.3.3.2. Par trenzado

Es el tipo de cable más común y se originó como solución para conectar teléfonos, terminales y ordenadores sobre el mismo cableado. Cada cable de este tipo está compuesto por una serie de pares de cables trenzados. Los pares se trenzan para reducir la interferencia entre pares adyacentes. Normalmente una serie de pares se agrupan en una única funda de color codificado para reducir el número de cables físicos que se introducen en un conducto.

El número de pares por cable son 4, 25, 50, 100, 200 y 300. Cuando el número de pares es superior a 4 se le llama cables multipar.

1.3.3.3. Fibra óptica

La forma en que la fibra óptica ha ganado terreno en el área de las telecomunicaciones, esto debido a la capacidad de transmitir grandes cantidades de información con mínimas pérdidas o requerimientos de potencia. Las fibras ópticas son guías de luz que tienen el grosor de un cabello humano, y poseen la capacidad de transmitir a grandes distancias, por su característica de mínima pérdida de potencia durante la transmisión de una señal, transportan la información por medio de ondas luminosas y no mediante electricidad, lo que evita la interferencia de ruido eléctrico y degradación de la señal.

La fibra óptica es un filamento de plástico o cristal de alta pureza constituido por dos cilindros concéntricos con índices de refracción distintos; siendo el índice de refracción la relación entre la velocidad de la luz en el vacío y la velocidad de la luz en otro medio, dicho índice de refracción es una propiedad característica de cada medio.

Ecuación de índice de refracción

$$\eta = \frac{C}{U}$$

Donde:

N = índice de refracción

C = velocidad de la luz en el vacío

U = velocidad de la luz

Las fibras ópticas han sustituido completamente a los cables coaxiales que a diferencia de las fibras, transportan electricidad por un alambre de cobre rígido como núcleo, rodeado por varias capas de materiales como lo son un dieléctrico, una malla metálica y finalmente un material plástico que sirve de protección.

Para aumentar la cantidad de información transportada en las fibras ópticas esto es el aumento del caudal, se usan la técnica de multiplexado y de conmutación. El multiplexado consiste en transportar por un mismo medio físico. La conmutación es una operación de direccionamiento a nivel de la red global, por lo que cada destinatario recibe al final de la línea, la información que se le envía. Una de las técnicas de multiplexado óptico actuales se conoce como WDM (*Wavelength Division Multiplexing*), que consiste en enviar varias señales luminosas de diferentes longitudes de onda, simultáneamente por la misma fibra.

La técnica de multiplexación densa en longitud de onda DWDM (*Dense Wave Division Multiplexing*) se basa en la existencia de ciertos rayos láser que

disparan bandas múltiples de luz a través de una sola fibra óptica, cada banda de luz tiene su propio color (longitud de onda) diferente a las demás.

La diferencia entre las redes de comunicaciones basadas en cobre y las redes diseñadas con cables de fibra óptica son enormes. Si con el cobre se pueden transmitir 14 mil 400 conversaciones telefónicas a la vez, la fibra óptica permite, simultáneamente, hasta tres millones y medio de llamadas sin interferencias eléctricas ni de radio. Sin embargo, a pesar de estas múltiples ventajas, la penetración del cable de fibra óptica en última milla es todavía muy escasa, ya que hace falta desplegar una infraestructura que requiere tiempo e importantes inversiones, las cuales no se recuperarán rápidamente, lo que hace que muchas empresas del ramo, no se decidan a invertir en estos cambios tecnológicos.

Tabla II. **Comparación de los medio en comunicaciones guiadas**

	UTP	STP	COAXIAL	FIBRA OPTICA
Tecnología ampliamente	Si	Si	Si	Si
Ancho de banda	Medio	Medio	Alto	Muy alto
Hasta 1 Mhz.	Si	Si	Si	Si
Hasta 10 Mhz.	Si	Si	Si	Si
Hasta 20 Mhz.	Si	Si	Si	Si
Hasta 100 Mhz.	Si	Si	Si	Si
Canales de video	No	No	Si	Si
Canal Full Dúplex	Si	Si	Si	Si
distancias	100 m	100 m	500	2 km (Multimodo)
Medias	65 Mhz	67 Mhz	(Ethetnet)	100 km (Monomodo)
Inmunidad Electromagnetica	Limitada	Media	Media	Alta
seguridad	Baja	Baja	Media	Alta
Costo	Bajo	Medio	Medio	Alto

Fuente: elaboración propia, con programa Microsoft Excel.

1.3.3.4. Transmisión inalámbrica

La transmisión como la recepción se lleva a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional la antena de transmisión emite toda la energía concentrándola en un haz que es emitido en una cierta dirección, por lo que tanto las antenas el emisor como el receptor deben estar perfectamente alineados. En el método omnidireccional la antena emite la radiación de la energía dispersadamente (en múltiples direcciones), por lo que varias antenas pueden captarla.

Cuanto mayor es la frecuencia de la señal a transmitir más factible es confinar la energía en un haz direccional (la transmisión unidireccional). En el estudio de las comunicaciones inalámbricas, se van a considerar tres rangos de frecuencias.

Tabla III. **Rangos de frecuencia de la transmisión inalámbrica**

Trasmisión Inalámbrica	Banda
Radio frecuencia	10 Khz a 300 Mhz
Micro ondas	300 Mhz a 300 Ghz
Infra rojo	300 Ghz a 400 Thz

Fuente: elaboración propia, con programa Microsoft Excel.

En la tabla se resumen las características de transmisión en medios no confinados para las distintas bandas de frecuencia. Las microondas cubren parte de la banda de UHF y cubren totalmente la banda SHF; la banda de ondas de radio cubre la VHF y parte de la banda UHF.

1.3.4. Por el tipo de información

Por el tipo de información están la telefónica fija, que es aquella que hace referencia a las líneas y equipos que se encargan de la comunicación entre terminales telefónicos no portables, telefonía móvil básicamente está formada una red de comunicaciones y los terminales que permiten el acceso a dicha red y datos que se presenta.

1.3.4.1. Red de telefonía fija

El servicio de telefonía fija surge como respuesta a la necesidad de interconectar los diversos usuarios que deseaban establecer una comunicación vocal y aunque al principio era una iniciativa privada pronto se convirtió en un servicio público. En la mayoría de los países se realizó la concesión de la explotación de estas redes a una única empresa, de carácter estatal con fuerte presencia gubernamental, a modo de monopolio. Mediante el servicio de telefonía fija lo que se ofrece es la posibilidad de establecer comunicaciones vocales entre dos puntos cualesquiera de la red.

Los conmutadores usados para enrutar las llamadas telefónicas, que fueron alguna vez electromecánicas son ahora ampliamente reemplazadas por de conmutadores electrónicos digitales sofisticados los sistemas conmutadores electrónicos son mucho más flexibles porque ellos pueden ser programados

para proveer nuevos servicios. Las últimas generaciones de conmutadores han hecho un número de nuevas características posible.

1.3.4.2. Red de telefonía móvil

La red de telefonía móvil o celular consiste en un sistema telefónico en el que mediante la combinación de una red de estaciones transmisoras-receptoras de radio (estaciones base) y una serie de centrales telefónicas de conmutación, se posibilita la comunicación entre terminales telefónicos portátiles (teléfonos móviles) o entre terminales portátiles y teléfonos de la red fija tradicional.

La palabra celular referido a la telefonía móvil, deriva del hecho de que las estaciones base, que enlazan vía radio los teléfonos móviles con los controladores de estaciones base están dispuestas en forma de una malla, formando células o celdas cada estación base está situada en un nodo de estas células y tiene asignado un grupo de frecuencias de transmisión y recepción propio. Como el número de frecuencias es limitado con esta disposición es posible reutilizar las mismas frecuencias en otras células, siempre que no sean adyacentes, para evitar interferencia entre ellas. Básicamente existen dos tipos de redes de telefonía móvil:

- Red de telefonía móvil análoga. Como su propio nombre indica en esta red la comunicación se realiza mediante señales vocales analógicas tanto en el tramo radioeléctrico como en el terrestre, trabajando posteriormente en una banda de los 900 MHz.
- Red de telefonía móvil digital. En esta red la comunicación se realiza mediante señales digitales lo que permite optimizar tanto el aprovechamiento de las bandas de radiofrecuencia como la calidad de

transmisión. Su exponente más significativo en el ámbito público es el estándar GSM y su tercera generación, UMTS. Funciona en las bandas de 850/900 y 1800/1900 MHz. Hay otro estándar digital denominado CDMA. En el ámbito privado y de servicios de emergencias como policía, bomberos y servicios de ambulancias se utilizan los estándares *Tetrapol* y *Terrestrial Trunked RAdio* (TETRA) en diferentes bandas de frecuencia.

1.3.4.3. Red de datos

Se instalan para compartir recursos como impresoras o discos duros para compartir información, bases de datos para tener acceso a computadores centrales; para tener comunicación más expedita, usando el correo electrónico y para tener conectividad.

A una red de datos se puede conectar computadoras personales, servidores de comunicaciones, faxes, minicomputadoras, computadoras centrales.

1.4. Modelo OSI

El sistema de comunicaciones del modelo OSI estructura el proceso en varias capas que interaccionan entre sí. Una capa proporciona servicios a la capa superior siguiente y toma los servicios que le presta la siguiente capa inferior. De esta manera, el problema se divide en sub problemas más pequeños y por tanto más manejables.

Para comunicarse dos sistemas, ambos tienen el mismo modelo de capas. La capa más alta del sistema emisor se comunica con la capa más alta del sistema receptor, pero esta comunicación se realiza vía capas inferiores de

cada sistema. La única comunicación directa entre capas de ambos sistemas es en la capa inferior (capa física). Los datos parten del emisor y cada capa le adjunta datos de control hasta que llegan a la capa física. En esta capa son pasados a la red y recibidos por la capa física del receptor.

1.4.1. Las capas de OSI

El modelo OSI se divide en 7 capas; el proceso de transmisión de la información entre equipos informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global, estas se pueden clasificar en:

- Capa física
- Capa de enlace de datos
- Capa de red
- Capa de transporte
- Capa de sesión
- Capa de presentación
- Capa de aplicación

1.4.1.1. Capa física

Se encarga de pasar bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

1.4.1.2. Capa de enlace de datos

Esta capa debe encargarse de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.

1.4.1.3. Capa de red

Esta capa se encarga de enlazar con la red y encaminar los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos. Esta y las dos capas inferiores son las encargadas de todo el proceso externo al propio sistema y que están tanto en terminales como en enlaces o repetidores.

1.4.1.4. Capa de transporte

Se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos) o no orientado a conexión (datagramas).

1.4.1.5. Capa de sesión

Se encarga de proporcionar diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones. Puede agrupar datos de diversas aplicaciones para enviarlos juntos o incluso detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.

1.4.1.6. Capa de presentación

Esta capa se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación.

1.4.1.7. Capa de aplicación

Esta capa acoge a todas las aplicaciones que requieren la red. Permite que varias aplicaciones compartan la red para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros (FTP).

1.5. Protocolos TCP/IP

Es un protocolo abierto, lo que significa que se publican todos los aspectos concretos del protocolo y cualquiera los puede implementar, TCP/IP está diseñado para ser un componente de una red, principalmente la parte del software. Todas las partes del protocolo TCP/IP tienen unas tareas asignadas como enviar correo electrónico, proporcionar un servicio de acceso remoto, transferir ficheros, asignar rutas a los mensajes o gestionar caídas de la red.

1.5.1. Arquitectura de protocolos TCP/IP

No hay un estándar para este modelo al contrario del OSI, una referencia común es la arquitectura ideal del protocolo de conexión de redes desarrollada por la International Organization for Standardization (ISO), pero generalmente se pueden clasificar en cinco capas:

- Capa de aplicación
- Capa de transporte
- Capa de Internet (IP)
- Capa de acceso a la red
- Capa física

1.5.1.1. Capa de aplicación

La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. Proporciona comunicación entre procesos o aplicaciones en computadores distintos.

1.5.1.2. Capa de transporte (TCP)

La capa de transporte, proporciona servicios de transporte desde el *host* origen hacia el *host* destino, esta capa forma una conexión lógica entre los puntos finales de la red, el *host* transmisor y el *host* receptor. Encargada de transferir datos entre computadores sin detalles de red pero con mecanismos de seguridad.

1.5.1.3. Capa de Internet (IP)

La capa de Internet selecciona la mejor ruta para enviar paquetes por la red, el protocolo principal que funciona en esta capa es el Protocolo de Internet (IP), que se encarga de direccionar y guiar los datos desde el origen al destino a través de la red o redes intermedias.

1.5.1.4. Capa de acceso a la red

La capa de acceso de red, es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red, es la Interfaz entre sistema final y la subred a la que está conectado.

1.5.1.5. Capa física

La capa de red física, define las características del medio, señalización y codificación de las señales, especifica las características del hardware que se utilizará para la red.

1.5.2. Funcionamiento de TCP e IP

IP está en todas las computadoras y dispositivos de encaminamiento y se encarga de retransmitir datos desde un computador a otro pasando por todos los dispositivos de encaminamiento necesarios. TCP está implementado sólo en las computadoras y se encarga de suministrar a IP los bloques de datos y de comprobar que han llegado a su destino.

Cada computadora debe tener una dirección global a toda la red además cada proceso debe tener un puerto o dirección local dentro de cada computador para que TCP entregue los datos a la aplicación adecuada. Ejemplo una computador A desea pasar un bloque desde un puerto 1 a un puerto 2 en un computador B, TCP de A pasa los datos a su IP, y éste sólo mira la dirección del computador B, pasa los datos por la red hasta IP de B y éste los entrega a TCP de B, que se encarga de pasarlos al puerto 2 de B.

La capa IP pasa sus datos y bits de control a la de acceso a la red con información sobre qué encaminamiento tomar, y ésta es la encargada de pasarlos a la red. Cada capa va añadiendo bits de control al bloque que le llega antes de pasarlo a la capa siguiente. En la recepción, el proceso es el contrario. TCP adjunta datos de: puerto de destino, número de secuencia de trama o bloque y bits de comprobación de errores.

1.5.3. Interfaces de protocolo, las aplicaciones

Hay muchas aplicaciones que no requieren todos los protocolos y pueden utilizar sólo algunos sin problemas. Hay una serie de protocolos implementados dentro de TCP/IP:

1.5.3.1. Protocolo sencillo de transferencia de correo (SMTP)

Es un protocolo de servicio de correo electrónico, listas de correo y su misión es tomar un mensaje de un editor de texto o programa de correo y enviarlo a una dirección de correo electrónico mediante TCP/IP.

1.5.3.2. Protocolo de transferencia de ficheros (FTP)

Permite el envío y recepción de ficheros de cualquier tipo de o hacia un usuario. Cuando se desea el envío, se realiza una conexión TCP con el receptor y se le pasa información sobre el tipo y acciones sobre el fichero así como los accesos y usuarios que pueden acceder a él.

2. DESCRIPCIÓN GENERAL DE SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES

2.1. Planificación de la seguridad

Antes de analizar los aspectos técnicos de la seguridad en redes de telecomunicación y las tecnologías de seguridad relacionadas, es conveniente repasar algunos aspectos de planificación y organización que resultan relevantes para afrontar una estrategia de seguridad en redes de telecomunicación. Este tipo de planificación debe realizarse en una estrategia integral de protección de los sistemas de información de una organización existen distintas normas y recomendaciones que permiten implantar, administrar, mantener y verificar una política de seguridad.

2.1.1. Ciclo de seguridad

La planificación de seguridad puede ser descrita de forma general como un flujo de procesos destinados a la realización de un análisis de riesgos final, en lo que se denomina ciclo de seguridad, el ciclo de seguridad básico consta de varias fases:

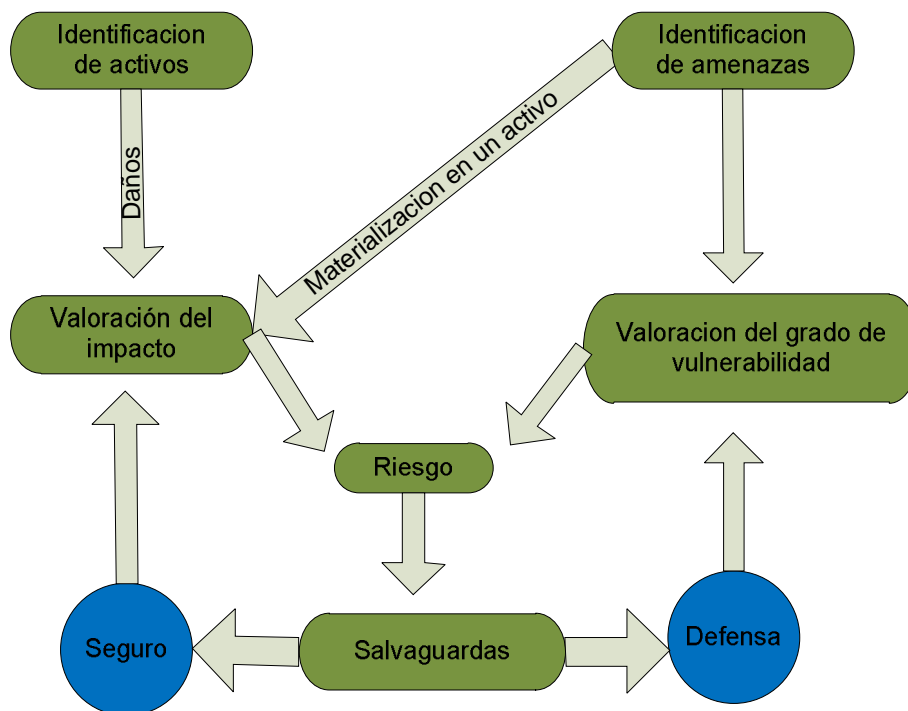
- Identificación de los activos de la organización susceptibles de ser atacados. Se distinguen múltiples tipos de activos, tales como equipos, utilización de recursos, prestigio e imagen.
- Identificación de las amenazas que podrían realizarse sobre dichos activos, desde amenazas por efectos atmosféricos o medioambientales,

hasta amenazas más técnicas como puede ser un ataque desde redes externas.

- Valoración del impacto que una amenaza puede tener en un activo en caso de materializarse.
- Valoración de la vulnerabilidad del activo a dicha amenaza.

La combinación de vulnerabilidad e impacto de un potencial ataque define el grado de riesgo que se está corriendo ante dicho ataque, como se muestra en la figura 2.

Figura 2. **Ciclo de seguridad**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

2.1.2. Activos

Se considera un activo todo aquello que usa o posee una organización y que es susceptible de ser atacado. En un entorno de sistemas de información y redes de telecomunicación existirán activos tales como:

Recursos físicos, que tienen un valor económico en sí mismos. Utilización de recursos, ya que un ataque que atente contra la utilización de los recursos tiene un determinado impacto, bien sea por falta de disponibilidad o por pago por utilización. Información almacenada en los sistemas de información de la organización independientemente de la naturaleza de la misma (datos, software.

Información en tránsito. Este activo, específico en los entornos que utilizan redes de telecomunicación, es el único que puede estar localizado en entornos externos al ámbito de una organización ya que por información en tránsito se consideran los datos de la organización que están siendo transmitidos a través de redes externas a la organización. Esta información necesita unos mecanismos de protección distintos al resto; mientras que los activos localizados en el interior de la organización pueden ser objeto de mecanismos de defensa evitar que el ataque llegue al activo, para estos activos sólo se pueden aplicar mecanismos de seguro minimizar el impacto del ataque.

Imagen de la organización este activo es de suma importancia en ciertos casos, ya que un ataque a la imagen de una organización puede ser publicitado en medios públicos, y la reputación de tal organización quedaría en entredicho.

2.1.3. Amenazas

Una amenaza es cualquier evento que puede desencadenar un incidente en la organización, produciendo daños en sus activos. La identificación de amenazas se puede hacer según su origen o según el activo objetivo de estas amenazas.

Según el origen se pueden clasificar en amenazas originadas en el entorno común a cualquier análisis de riesgos que conlleve recursos físicos, tales como amenazas climatológicas, ambientales, suministro eléctrico y amenazas originadas por personas. Dentro de este último tipo de amenazas, se distingue a su vez entre amenazas de personal interno malintencionado, errores de personal interno y amenazas de personas externas malintencionadas.

Aunque las amenazas más famosas en el entorno de Internet y las redes abiertas de telecomunicación son las producidas por personal externo que intenta entrar en la red de una organización, son mucho más peligrosas las amenazas del personal interno malintencionado. El motivo radica en que para defenderse del exterior es posible desarrollar tecnologías que bloqueen o filtren estas amenazas, pero es mucho más complicado impedir potenciales ataques del personal interno, ya que este personal tiene acceso a todos los recursos de la organización, siendo más difícil su detección y bloqueo.

Existen formas de mitigar el problema, como el uso de sistemas de autenticación y autorización de acceso a recursos internos por parte del personal de la empresa, los propios administradores de seguridad. Este perfil es muy sensible dentro de una organización, por lo que es necesario tener un seguimiento en detalle de estas personas, en cuanto a su predisposición a realizar ataques a la red de la organización.

Cabe destacar como potencial amenaza los propios errores del personal interno que, sin intención pueden ser capaces de destruir o modificar activos del sistema y red. Como medida preventiva de este tipo de amenazas, es necesario incluir los adecuados sistemas de autenticación y autorización, así como unos métodos de recuperación de activos apropiados.

Se han revisado las distintas amenazas existentes desde el punto de vista del origen. Se detallan a continuación las amenazas más importantes en función de los activos objetivos:

- Amenazas a recursos físicos
- Amenazas a la utilización de recursos
- Amenazas a la información almacenada
- Amenazas a la información en tránsito
- Amenazas a la imagen y reputación
- Daños a terceros

2.1.3.1. Amenazas a recursos físicos

Las amenazas que pueden afectar a los recursos físicos son las mismas que en cualquier otro entorno de seguridad, como seguridad civil, seguridad del hogar. Estas amenazas pueden ser:

- Amenazas intencionadas producidas por personas malintencionadas: robo, alteración, destrucción de equipos y sistemas informáticos.
- Amenazas de entorno: desastres naturales inundaciones, terremotos, incendio, suministro eléctrico, temperatura.

Las medidas de seguridad para este tipo de amenazas deben basarse en:

- Sistemas de control de acceso físico, para evitar el acceso de personal no autorizado a los recursos físicos.
- Sistemas de detección y prevención contra incendios, suministro eléctrico, sistemas de alimentación ininterrumpida.

Es necesario ante este tipo de amenazas, desarrollar un denominado Plan de Contingencia de la organización, que permita establecer los procedimientos de actuación para minimizar las consecuencias y el impacto de este tipo de amenazas.

2.1.3.2. Amenazas a la utilización de recursos

La utilización de los recursos, es un activo importante de una organización que puede ser atacado causando un cierto impacto. Las amenazas son frecuentemente provocadas por personas internas o externas que efectúan una utilización inadecuada de los recursos de la organización. Las consecuencias de este tipo de amenazas, se plasman en una reducción de disponibilidad de los recursos y una pérdida económica cuando la utilización de los recursos implique un costo económico.

2.1.3.3. Amenazas a la información almacenada

Las amenazas de información de la organización bien sean datos o programas almacenados en los discos o sistemas de almacenamiento. El impacto es mayor normalmente cuando se produce un ataque a los datos,

software y a las aplicaciones ya que suele suponer pérdidas de tiempo para la reinstalación de los sistemas de red.

2.1.3.4. Amenazas a la información en tránsito

La información en tránsito es otro activo que hay que proteger. Es la información de la organización que está en tránsito por redes externas sobre las que no se tiene control para implantar salvaguardas de tipo físico. Por lo tanto, todas las medidas de seguridad estarán orientadas a minimizar el impacto de este ataque, ya que es imposible llevar a cabo medidas de tipo defensivo. Los ataques que pueden darse son:

- Acceso al contenido de la información en tránsito ataque a la confidencialidad.
- Modificación en tránsito del contenido de la información ataque a la integridad.
- Introducción en tránsito de información falsa ataque a la autenticación.
- Eliminación de datos ataque a la disponibilidad.

Existen otros tipos de ataques específicos de la información en tránsito, que son los denominados ataques de repudio, los cuales se fundamentan en realizar una transmisión o recepción de datos, y negarlo posteriormente. Existen dos variantes de este tipo de ataques:

- Repudio de transmisión: negación de haber enviado datos alegando un ataque de autenticación (no lo transmití, alguien ha falsificado mi identidad para enviar esos datos).
- Repudio de recepción: negación de haber recibido datos alegando un ataque de disponibilidad (no lo recibí, alguien ha eliminado los datos antes de que llegar a su destino).

2.1.3.5. Amenazas a la imagen y reputación

Las amenazas a la imagen y reputación de una organización son unas de las más extendidas actualmente por su facilidad relativa de realización. Son ataques que suponen un impacto pequeño en otros activos, pero un gran impacto por la pérdida de credibilidad y reputación que supone la publicidad de estos hechos a gran escala.

Es uno de los ataques más frecuentes actualmente en Internet y se basa precisamente en la publicidad posterior del ataque, aunque éste no hubiese producido ningún impacto de consideración en los activos de la organización. El hecho de que se conozca a gran escala que la organización fue objeto de un ataque supone un perjuicio considerable para la imagen y la reputación de la organización.

2.1.3.6. Daños a terceros

Existen amenazas que no están dirigidas contra ninguno de los activos de una organización, que consisten en la utilización de los recursos de una organización para efectuar daños a terceros. De esta forma organizaciones que no tienen unas adecuadas medidas de seguridad pueden ser convertidas en

pasarelas de ataques a otros destinos pudiendo ser objeto posterior de una posible petición de responsabilidades por los daños realizados.

Este es el caso de las denominadas redes de bots (*botnets*) que se esparcen accediendo a sistemas informáticos sin las adecuadas medidas de seguridad y desde ellos realizando diversas acciones como por ejemplo, envío de publicidad no solicitada participación en un ataque masivo de negación de servicio distribuido.

2.1.4. Vulnerabilidades e impacto

Un análisis de riesgos es la valoración de las vulnerabilidades específicas de la organización a las amenazas identificadas y los impactos que dichas amenazas pueden producir en los activos de la organización como la vulnerabilidad e impacto.

- La vulnerabilidad debe medir de alguna forma la posibilidad real de que una amenaza se materialice sobre un activo de la organización. Este depende de muchos factores globales y específicos de la organización, como su visibilidad global, su percepción por los usuarios.
- El impacto debe medir las consecuencias de la materialización de una amenaza sobre un activo de la organización. En algunas ocasiones se puede imputar una cantidad económica pero la mayoría de las veces el impacto tiene componentes subjetivos específicos de la organización como por ejemplo una interrupción de un servicio, una incidencia medios de comunicación.

Se trata de elementos muy difíciles de estimar cuantitativamente por lo que es necesaria muchas veces una cuantificación relativa para un análisis de riesgos lo importante es conocer que es más vulnerable a una cierta amenaza que a otra, o que un ataque tiene más impacto que otro. Este grado de cuantificación relativa para las vulnerabilidades y los impactos pueden ser suficientes para abordar un análisis de riesgos.

2.1.5. Identificación de riesgos

El análisis de riesgos, es la identificación de riesgos para aplicar una política de seguridad optimizada para dichos riesgos. Es necesario identificar los riesgos a los que está sujeta la organización y que se deducen de los pasos anteriores al valorar las vulnerabilidades y los impactos.

Un riesgo representa una amenaza que puede materializarse sobre un activo y que se caracteriza por el grado de vulnerabilidad a la amenaza y por el impacto que supondría el ataque. La combinación vulnerabilidad e impacto es el grado de importancia de un riesgo cuanto mayor sea el impacto y más vulnerable se sea a un riesgo, más importante será el riesgo. Los peores riesgos son aquellos a los que son muy vulnerables y que genera un gran impacto.

Una vez elaborada el análisis de riesgos, el siguiente paso es decidir qué riesgos van a ser asumidos por la política de seguridad de la organización, afrontando en primer lugar los riesgos más importantes y continuando por los riesgos menos importantes del resto de análisis de riesgos. Pero llegará un momento en el que será necesario parar, ya que no es económicamente rentable afrontar todos los posibles riesgos de una organización, puesto que el

costo de afrontar el riesgo puede ser mayor que el costo que conlleva el impacto del riesgo. Los costos de la seguridad pueden ser:

- Costos directos que son provocados por la instalación, implantación y operación de procesos y tecnologías de seguridad. En estos costos deberán estar incluidos las inversiones en nuevos equipos, sistemas, software, así como su amortización, mantenimiento, operación y los gastos de personal específicos dedicados a la seguridad.
- Costos indirectos que son provocados por la afección a los procesos de negocio de la política de seguridad diseñada. En estos costos que usualmente son subjetivos, deberán valorarse los costos derivados de la dificultad de uso para los usuarios que conlleva cumplir la disciplina de seguridad derivada de la política, las restricciones de servicios y funcionalidades provocadas por la política de seguridad y la reducción de prestaciones que se puede dar en los servicios, derivadas de las tecnologías de seguridad.

El coste total de la seguridad será la suma de dos componentes que son:

- Costos (directos más indirectos) provocados por la introducción de medidas de seguridad.
- Costos provocados por los impactos de los riesgos no cubiertos por la política de seguridad.

La identificación de este punto de equilibrio financiero de la seguridad desvela los riesgos que deben ser afrontados por la política de seguridad a

partir de aquí, es necesario diseñar una política de seguridad que permita disminuir la importancia de esos riesgos, son los siguientes:

- Medidas defensivas, que disminuyan la vulnerabilidad de la organización asociada a ese riesgo y disminuir la importancia del riesgo.
- Medidas de seguro, que disminuyan el impacto del riesgo y por lo tanto, su importancia.

La política de seguridad debe ser diseñada como un conjunto de procedimientos y actuaciones destinado a disminuir la importancia de estos riesgos. Estos procedimientos y actuaciones imponen una disciplina que puede ser implantada mediante productos, tecnología de seguridad y/o simplemente recomendados. Es importante que la política de seguridad se publicado y difunda adecuadamente entre los usuarios de la organización.

2.2. Políticas generales de seguridad

La política de seguridad de las redes de telecomunicaciones, se define como el conjunto de requisitos definidos por los responsables directos o indirectos de la red que indican los términos generales qué está y qué no está permitido en la red.

2.2.1. Qué son las políticas de seguridad redes de telecomunicaciones

Una política de seguridad de las redes de telecomunicaciones es una forma de comunicarse con los usuarios, los gerentes y personal de una organización, los PSI (sistema de prevención de intrusos) establecen el canal

del personal en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la organización.

2.2.2. Elementos de una política de seguridad

El PSI (sistema de prevención de intrusos), debe orientar las decisiones que se toman en relación con la seguridad. Requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios.

- Responsabilidades por cada uno de los servicios y recursos de la red a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de la red que al alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Los PSI (sistema de prevención de intrusos), establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la organización. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

La política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley, las PSI (sistema de prevención de intrusos) como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes crecimiento de la planta de personal, cambio en la infraestructura de la red, alta rotación de personal, desarrollo de nuevos servicios, cambio y/o diversificación de negocios entre otros.

2.2.3. Parámetros para establecer políticas de seguridad

Las características de la PSI (sistema de prevención de intrusos), muestran una perspectiva de las implicaciones en la seguridad, algunos aspectos generales recomendados.

- Considere efectuar un ejercicio de análisis de riesgos informático de la red, a través del cual valore sus activos, el cual le permitirá afinar las PSI (sistema de prevención de intrusos) de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance.
- Comunicar a todo el personal involucrado en el desarrollo de las PSI (sistema de prevención de intrusos), los beneficios, riesgos relacionados con los recursos, bienes y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la organización.
- Desarrolle un proceso de monitoreo periódico en la seguridad de la organización, para realizar una actualización de la seguridad.

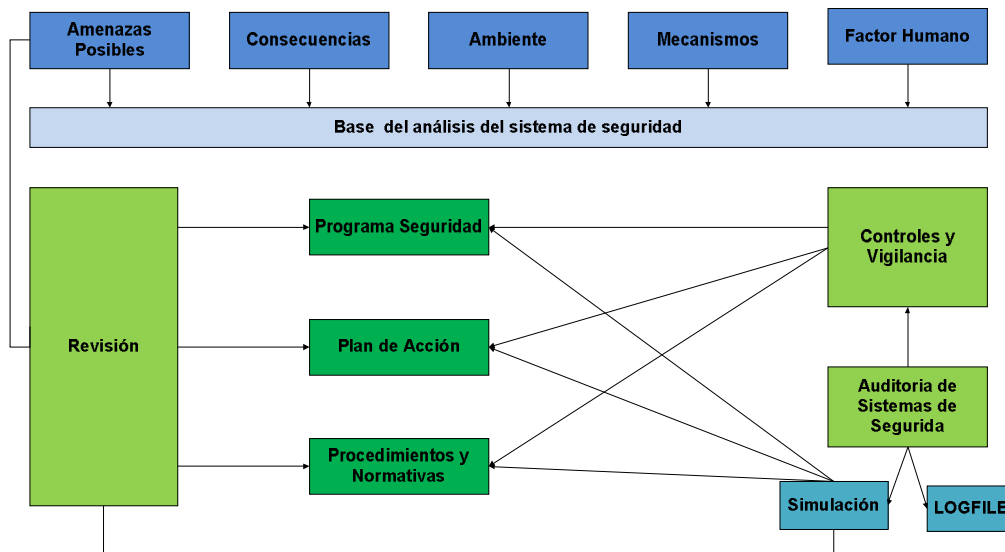
2.2.4. Proposición de una forma de realizar el análisis para llevar a cabo un sistema de redes de telecomunicaciones

Se comienza realizando una evaluación del factor humano interviniente teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad de los mecanismos con que se cuentan para llevar a cabo los procesos necesarios mecanismos técnicos, físicos, lógicos y el medio ambiente en que se desempeña el sistema, las consecuencias que puede traer defectos en la seguridad pérdidas físicas, pérdidas económicas, en la imagen de la organización y cuáles son las amenazas posibles.

Una vez aprobado se origina un programa de seguridad, que involucra los pasos a tomar para la seguridad que se desea. Luego se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

Con el propósito de asegurar el cumplimiento se realizan los controles y la vigilancia que aseguran el fiel cumplimiento de los temas anteriores. Para asegurar un marco efectivo, se realizan auditorías a los controles y a los archivos logísticos que se generen en los procesos implementados de nada vale tener archivos logísticos si nunca los analizan o los analizan cuando ya ha ocurrido un problema. El proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas, como se muestra en la figura 3.

Figura 3. Diagrama para el análisis de un sistema de seguridad



Fuente: manual de Seguridad en Redes ArCERT.

2.2.5. La políticas de seguridad generalmente no consiguen implantarse

En las organizaciones realizan grandes esfuerzos para definir la seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que llevan a los altos directivos a pensamientos como: más dinero para los juguetes de los ingenieros. Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que lleva a comprometer su información sensible y su imagen corporativa.

Los encargados de la seguridad deben asegurarse de que las personas relevantes entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir.

2.2.6. Las políticas de seguridad como base de la administración de la seguridad integral

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización la seguridad tiene varios estratos:

- El marco jurídico adecuado
- Medidas técnico administrativas como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto de otra. No tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados porque podría planificar un fraude o encubrir cualquier anomalía, deben intervenir personas diferentes. La seguridad física como la ubicación de los centros de procesos, las protecciones físicas, el control físico de accesos, los vigilantes, las medidas contra el fuego, el agua.

La seguridad lógica, como el control de accesos a la información exige la identificación y autenticación del usuario, el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, de información transmitida por línea.

2.2.7. Riesgos

Los riesgos pueden ser múltiples el primer paso es conocerlos y el segundo es tomar decisiones al respecto, los funcionarios se preguntan cuál es el riesgo máximo que podría soportar su organización. La respuesta no es fácil porque depende de la criticidad del sector y de la entidad misma, de su dependencia respecto de la información y del impacto que pudiera tener en la entidad. Si se basa en el impacto nunca debería aceptarse un riesgo que pudiera llegar a poner en peligro la propia la entidad.

Por debajo de ello hay daños de menores consecuencias siendo los errores y omisiones la causa más frecuente normalmente de poco impacto pero frecuencia muy alta como por ejemplo:

- El acceso indebido a los datos (a veces a través de redes).
- La cesión no autorizada de soportes magnéticos con información crítica.
- Los daños por fuego, por agua (del exterior como puede ser una inundación, o por una tubería interior).
- La variación no autorizada de programas, su copia indebida persiguiendo el propio beneficio de causar un daño, a veces por venganza.

Otra figura es la del *hacker* que intenta acceder a los sistemas sobre todo para demostrar a sí mismo que es capaz de superar las barreras de protección que se hayan establecido. Las amenazas hechas realidad pueden llegar a afectar los datos, en los programas, en los equipos, en la red y algunas veces simultáneamente en varios de ellos, como puede ser un incendio.

Como consecuencia de cualquier incidencia se pueden producir pérdidas que pueden ser no sólo directas comúnmente que son cubiertas por el seguro, sino también indirectas como la no recuperación de deudas al perder los datos o no poder tomar las decisiones adecuadas en el momento de carecer de la información.

2.2.8. Niveles de trabajo

La seguridad en los niveles de trabajo en las redes de telecomunicaciones, establece que la información que está en la red se protegido de amenazas y ataques, para la portación se tiene los siguientes.

- Confidencialidad
- Integridad
- Autenticidad
- No Repudio
- Disponibilidad de los recursos y de la información
- Consistencia
- Control de Acceso

2.2.8.1. Confidencialidad

Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

2.2.8.2. Integridad

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

- Causadas por errores de hardware y/o software
- Causadas de forma intencional
- Causadas de forma accidental

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

2.2.8.3. Autenticidad

En cuanto a telecomunicaciones se refiere, la autenticidad garantiza que quien dice ser X es realmente X. Es decir se deben implementar mecanismos para verificar quién está enviando la información.

2.2.8.4. No – repudio

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

2.2.8.5. Disponibilidad de la información

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

2.2.8.6. Consistencia

Se trata de asegurar que el sistema siempre se comporte de la forma esperada, de tal manera que los usuarios no encuentren variantes inesperadas, cuando utilizan los recursos de la red.

2.2.8.7. Control de acceso a los recursos

Consiste en controlar quién utiliza el sistema de red o cualquiera de los recursos que ofrece y cómo lo hace, para tener un mejor control de la seguridad en la red.

2.3. Sistemas de defensa perimetral

Los sistemas de autenticación y autorización facilitan un control de acceso lógico a los servicios proporcionados a usuarios externos autorizados, el siguiente paso es proteger la infraestructura de la red de intentos de acceso a servicios que no deben ser utilizados por usuarios externos, los intentos de acceso a estos servicios son una de las principales fuentes de ataques, el principal mecanismo de defensa ante estos ataques se le conoce como defensa perimetral que es un conjunto de filtros que restringen el acceso de las peticiones entrantes antes de que lleguen en los servicios internos de la organización.

Existen dos soluciones básicas de defensa perimetral que dependen del alcance de la infraestructura de la red: la defensa perimetral de un sistema y la defensa perimetral de red.

2.3.1. Defensa perimetral de sistema

Este tipo de defensa perimetral se denominan cortafuegos personales este método se basa en proteger un sistema individual de los intentos de ataque que le llegan por la red, esta defensa debe establecer una interceptación de las peticiones antes de que lleguen a los servidores de la capa de aplicación y las intenten procesar, dependiendo del nivel donde se lleva a cabo esta interceptación y filtrado de las peticiones entrantes, se pueden tener distintos tipos de sistemas:

- Interceptores TCP(*TCP-Wrappers*). Se trata de filtros que se ubican entre el nivel de transporte y el nivel de aplicación y que capturan la petición justo antes de ser atendida por el servidor.
- Interceptores de nivel de red. El filtro se ubica en el nivel de red.

2.3.1.1. Interceptores TCP

Este tipo de soluciones de defensa perimetral de sistema fue el primero que se desarrolló como mecanismo de protección de sistemas, ya que no exigía modificar el software de la torre de protocolos y se basaba en los denominados servidores dinámicos, que se arrancaban bajo demanda cuando había una petición para ellos que se basaban en el sistema operativo UNIX, modificaban la secuencia de arranque del servidor de forma que se ejecutaba primero un filtro que comprobaba la petición entrante frente a un fichero de reglas si la petición es aceptada, entonces se arrancaba el servidor. Este sistema tenía muchos problemas que hacían que no fuera una solución adecuada:

- Sólo era válido para servicios basados en el protocolo TCP.
- No era válido para las conexiones salientes. Solo podía capturar conexiones entrantes.

2.3.1.2. Interceptores de nivel de red

Este tipo de sistemas de defensa perimetral proporcionaba una solución completa al problema de la defensa perimetral de sistemas. La solución se basa en incluir el interceptor de tráfico en el nivel de red, junto al protocolo IP, de esta forma todas las peticiones entrantes y las salientes deben atravesar el filtro, por lo que se corrige el principal problema de los interceptores TCP. Además es válido para servicios basados tanto en TCP como en UDP ya que captura el tráfico a nivel IP. Los datos suelen incluir la dirección IP origen y el servicio solicitado, permitiendo mayor o menor grado de granularidad para la definición de las reglas y de las acciones (típicamente aceptar o rechazar).

La aplicación de los cortafuegos personales para el control de las peticiones salientes, pudiendo indicar las aplicaciones autorizadas a conectarse a Internet de esta forma se puede luchar contra los programas espía que se conectan a Internet sin autorización para el envío de datos personales.

2.3.2. Defensa perimetral de red

La defensa perimetral de la red en un entorno más amplio en el que el número de sistemas de red es elevado y están interconectados entre ellos con distintas subredes y equipos de interconexión la complejidad de administración de los cortafuegos personales de cada uno de los equipos puede llegar a ser muy elevada, debido a tres factores principales:

- Multiplicidad de equipos. Una solución de cortafuegos personales sólo es viable desde un punto de vista de administración y mantenimiento cuando el número de sistemas a gestionar es pequeño. Cuando el volumen de sistemas a proteger aumenta, la complejidad de configuración aumenta, la aplicación de parches, es demasiado alta y el riesgo de fallos de administración de seguridad puede aumentar peligrosamente.
- Heterogeneidad de equipos. En un entorno compuesto por múltiples sistemas de red, éstos pueden ser heterogéneos desde el punto de vista de su arquitectura hardware y software con distintos sistemas de red, diferentes configuraciones de servicios de red. La configuración de seguridad de cada uno de ellos es una tarea específica y distinta.
- Inclusión de equipos antiguos, es necesaria la existencia de equipos con versiones antiguas e inseguras de sistemas operativos o servidores de red, a la necesidad de ejecutar programas que sólo pueden ser ejecutados con esas versiones antiguas. La protección de estos sistemas de red inseguros no puede realizarse en la mayoría de los casos con cortafuegos personales, tiene que ser realizada más allá del perímetro de la red.

Ante estas situaciones surge el concepto de cortafuegos de red, definido como un equipo que se ubica en un punto de interconexión de subredes de una organización y que aplica criterios de filtrado al tráfico que lo atraviesa.

Parámetros del flujo de tráfico implícitos en el tráfico.

- Usuario origen o destino del tráfico
- Condiciones de entorno (hora, fecha, carga)

Las acciones de filtrado que se pueden ejecutar cuando se satisfacen los requisitos que incluyen:

- Autorización de tráfico entrante o saliente
- Bloqueo de tráfico entrante o saliente
- Rechazo de tráfico entrante o saliente
- Desvío de tráfico
- Solicitud de autorización y/o autenticación

De esta forma se puede configurar la protección de un conjunto de sistemas y subredes en un solo punto, independientemente de su tamaño y heterogeneidad, la administración de la seguridad de una red se simplifica drásticamente, al tener un solo punto de configuración de la política de seguridad, siendo mucho más fácil su administración y evolución. Se mejora la capacidad de monitorización de la seguridad en la red, ya que sólo hay un punto expuesto a ataques todos los ataques deben atravesar primero el cortafuegos, la vigilancia y monitorización es más sencilla que en el caso de la defensa perimetral de sistema.

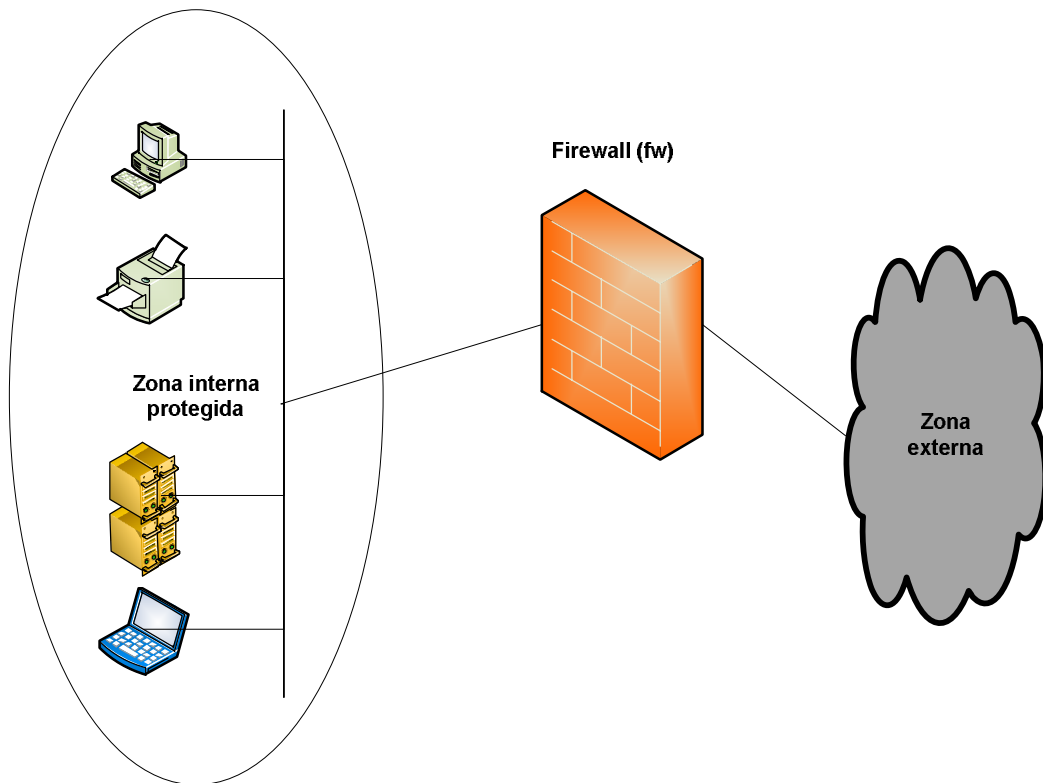
2.3.2.1. Zonas de seguridad

Para identificar las zonas de seguridad que existen en una organización es necesario identificar conjuntos de sistemas y subredes a los que se les puede aplicar una configuración de seguridad uniforme a todos ellos, una configuración puede incluir un determinado número de excepciones es recomendable que el número de excepciones sea lo más pequeño posible por

lo que es necesario que las zonas de seguridad estén compuestas por sistemas y subredes con los mismos o similares requisitos de protección.

El caso más simple que sólo se define una zona de seguridad interna en todas las redes de una organización y el resto de Internet es una zona externo. En este caso el cortafuegos se ubicaría en la conexión externa de las redes de la organización y se configuraría de una forma uniforme para todos los sistemas pertenecientes a la misma. Este tipo de zonificación tiene la ventaja de su simplicidad de administración, pero puede resultar demasiado rígido, necesitar la configuración de diversas excepciones, como se observa en la figura 4.

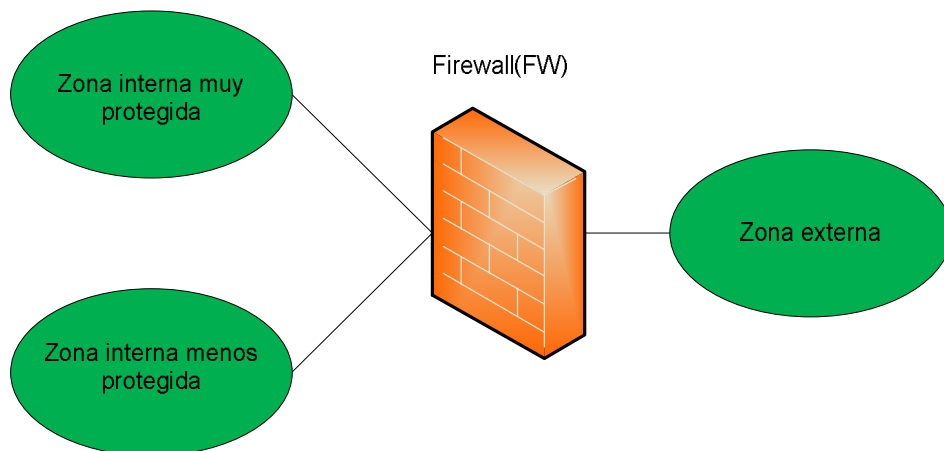
Figura 4. Cortafuegos de red con dos zonas de seguridad



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

La configuración de dos zonas de seguridad dentro de la organización una zona de configuración de seguridad más estricta, otra zona con una configuración menos estricta y la zona externa, de forma que el cortafuegos se ubica como interfaz entre estas dos zonas y también con la conexión externa (zona externa). La zona más segura tendrá una configuración de seguridad sin excepciones, y los equipos que necesiten una protección menos estricta se ubicarían en la segunda zona de seguridad, como se observa en la figura 5.

Figura 5. **Cortafuegos de red con tres zonas de seguridad**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

Dependiendo de las necesidades de cada organización pueden identificarse otro tipo de zonas de seguridad como por ejemplo, una zona de invitados, zona de investigación, el nivel de protección es distinto. En estos casos, será necesario ubicar uno o varios cortafuegos en las fronteras entre zonas.

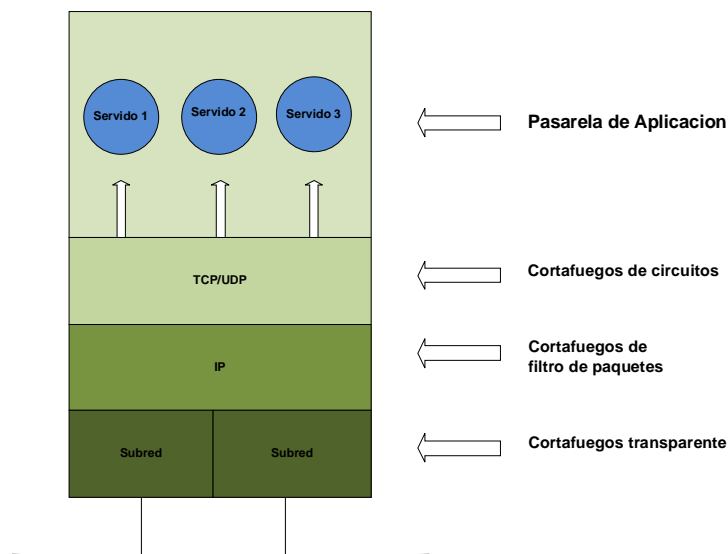
2.3.2.2. Tipos de cortafuegos

El cortafuego es un equipo que se ubica interconectando dos enlaces de red, que se encarga de aplicar la configuración de seguridad al tráfico que pretende atravesarlo en ambos sentidos. Al tener al menos dos conexiones de red, debe incluir una torre de protocolos que permita ejecutar los protocolos de Internet, en sus cuatro niveles:

- Nivel de enlace
- Nivel de red
- Nivel de transporte
- Nivel de aplicación

Se pueden distinguir cuatro tipos de cortafuegos, como se observa en la figura 6.

Figura 6. Tipos de cortafuegos



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

- Cortafuegos transparente: las funcionalidades de cortafuegos se incluyen en el nivel de enlace, actuando como un equipo puente entre distintos segmentos pertenecientes a una misma subred.
- Cortafuegos de filtro de paquetes: las funcionalidades de cortafuegos se incluyen en el nivel de red, actuando como un encaminador de datagramas IP entre distintas subredes.
- Cortafuegos de circuitos: las funcionalidades de cortafuegos se incluyen en el nivel de transporte, conectando o desconectando distintas conexiones TCP o UDP entre sí.
- Pasarela de aplicación: las funcionalidades de cortafuegos se incluyen dentro de la capa de aplicación como un conjunto de servicios de aplicación que imponen la configuración de seguridad de los cortafuegos.

2.3.2.2.1. Filtro de paquete

Este tipo de cortafuegos es el más simple y más utilizado, debido principalmente a la transparencia y nulo impacto en el resto de infraestructura de red, ya que no es necesario modificarla por el hecho de implantar los cortafuegos. Este tipo de cortafuegos también denominado *screeningrouter*, que actúa igual que un encaminador tradicional, aceptando datagramas IP que le llegan por sus enlaces y reencaminándolos por otros enlaces hacia otros destinos de acuerdo con una tabla de encaminamiento.

La principal diferencia con un encaminador tradicional es que antes de consultar la tabla de encaminamiento, se consulta la configuración de seguridad y en base a parámetros del propio datagrama IP o parámetros de entorno, el

datagrama es aceptado y encaminado hacia su destino o bloqueado según especifique la configuración de seguridad.

El cortafuegos de filtro de paquetes debe examinar los datagramas que llegan a él por cualquiera de sus interfaces y contrastarlos con la configuración de seguridad para determinar si el datagrama debe seguir su camino hasta su destino, según la tabla de encaminamiento o debe ser bloqueado o tratado de alguna otra manera. La configuración de seguridad se basa en contrastar parámetros de los datagramas IP ya que el cortafuegos de filtro de paquetes actúa a nivel de red, donde se manejan los datagramas del protocolo IP y se tiene acceso a los campos presentes en la cabecera de estos datagramas.

Estos campos incluyen la dirección IP origen y dirección IP destino del datagrama, resultan de gran utilidad para poder definir una configuración de seguridad en base al origen y el destino de los paquetes.

2.3.2.2.2. Transparentes

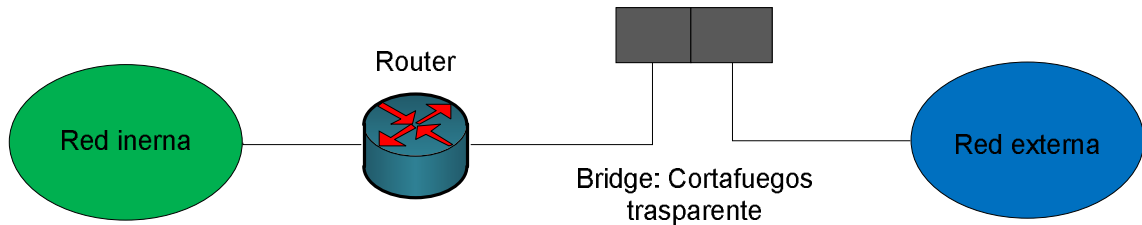
Los cortafuegos transparentes denominados cortafuegos de nivel de enlace, constituyen una variación del cortafuegos de filtro de paquetes, los cortafuegos de filtro de paquetes actúan como un encaminador, aceptando datagramas IP y encaminándolos por el enlace correspondiente según la tabla de encaminamiento hacia otra subred IP, el cortafuegos transparente actúa como una pasarela de nivel de enlace, lo que se conoce tradicionalmente como un *bridge*. Los *bridges* son equipos que interconectan dos o más enlaces y encaminan tramas de nivel de enlace entre ellos. Estos equipos han sido sustituidos actualmente por otro tipo de equipos, como los conmutadores *switches*.

El hecho de recuperar este tipo de tecnología para su utilización como cortafuegos radica en que este equipo funciona a nivel de enlace, encaminando tramas de nivel de enlace según las direcciones físicas, por lo que no necesita tener nivel de red, transporte o aplicación, si el equipo no tiene nivel de red, no soporta el protocolo IP y consecuentemente, no tiene dirección IP asociada.

Esta es la principal ventaja de este tipo de cortafuegos y de ahí su nombre, cortafuegos transparente, ya que al no tener una dirección IP, este cortafuegos es indetectable para un atacante remoto que esté en otra subred distinta a la del cortafuegos. Un cortafuegos de filtro de paquetes tiene una dirección IP que un atacante puede averiguar como consecuencia, intentar una serie de ataques dirigidos contra los propios cortafuegos motivo por el cual en las definiciones de reglas son las de autoprotección de los cortafuegos.

El cortafuegos transparente actúa como un *bridge* que interconecta normalmente dos enlaces Ethernet pertenecientes a una misma subred IP, pero inspecciona las tramas de nivel de enlace antes de encaminarlas por el enlace correspondiente, este tipo de cortafuegos no puede comparar solamente los parámetros que se encuentran en la cabecera de los protocolos de enlace, como hacen los bridges tradicionales, sino que deben ser más inteligentes y ser capaces de procesar el contenido de las tramas de enlace en busca de los paquetes IP, los parámetros de su cabecera y los paquetes TCP o UDP que se transportan en busca de los campos útiles como parámetros de filtrado, como se ilustra en la figura 7.

Figura 7. **Cortafuegos transparente**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

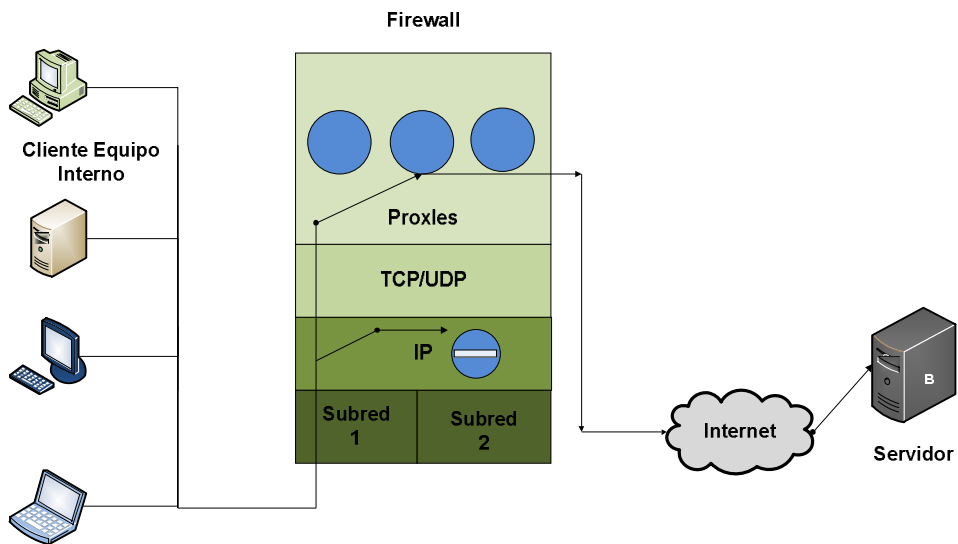
2.3.2.2.3. **Pasarela de aplicación**

En una pasarela de aplicación la funcionalidad de cortafuegos se realiza a nivel de aplicación en un conjunto de servidores pasarelas de aplicación o proxy de aplicación que aplican la configuración de seguridad a las conexiones que llegan a ellos. Una pasarela de aplicación es unos cortafuegos con dos o más enlaces conectados a distintas subredes que recibe datagramas IP por uno de sus enlaces, pero NO hace encaminamiento a nivel IP en ningún momento siendo ésta la característica principal de estos cortafuegos. Este hecho es una paradoja en la arquitectura de Internet, ya que supone en la práctica un corte en las comunicaciones IP ya que no existe conectividad entre las subredes interconectadas por los cortafuegos.

Un datagrama enviado desde un equipo interno con destino un equipo externo, será encaminado hasta llegar al cortafuegos donde se tirará, ya que el cortafuegos no lo encaminará a nivel IP hacia su destino final. Este tipo de cortafuegos corta las comunicaciones que intentan atravesarlo. La única forma de atravesar el cortafuegos pasa por establecer una comunicación desde el origen con el propio cortafuegos indicando el destino final de la conexión, que el

cortafuegos establezca una conexión con el destino requerido, como se muestra en la figura 8.

Figura 8. **Pasarela de aplicación**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

No existe conectividad directa entre las redes interna y externa por lo que un equipo interno que quiera establecer una conexión con un equipo externo, deberá primero establecer una conexión con el cortafuegos negociar con un servicio del cortafuegos la pasarela de aplicación y si la pasarela permite la conexión, establecer una conexión desde la pasarela hasta el equipo remoto requerido, la pasarela conecta las dos conexiones a nivel de aplicación. La conexión se hace efectiva en dos pasos: cliente-pasarela y pasarela-servidor, siendo necesario una pasarela por servicio.

Esta tecnología presenta una serie de ventajas e inconvenientes que a continuación se presentan.

La principal ventaja respecto a los cortafuegos de filtro de paquetes radica en la flexibilidad que tienen estos cortafuegos para establecer los parámetros de la configuración de seguridad, puesto que el equipo interno debe establecer una conexión con la pasarela de aplicación y negociar la conexión que requiere.

En esta negociación la pasarela de aplicación puede imponer los criterios que desean, como por ejemplo, dirección fuente, dirección destino, hora, parámetros similares a los especificados en los cortafuegos de filtro de paquetes lo que es más importante, identidad del usuario. Las pasarelas en respuesta a una petición de conexión remota, pueden solicitar el nombre del usuario y su clave, aplicar este criterio como un parámetro más de filtrado, permitiendo establecer configuraciones de seguridad mucho más detalladas. Se puede realizar filtrado por identidad de usuario a diferencia de los cortafuegos de filtro de paquetes en los que no era posible.

Por otra parte el cortafuegos aísla las redes que interconecta a nivel IP, permite que las redes internas no tengan conexión directa a Internet, por lo que se puede utilizar un plan de direccionamiento IP privado. Ninguna de las direcciones internas son visibles en Internet la única dirección IP visible será la del interfaz externo del cortafuegos. El hecho de no existir conexión directa a Internet desde el interior de la organización, se tiene una mayor seguridad.

El gran inconveniente este tipo de cortafuego es que no respeta la arquitectura de Internet, por lo que es necesario aplicar parches para su correcto funcionamiento. El principal parche que implican estos cortafuegos es la utilización de aplicaciones específicas, ya que el uso de aplicaciones normales no es válido. Una aplicación normal de Internet intentará establecer conexiones extremo a extremo, por lo que el cortafuego bloqueará esa conexión. Es necesario que la conexión se realice en dos pasos:

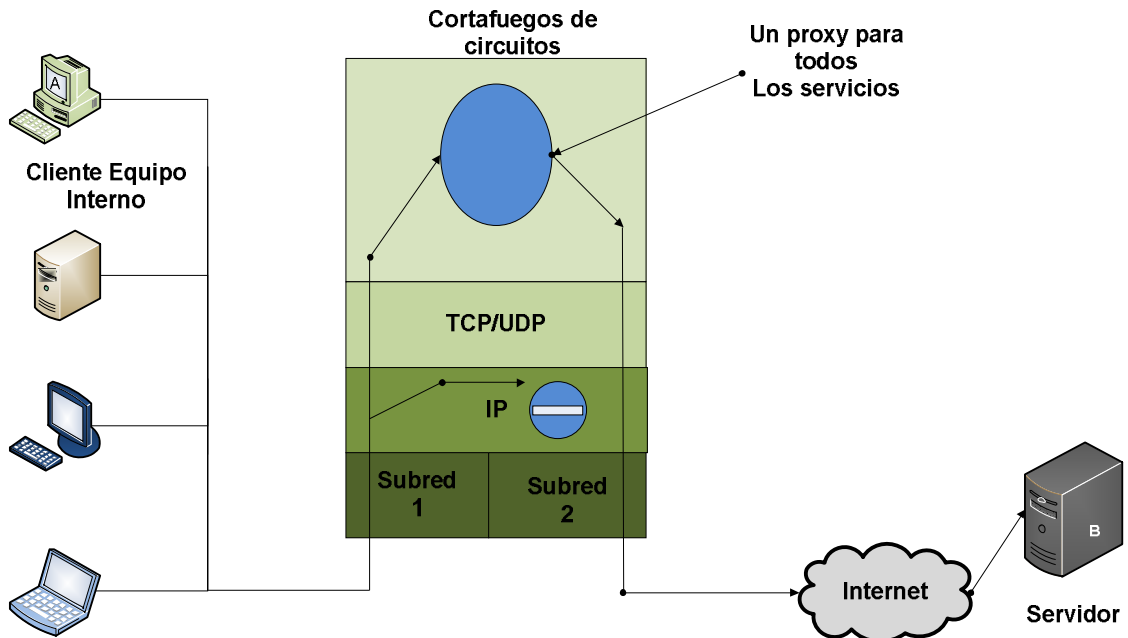
- Conexión cliente-cortafuegos en la que se establece la negociación de seguridad necesaria.
- Conexión cortafuegos-servidor donde se puentean ambas conexiones a nivel de aplicación.

2.3.2.2.4. Circuitos

El cortafuego de circuitos o cortafuegos de nivel de transporte es una variación de los cortafuegos de pasarela de aplicación. A pesar de estar ubicado en el nivel de transporte se trata de unos cortafuegos de nivel de aplicación basado en el concepto de pasarela de aplicación. La principal diferencia con las pasarelas de aplicación es existe una única pasarela servidora que se encarga del filtrado de todos los servicios por lo que la configuración de seguridad de cada servicio ya no puede ser específica, en los cortafuegos de circuitos sólo existe una pasarela genérica que aplica la configuración de seguridad a todos los servicios de la misma forma, utilizando el mismo conjunto de parámetros, como las direcciones IP origen y destino, servicio.

La posibilidad de solicitar autenticación al originador de la conexión y aplicar la identidad del usuario como parámetro de configuración de seguridad, como se muestra en la figura 9.

Figura 9. Cortafuegos de circuitos



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

2.3.2.3. Arquitecturas de red con cortafuegos

El diseñar la topología de una arquitectura de red con cortafuegos de una red que necesita protección con unos cortafuegos, es necesario combinar 3 elementos para la protección:

- El propio cortafuegos, que efectúa las labores de filtrado utilizando cualquiera de las cuatro tecnologías expuestas.
- El router de acceso al exterior de la organización.
- El conjunto de servicios que deben ser proporcionados al exterior y que deben estar accesibles desde el exterior. Los servidores que se encargan

de proporcionar estos servicios no pueden ser protegidos en su totalidad, constituyen uno de los puntos más débiles de la red de la organización.

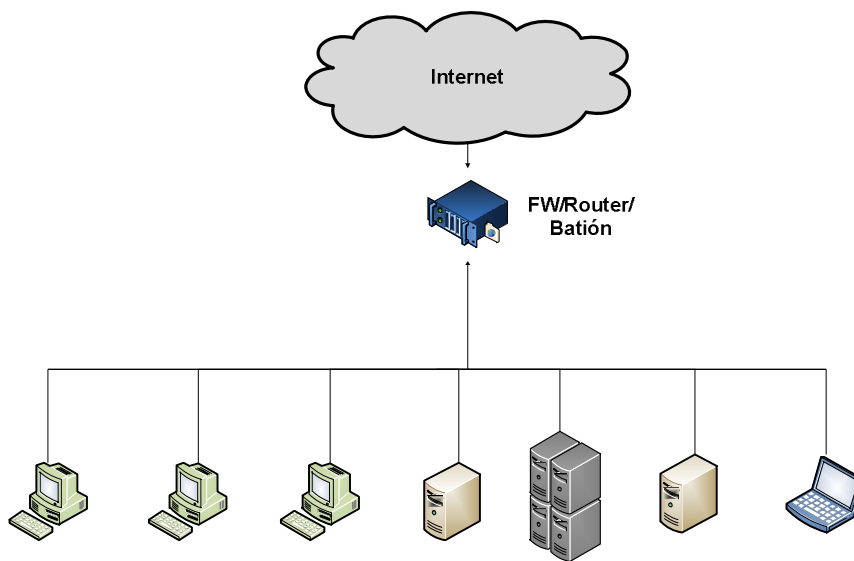
Tipos de arquitecturas de red con cortafuegos.

- Arquitectura *Dual-homed host*
- Arquitectura *Screened host*
- Arquitectura *Screened-subnet*

2.3.2.3.1. *Dual homed host*

La arquitectura *Dual homed host* es la arquitectura más simple y barata consiste en incluir los tres elementos mencionados en un solo equipo, como se muestra en la figura 10.

Figura 10. **Arquitectura *Dual homed host***



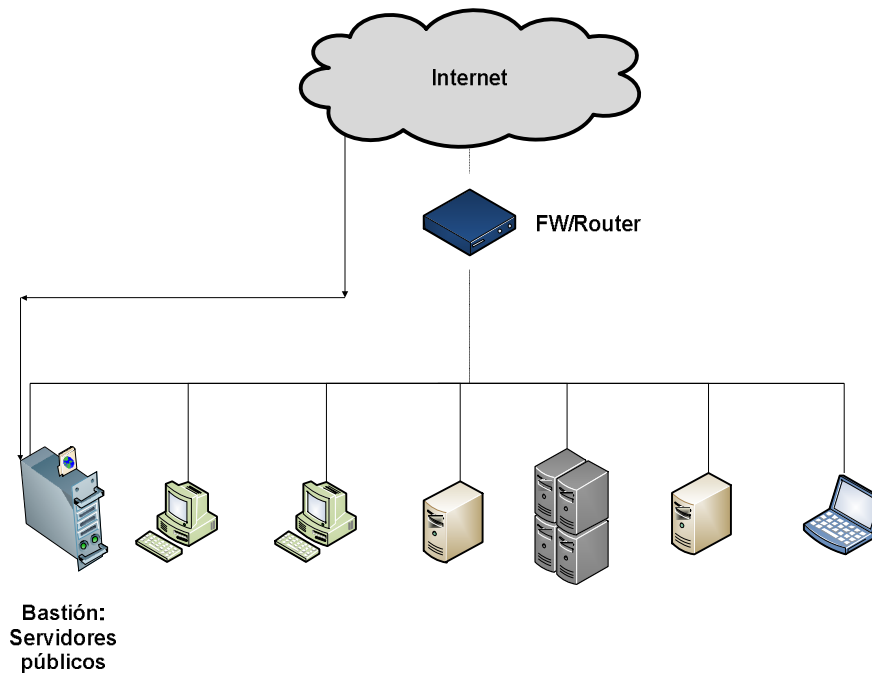
Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

En esta arquitectura no se tiene necesidad de interconexión desde el exterior hacia el interior, por lo que el cortafuegos puede ser de tecnología de circuitos o pasarela de aplicación, además de filtro de paquetes. El nivel de aplicación de los propios cortafuegos albergará los servicios públicos que la organización ofrecerá al exterior como Web, mail, DNS. Si es de tipo pasarela de aplicación, su nivel de aplicación también albergará las pasarelas que se hayan configurado. Si es de tipo filtro de paquetes, deberá ser configurado con las excepciones necesarias para poder llegar a los servicios públicos albergados en los propios cortafuegos.

2.3.2.3.2. *Screened host*

La arquitectura *Screened host* combina las funcionalidades de cortafuegos y de *router* de acceso, separando los bastiones en máquinas independientes que deberán ser declaradas explícitamente en la configuración de seguridad. Se tienen por un lado en la misma máquina cortafuegos y *router* de acceso, y por otro, los bastiones, como se muestra en la figura 11.

Figura 11. **Arquitectura Screened host**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

El cortafuego en este tipo de arquitectura debe ser de filtro de paquetes, no siendo aplicable el cortafuego de pasarela de aplicación ya que es necesario efectuar conexiones desde el exterior hacia los bastiones que están ubicados en la zona protegida de la organización. La configuración de estos cortafuegos debe incluir unas reglas de seguridad que permitan únicamente las conexiones hacia los servicios accesibles de los bastiones, restringiendo el resto de conexiones hacia el interior.

2.3.2.3.3. **Screened subnet**

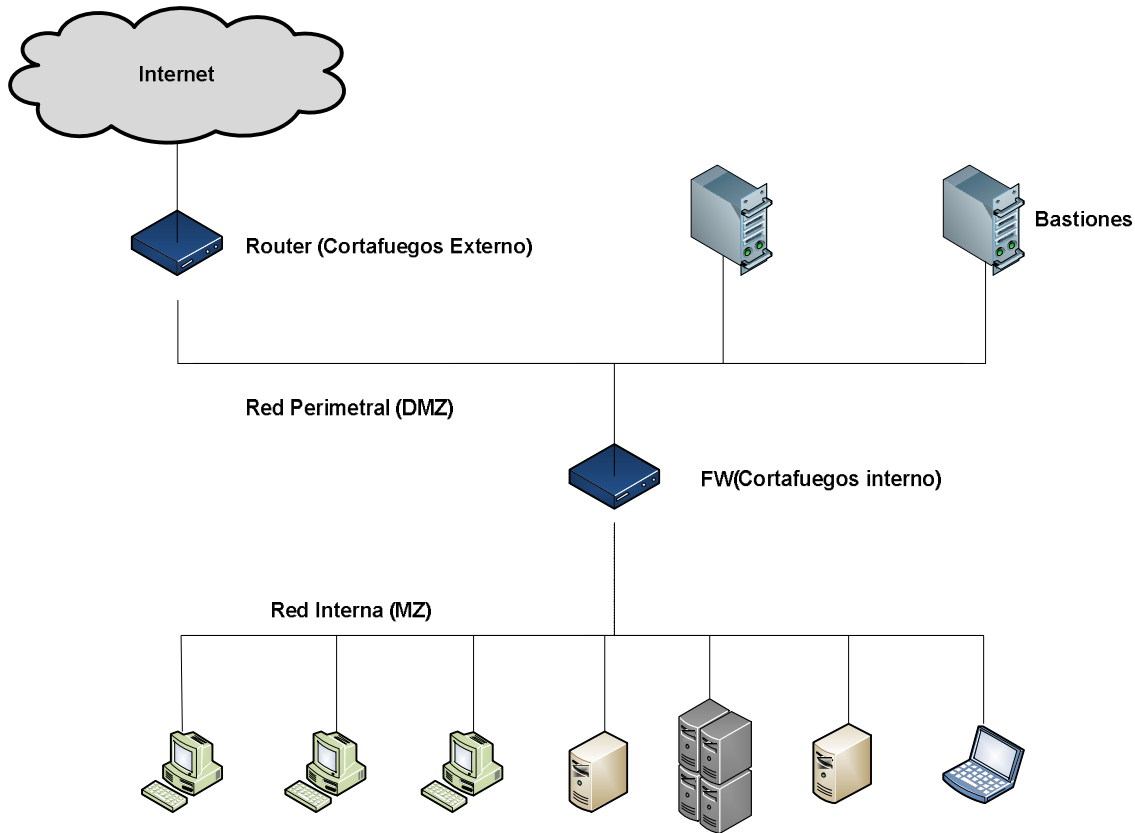
En la arquitectura *Screened subnet* se separan las tres funcionalidades necesarias en tres máquinas distintas, una para el *router*, otra para el

cortafuego y otra para el bastión que alberga los servicios. Esta es la solución más costosa, ya que necesita más infraestructura en cuanto al número de máquinas, más compleja desde el punto de vista de la topología de red, es necesario añadir una nueva red entre el *router* de acceso a Internet y el cortafuego. Esta red debe albergar los servicios accesibles desde el exterior de forma que en la zona interna no debe residir ninguno de estos servicios, el cortafuegos no tiene ninguna excepción de entrada configurada, y prohíbe toda conexión entrante procedente del exterior.

Esta arquitectura es la más recomendable desde el punto de vista de seguridad a cambio de una mayor inversión económica a pesar de que los bastiones siguen siendo vulnerables a posibles ataques y no están protegidos, un ataque a los bastiones no implica ningún otro riesgo de seguridad adicional. Esto se debe a que desde los bastiones no se puede acceder a la red interna ya que el cortafuego lo impide.

El *router* externo puede ser sustituido por un cortafuego de filtro de paquetes que permita solamente las conexiones necesarias a los bastiones, incrementado el nivel de seguridad y ofreciendo una protección adicional a los bastiones, como se muestra en la figura 12.

Figura 12. **Arquitectura Screened subnet**



Fuente: Villagrá González Víctor A. Seguridad en redes de telecomunicaciones.

2.3.2.4. Características avanzadas de cortafuegos

Se ha analizado el cortafuego desde el punto de vista de su funcionalidad básica, el filtrado de conexiones en base a una política de seguridad expresada en forma de reglas, el cortafuegos se ha convertido en un elemento esencial en la arquitectura de seguridad de red de las organizaciones motivo por el que poco a poco se ha ido enriqueciendo en cuanto a funcionalidades y ha ido asumiendo otro tipo de funciones relacionadas con la seguridad.

2.3.2.4.1. Traducción automática de direcciones

La funcionalidad adicional de los cortafuegos es la utilización de traducción automática de direcciones (*Network Address Translation NAT*). Muchas organizaciones necesitan utilizar NAT por diversos motivos, como el uso de direcciones privadas, confidencialidad del plan de direcciones interno, etc. se requiere un equipo específico que modifique las direcciones en la salida a Internet y que sea capaz de mantener tablas de correspondencia de direcciones en las conexiones establecidas.

Si la organización se protege del exterior con un cortafuegos de tipo pasarela de aplicación o de circuitos, la funcionalidad de NAT es innata a ellos, la única dirección visible de la organización en Internet es la del interfaz externo del cortafuegos pero si se tiene un cortafuegos de filtro de paquetes, es necesario incluir la funcionalidad de NAT en la salida a Internet.

2.3.2.4.2. Pasarela de aplicación transparente

Esta funcionalidad, pretende combinar las ventajas de las dos principales tecnologías de cortafuegos para la protección de la seguridad de las redes de telecomunicaciones se tiene los siguientes:

- Los cortafuegos de tipo filtro de paquetes son transparentes para el usuario que no tiene que modificar sus clientes o su configuración para atravesarlos.

- Los cortafuegos de tipo pasarela de aplicación permiten el uso de la identidad del usuario como parámetro para establecer las configuraciones de seguridad, permitiendo reglas de seguridad mucho más específicas y concretas. Permiten filtrar por usuario.

2.3.2.4.3. Seguridad en los contenidos

Los cortafuegos originales son utilizados como parámetros de filtrado de tráfico de las cabeceras de los protocolos de transporte y red, siendo en la mayoría de los casos suficiente para poder expresar las políticas de seguridad requeridas, éstas se referían a los servicios en su totalidad sin embargo surgieron nuevos ataques basados en la utilización anormal de los servicios atacando servidores Web con peticiones HTTP dañinas o intercambiando virus a través de mensajería instantánea.

Surgió la necesidad de diseñar las políticas de seguridad de tal forma que fueran capaces de discriminar por el contenido de los servicios, utilizando como parámetro de filtrado los campos de los protocolos de aplicación o incluso el propio contenido de los protocolos de aplicación pueden ser detectados los contenidos maliciosos, improductivos. Esto permite que el cortafuegos sea capaz de procesar no sólo las cabeceras de los protocolos de red y de transporte, sino también las de aplicación e incluso en algunos casos ser capaz de inspeccionar los contenidos del propio protocolo de aplicación.

2.4. Sistemas de detección de intrusos (IDS)

Se puede definir la detección de intrusos (*Intrusion Detection o ID*) como un modelo de seguridad aplicable a redes como a ordenadores. Un sistema IDS recolecta y analiza información procedente de distintas áreas de un red de ordenadores para identificar posibles fallos de seguridad. Este análisis en busca de intrusiones incluye tanto los posibles ataques externos desde fuera de nuestra organización como los internos debido al mal uso o fraudulento de los recursos. Los sistemas IDS suelen utilizar técnicas de análisis de vulnerabilidades a veces referenciado como *scanning*, es decir examinan todos nuestros sistemas en búsqueda de alguna vulnerabilidad.

Un sistema de detección de intrusos o IDS (*Intrusion Etection System*) es un paradigma que por su naturaleza intrínseca de supervisión de los recursos es aplicado tanto a ordenadores como a las redes. En el caso de los ordenadores se realiza a nivel de sistema operativo para controlar los accesos de los usuarios, modificación de ficheros del sistema, uso de recursos (CPU, memoria, red, disco), para de detectar cualquier comportamiento anómalo que pueda ser indicativo de un abuso del sistema.

En el caso de redes de ordenadores pueden monitorizarse usos de anchos de banda, accesos de direcciones no permitidas, uso de direcciones falsas. Para de encontrar un comportamiento anómalo o atípico en el tráfico de la red supervisada que nos pueda indicar una posible anomalía.

2.4.1. Firmas (*signatures*)

En cualquiera de los paquetes que circulan por la red, puede encontrarse un intento de ataque, el paseo triunfal de un *hacker* que ya ha conseguido

entrar en algún sistema de red. ¿Qué se puede? se puede una firma (*signature*) como aquello que define o describe un patrón de interés en el tráfico de nuestra red, se dirá que un filtro es la transcripción de una firma (*signature*) a un lenguaje comprensible por los sensores que monitorizan nuestra red.

Las firmas (*signatures*) permiten diferenciar entre todo el tráfico generado por la red y obtener un subconjunto de este lo suficientemente pequeño como para que sea tratable computacionalmente y lo suficientemente amplio como para poder detectar comportamientos anómalos en tiempo real o casi. Las firmas utilizadas en IDS usualmente son simples patrones que permiten detectar ataques ya conocidos (*Smurf, Land*). Su funcionamiento es el mismo que el de los antivirus, se basan en encontrar coincidencias de ataques ya conocidos en el tráfico actual de la red.

Algunos productos IDS permiten la creación de filtros por el usuario lo que facilita la adaptación del sistema a nuestras necesidades. Sin embargo, realizar filtros útiles necesita al menos de:

- Que el administrador de seguridad de la red esté calificado conozca perfectamente el protocolo IP y su propia red.
- Que el IDS proporcione un lenguaje suficientemente potente como para poder expresar nuestras necesidades.

La capacidad de crear filtros permite una gran flexibilidad y potencia en la detección de tráfico anómalo. Un ejemplo de esto podrían ser los filtros que se realizan sobre un protocolo en concreto (por ejemplo en HTTP) y que permiten incluso guardar log de las conexiones que envían y reciben determinada información (como por ejemplo los filtros contra pornografía).

La actualización de las firmas debe ser constante ya que usualmente un nuevo tipo de ataque no será detectado por el sistema

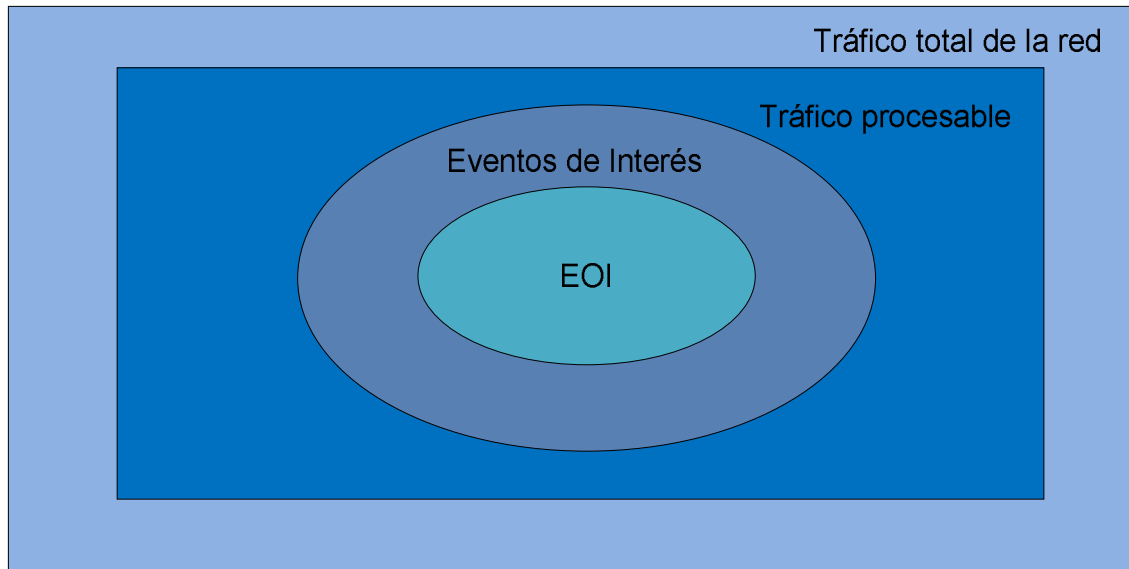
IDS que simplemente se dedique a buscar patrones en el tráfico de la red, el uso de un *firewall* bien configurado limitará la cantidad de tráfico a procesar así como la personalización adecuada de los filtros aplicados en la red, protegerá de un sistema seguro y útil en el que se puede confiar.

2.4.2. Eventos de interés (EOI)

Se define los eventos de interés (*Events Of Interest, EOI*) como el subconjunto mínimo de muestras que se debe analizar para considerar nuestra red segura o como el subconjunto de los genuinos positivos verdaderos.

Este subconjunto se obtiene a partir del resultado de aplicar los filtros, firmas y reglas personalizadas del sistema de detección de intrusos al tráfico total, como se muestra en la figura 13.

Figura 13. **Eventos de interés (EOI)**



Fuente: Verdejo Álvarez Gabriel Seguridad en redes IP IDS capítulo 3.

Proponer una fórmula de evaluación de riesgos para los eventos de interés detectados (EOI) y que puede ayudar a cuantificar numéricamente la gravedad del evento detectado los aspectos a tener en cuenta en esta fórmula.

$$\text{Severity} = (\text{Criticality} + \text{Lethality}) - (\text{System countermeasures} + \text{network countermeasures})$$

- Criticidad (*Criticality*). No todos los ordenadores tienen la misma función de esta forma un ataque a un servidor DNS, a un *firewall* o a un PC cliente se valoran de distinta forma.
- Letalidad (*Lethality*). Los diferentes ataques (*exploits*) no tienen siempre el mismo objetivo. Dependiendo de si simplemente tiene posibilidades de funcionar en algún sistema no parcheado a si permite bloquear la

máquina un ataque de tipo DOS por ejemplo, ganar acceso como usuario simple o root, se evalúa el ataque.

Contramedidas (*countermeasures*). Una vez detectado un ataque o un inicio de posible ataque nuestra capacidad de respuesta es otro factor a tener en cuenta y que pondera en la fórmula de aquí la importancia de IDS en tiempo real. Las contramedidas a aplicar pueden ser de sistema bloquear una cuenta de usuario parar un servicio temporalmente o incluso apagar la máquina o de red interceptar las comunicaciones desde una dirección determinada ajustar anchos de banda de entrada y salida de la red.

2.4.3. Sistema de prevención de intrusos (IPS)

Se define un sistema de prevención de intrusos como un dispositivo hardware o software que tiene la habilidad de detectar ataques tanto conocidos como desconocidos y reaccionar a esos para impedir su éxito. Los sistemas de prevención de intrusos pueden verse como la evolución de dos elementos que han dominados la seguridad en todas las redes:

- IDS: permite mantener el estado de las conexiones y examinar el contenido de los paquetes que circulan por nuestra red.
- *Firewall*: es el elemento que garantiza o bloquea el acceso a los recursos de nuestra red.

Los IPS pueden agruparse en cinco categorías dependiendo de su arquitectura y ubicación dentro de la red a proteger:

- *Inline IPS*. Estos sistemas de prevención de intrusos se caracterizan por colocarse entre la red y el ordenador a proteger.
 - La primera conectada a la red exterior y que no dispone de dirección IP. Su función es la de realizar *bridging* transparente entre la red y el IPS, al no disponer de dirección IP, este interface es totalmente invisible y no puede recibir ningún tipo de tráfico expreso (ni ser atacado).
 - La segunda tarjeta está conectada a la red segura o interna y nos permite que se conecte al sistema IPS para su gestión y configuración.

El sistema IPS procesa todo el tráfico entrante y saliente de manera que cada paquete puede pasar (*forward*), eliminarlo (*drop*), grabarlo en el log (*log*), borrarlo del log (*unlog*) o incluso rescribir el paquete eliminando elementos potencialmente peligrosos (*rewrite*).

- *Layerseven switches*. Los conmutadores o *switches* son dispositivos de capa 2 del modelo OSI. En el caso de las redes IP, los diferentes protocolos para los distintos servicios HTTP, FTP, SSH, se sitúan en la capa 7 del modelo OSI. De esta forma, para poder inspeccionar paquetes IP de diferentes servicios necesitamos un conmutador de nivel 7.

Estos IPS contienen un componente hardware muy importante que le proporciona una velocidad de proceso en el filtrado de paquetes de red muy superior a los sistemas convencionales basados en un programa que se ejecuta en un ordenador. Por otro lado, la flexibilidad de reconfiguración y nuevas

versiones de los IPS basados en programas queda sacrificada al ser un elemento hardware en su casi totalidad.

Su modo de funcionamiento se basa en un único puerto del *switch* encargado de mantener la conexión de red con el exterior, y el resto de puertos conectados a los distintos servidores a monitorizar.

Es capaz de filtrar el tráfico, buscar patrones en la red y controlar las conexiones de entrada y salida a los servidores. A diferencia de los sistemas basados únicamente en hardware, son capaces de controlar eficientemente el ancho de banda utilizado en cada uno de los servidores y variarlo en función de las necesidades de cada momento.

- *Application firewall / IDS*. Este grupo de IPS son programas autónomos que corren en cada uno de los servidores a proteger, se encargan de proteger únicamente un ordenador o servicio concreto y no una red o conjunto de ordenadores.

La sobrecarga de proceso que produce en el ordenador queda compensada por su gran capacidad de configuración, lo que permite que se centre únicamente en las partes o servicios que nos interese proteger.

La aplicación IPS se coloca entre el gestor de comunicaciones del sistema operativo y la aplicación, monitorizando todo el tráfico y efectuando todas las acciones que considere necesarias (*forward, drop, log, unlog, rewrite*) según la configuración creada o perfil.

- *Hybrid switches*. Estos sistemas de prevención de intrusos se basan en combinar una parte de software y otra de hardware.

La parte hardware es la encargada de filtrar el tráfico en tiempo real debido a su mayor velocidad de proceso, limitar el número de peticiones a los servidores y regular los anchos de banda de entrada y salida adecuándolos a las necesidades y demandas en cada momento.

La parte software se instala en cada uno de los servidores a monitorizar de forma que se crea un perfil específico para cada una de los servicios. Este componente se comunica con la parte hardware para conseguir un comportamiento más adecuado a las necesidades reales. Por otro lado, también realiza parte del filtrado para descargar el hardware.

- *Deceptive applications*: Se basa en una aproximación diferente y más proactiva frente a la detección de intrusos. Su aplicación se divide en tres fases.
 - En una primera fase se analiza todo el tráfico de la red para crear un modelo que represente todo el tráfico normal que circula por la red después se retoca el modelo manualmente por parte del administrador de la red de sistema para adecuarlo a la realidad de la red finalmente el sistema asignará unos pesos a cada uno de los distintos eventos que ha observado en el análisis.
 - En una segunda fase, el sistema monitoriza el tráfico y las peticiones que circulan por la red. Cuando observa peticiones a servicios que no existen o que no están disponibles, reacciona enviando como respuesta un paquete marcado simulando la existencia del servicio y anotando los parámetros de origen de la petición.

- La tercera fase se produce cuando el atacante utiliza los datos obtenidos en incursiones anteriores a la red para lanzar un ataque sobre servidores o servicios. En este momento el sistema reconoce al atacante y bloquea su acceso a la red.

2.4.4. Firewalls

La seguridad en redes más extendido ha sido únicamente el uso de un *firewall* que permite de una manera simple y eficaz aplicar filtros tanto para el tráfico de entrada como para el de salida en nuestra red. Se puede diferenciar entre dos políticas básicas de configuración de *firewalls*.

Permisividad máxima dónde el uso de filtros es mínimo o inexistente, esta política permite prácticamente la circulación de todo el tráfico y se utiliza principalmente en Intranets/LAN, campus universitarios y organizaciones dónde la libertad de uso de aplicaciones es necesaria para el funcionamiento ordinario de la red. Es una política que dificulta enormemente el uso de otros sistemas y deja a la red muy vulnerable prácticamente cualquier tipo de ataque interno o externo. En estos casos se recomienda segmentar la red en dominios y acotar cada uno de estos dominios, ya que raramente todos los ordenadores tienen que acceder a todos los recursos disponibles de la red.

Permisividad mínima en este caso se deniega acceso a todos los servicios de la red y se van permitiendo accesos a estos a medida que se necesiten, de esta forma es bastante improbable que se reciba un ataque a un servicio que se desconocía que se tiene en la red. El trabajo de otros sistemas se facilita enormemente ya que pueden configurarse para que detecten fácilmente cualquier comportamiento anómalo en la red simplemente se debe monitorizar los accesos a los servicios y comprobar si esos accesos están permitidos

destacar que el simple uso de un *firewall* puede crear una falsa sensación de seguridad de nada sirve si no son configurados y mantenidos al día aplicación de los parches del fabricante, supervisión y adaptación al tráfico de la red.

2.4.5. Falsos positivos y falsos negativos

Se ha analizado las diferentes partes que integran un esquema IDS. También se ha comentado los diferentes protocolos utilizados para conseguir la comunicación entre los distintos programas existentes, así como varias herramientas que se utilizan para la detección de los posibles incidentes firmas, reglas, correlaciones. Un punto básico a tratar tras el análisis de las muestras obtenidas eventos de interés de nuestra red es el de la detección de falsos positivos y falsos negativos.

- Un falso positivo: es un término aplicado a un fallo de detección en un sistema de alertas usualmente en sistemas antivirus o de detección de intrusos. Sucede cuando se detecta la presencia de un virus o una intrusión en el sistema que realmente no existe.
- Un falso negativo: es un término que hace referencia a un fallo en el sistema de alerta, sucede cuando un virus o una intrusión existen en nuestro sistema y es permitida (ignorada o no detectada) por el sistema de alerta.

Los falsos positivos pueden agruparse dependiendo de la naturaleza de su origen.

- *Reactionary Trafficalarms*. Se detecta un comportamiento sospechoso como consecuencia de tráfico generado anteriormente generalmente no

malicioso. Por ejemplo la detección de muchas respuestas *ICMP network unreachable* procedentes de un router porque el equipo destino no se encuentra operativo o accesible en esos momentos.

- *Equipment related alarms.* Las alarmas del NIDS detectan paquetes dentro del tráfico de la red que identifica como no usuales. Esto puede ocurrir por ejemplo con balanceadores de carga, puesto que generan paquetes específicos para el control de todos los nodos.
- *True False Positives.* Todos aquellos falsos positivos que no se encuadren en ninguna de las categorías anteriores.

El sistema de detección de intrusos debe producir los mínimos falsos positivos posibles y ningún falso negativo porque con uno sólo ya se tiene al intruso en nuestro sistema de red, y toda la inversión en seguridad se vuelve inútil y de difícil justificación.

Los falsos negativos son más complicados de encontrar, ya que implicaría que alguien consiguió un acceso no autorizado a una red segura y a nadie le hace gracia reconocer esto públicamente muchas veces no se reconoce ni en privado. Generalmente los falsos negativos suelen producirse por:

- Configuración deficiente de los recursos de la red: tener varios elementos de seguridad IDS, *firewalls*, VPN. No es suficiente para considerar nuestra red segura. Estos deben estar convenientemente configurados y adaptados a su medio el tráfico de las redes no es estático y varía.
- Ataques desde dentro: el uso de los recursos de nuestra red desde dentro. El atacante no siempre es un *hacker* de un país extraño que se

dedica a hacer el mal. Tener controles internos también permitirá detectar programas o troyanos encargados de facilitar acceso desde dentro a posibles atacantes.

2.4.6. Limitaciones de los IDS

Los IDS tienen un máximo de capacidad de proceso, por lo que en momentos de mucho tráfico suelen descartar los paquetes que no pueden procesar, los NIDS se basan en la observación del tráfico que circula por la red, esta única fuente de información le confiere una serie de limitaciones.

- Si alguien crea una puerta trasera o crea una red paralela en la intranet, probablemente los IDS no lo detectarán puesto que están pensados y configurados para el rango IP señalado.
- Si alguien se apropia de una cuenta y se autentica con el *login* y *password* correcto tampoco.
- Si los sensores que alimentan al IDS o el propio IDS no funciona, no se observa nada.

Es importante realizar un seguimiento periódico de la actividad de estos programas, ya que el hecho de tenerlos instalados o hacer un simple ping a la máquina para ver si está operativa no es una política de seguridad aceptable es conveniente calibrar periódicamente si el IDS es capaz de soportar realmente toda la carga de la red accesos a discos, swap, filtros muy complicados. No hay que olvidar que usualmente un IDS no es más que un programa que funciona en un ordenador.

Un IDS basado únicamente en la búsqueda de firmas al igual que muchos antivirus presenta dos grandes problemas:

- El número de firmas va aumentando cada año y tan sólo refleja los ataques que han sido ya identificados y analizados en los informes de ataques recibidos, siempre salen reflejados los mismos ataques que en el resto de Internet. Esto es debido a que los nuevos ataques aún no han sido detectados y documentados, con lo que no existe una firma a la que asociar el ataque recibido, lo que puede crear una falsa sensación de seguridad al ver que se detecta siempre los mismos ataques.
- En el caso de una red con cientos de ordenadores, todo y detectar ataques ya conocidos con nuestros IDS ¿se puede estar seguros que todos nuestros ordenadores son invulnerables a este ataque?

2.4.7. Arquitecturas de los NIDS

Según la aproximación utilizada para la monitorización del tráfico de la red, la arquitectura de los NIDS presenta funciones específicas, se tiene 3 grupos distintos de arquitectura:

- *Signature based* NIDS. Se basan en la búsqueda de patrones conocidos (firmas) en el tráfico de la red.
- *Anomaly based* NIDS. Se basan en analizar el tráfico de la red creando estadísticas y asignándoles pesos. Cuando se detecta tráfico sospechoso, se confronta con las estadísticas anteriores y en función del peso asignado y la cantidad de ocurrencias del evento se dispara una alarma o no.

- *Protocol modeling NIDS*. Estos sistemas de detección de intrusos buscan paquetes que contengan anomalías o configuraciones poco comunes de los protocolos de red, los datos van encapsulados en distintos datagramas de distintos protocolos.

Existen dos componentes básicos para cualquier sistema de detección de intrusos (IDS) que son los sensores y la consola.

- Los sensores (*sensors*) de un IDS son elementos pasivos que examinan todo el tráfico de su segmento de red en búsqueda de eventos de interés. Dependiendo del paradigma que utilicen para comunicarse con la consola del sistema detector de intrusos pueden clasificarse en dos grupos.
 - *Push*. Cuando se detecta un evento de interés el sensor crea un paquete de datos que envía a la consola. Un protocolo muy utilizado con este tipo de sensores es el *SNMP* que permite la definición de *traps* para el envío de información a un receptor la consola en este caso. Su principal inconveniente es que pueden ser observado por el atacante para descubrir cómo ha sido configurado y ante qué tipo de patrones reacciona, lo que permite establecer que patrones ignora el sensor y por tanto cuales emplear en un ataque.
 - *Pull*. Almacenan los eventos de interés hasta que la consola pregunta por ellos al sensor. Si se establece un protocolo de intercambio de mensajes cifrado y se pregunta regularmente a los sensores puede ofrecer un mecanismo eficaz de comunicación con la consola.

- La consola de un sistema de detección de intrusos, se encarga de recibir toda la información de los sensores de *pull* o *push* presentarla de forma entendedora al operador. Desde la consola se pueden configurar los distintos sensores así como emprender acciones en respuesta a los datos recibidos de los sensores.

2.4.7.1. Marco de detección de intrusión común (*Common Intrusion Detection Framework*) (CIDF)

Es la creación de interfaces de aplicaciones (API) y protocolos que permitan la comunicación entre los diferentes IDS de esta forma, simplemente define las funcionalidades genéricas deseadas y sus interconexiones. Los componentes principales son:

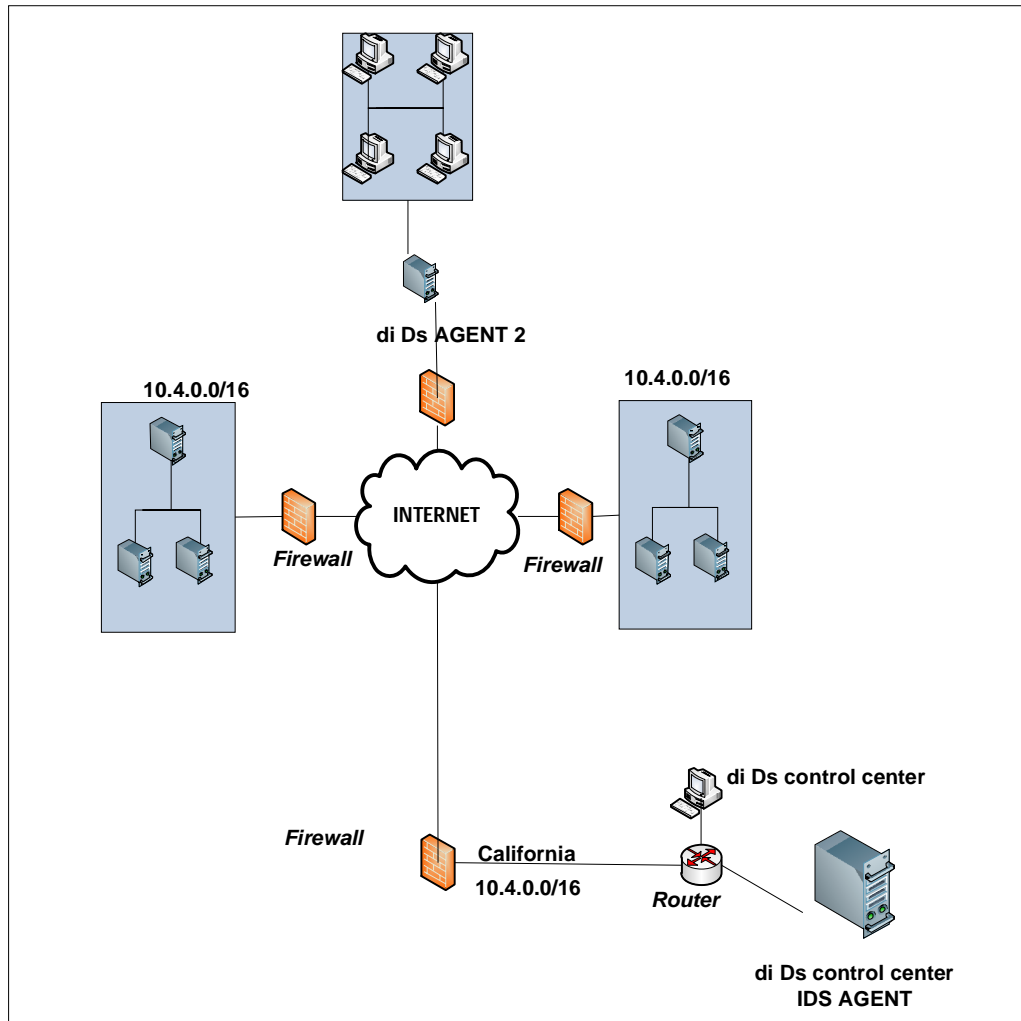
- *Event generator*. Describe la función de los sensores del sistema de detección de intrusos. Su función es recoger información de la red y generar informes alertas para la consola de monitorización.
- *Analysis*. Son las encargadas de procesar la información obtenida de los sensores y realizar su análisis. Se admite como ampliación de su funcionalidad la capacidad de realizar recomendaciones al operador e incluso de actuar proactivamente.
- *Database*. Simboliza la base de datos (o base de conocimiento) dónde se almacenan los informes, firmas y patrones detectados en la red por el IDS. Para mantener esta información es doble.

- *Response*. Este elemento es el encargado de proporcionar una respuesta ante los eventos obtenidos de los anteriores, así sugerir acciones al operador de consola bloquear el acceso desde una dirección IP, limitar el número de conexiones nuevas aceptadas por segundo.

2.4.7.2. Distributed Intrusion Detection System (DIDS)

En grandes organizaciones multinacionales o universidades dónde hay diferentes facultades, departamentos y laboratorios. Un único sistema IDS no proporciona la flexibilidad necesaria para la heterogeneidad de los elementos de que se dispone los sistemas DIDS (*Distributed Intrusion Detection System*) proporcionan este servicio de detección de intrusos para grandes redes. Su característica diferenciadora respecto a los sistemas NIDS tradiciones, es la presencia de dos elementos nuevos en su arquitectura, como se muestra en la figura 14.

Figura 14. Ejemplo de sistema DIDS



Fuente: Verdejo Álvarez Gabriel Seguridad en redes IP IDS. Capítulo 3.

- *Central Analysis Server.* Es el centro del sistema DIDS y es el encargado de recibir toda la información procedente de los agentes y realizar un repositorio común de conocimiento. También realiza las funciones de control y sincronización de los diferentes nodos que forman parte del sistema.

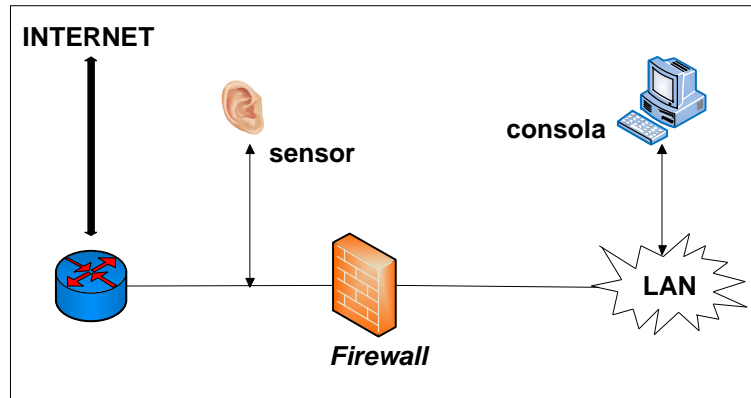
- *Cooperative Agent network*. Es un sistema autónomo encargado de la monitorización de una red. Detecta posibles incidentes e informa al servidor central para que comunique a todos los nodos el ataque detectado así como las contramedidas a realizar. Dependiendo de la implementación, el agente puede llegar a tomar contra medidas de forma autónoma aunque siempre informando al servidor central.

2.4.8. Ubicación de los NIDS

Una vez explicados los componentes básicos de un sistema IDS, se ha de decidir de qué tipo han de ser los distintos sensores que utilizará el NIDS (*pull o push*), finalmente se ha de concretar en qué lugar o lugares de la red deben colocarse:

Antes del *firewall* esta arquitectura se basa en detectar todos los paquetes que llegan a nuestra red antes de ser filtradas por el *firewall* se realiza una búsqueda de eventos de interés en todo el tráfico recibido sin interferencias de filtros del *firewall*, como se muestra en la figura 15.

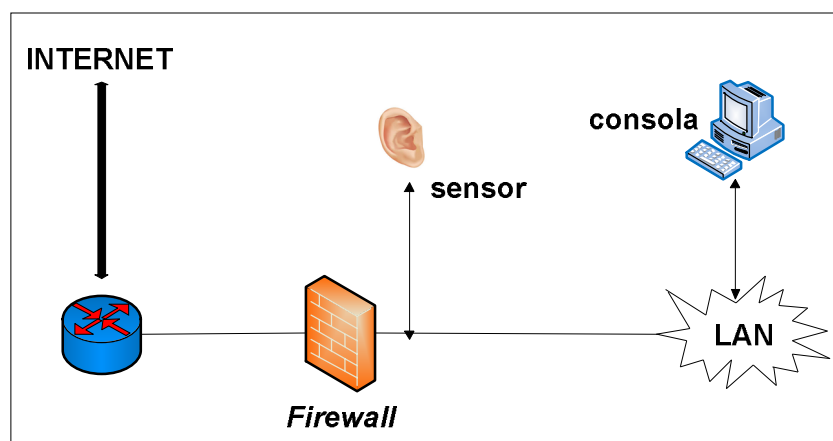
Figura 15. **Sensores antes del *firewall***



Fuente: Verdejo Álvarez Gabriel Seguridad en redes IP IDS. Capítulo 3.

- En el *firewall* o adyacente consiste en situar el sensor en el propio *firewall*, se evitan ataques de intrusos a los sensores externos y se eliminan muchos falsos positivos, ya que se procesa únicamente el tráfico que el *firewall* deja pasar, como se muestra en la figura 16.

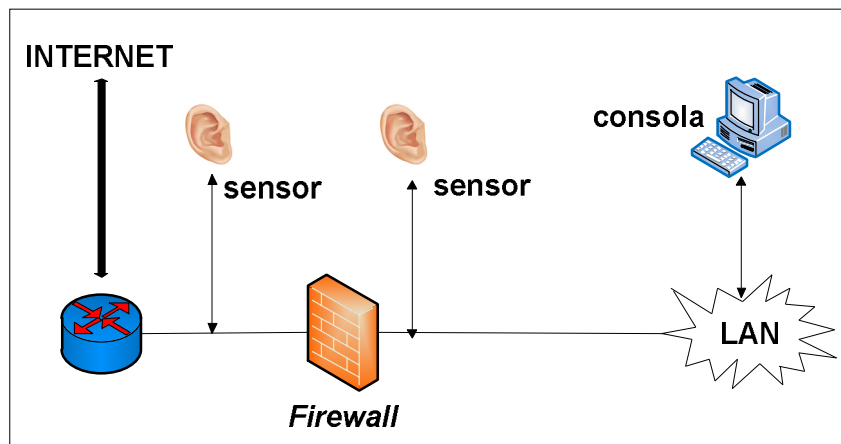
Figura 16. **Sensores en el *firewall***



Fuente: Verdejo Álvarez Gabriel Seguridad en redes IP IDS. Capítulo 3.

- Antes del *firewall* y en el *firewall* o adyacente es la opción es más costosa pero que ofrece mayor seguridad, se obtiene lecturas del tráfico total y del tráfico filtrado por el *firewall*, permite examinar la configuración del *firewall* y comprobar si filtra correctamente o no, como se muestra en la figura 17.

Figura 17. **Sensores antes y en el *firewall***



Fuente: Verdejo Álvarez Gabriel Seguridad en redes IP IDS. Capítulo 3.

2.4.9. **Protocolos de comunicación sensor-consola**

Cuando una compañía desarrolla un nuevo producto suele acompañarlo de un protocolo propietario encargado de gobernar las comunicaciones entre las diferentes partes del sistema de red. En los primeros productos o primeras versiones de sistemas de detección de intrusos esto ha sido una constante, lo que obligaba al usuario a depender de un único fabricante de producto.

Conforme se han ido extendiendo los productos IDS y el mercado ha ido creciendo, los usuarios y expertos demandaban la búsqueda de un lenguaje

protocolo común, ya que si simplemente se quiere compartir los datos con el propio ISP para mejorar la seguridad o detectar nuevas firmas de ataques desconocidos están obligados ambos a poseer el mismo producto.

Los ataques a redes de ordenadores se concentran en determinadas máquinas que sostienen los servicios vitales de la empresa o universidad servidores de ficheros o impresoras, servidores de nombres. Esto es debido a que muchos atacantes se nutren de listas de ordenadores denominadas listas de la compra (*shopping lists*) que contienen las direcciones IP de los servicios ofrecidos en cada red.

Poder compartir los datos obtenidos por el IDS con el de otras organizaciones u empresas puede evitar problemas en un futuro, usualmente los atacantes utilizan las mismas técnicas en las diferentes organizaciones obtenidas usualmente de listas de la compra con la esperanza de encontrar una que sea vulnerable al ataque perpetrado.

- *Raw Event Information.* Hace referencia a información básica obtenida directamente sin ningún tipo de post proceso. Principalmente tráfico de red y resultados de auditorías.
- *Analysis Results.* Descripciones de anomalías o ataques detectados.
- *Response prescriptions.* Conjunto de acciones de respuesta predefinidas para algunos comportamientos por ejemplo bloquear acceso desde una dirección IP si se detecta más de 1 000 conexiones por segundo procedente de ella.

2.4.10. Análisis de los datos obtenidos por sistemas NIDS

La cantidad de información debe ser almacenada de forma óptima para poder ser consultada ágilmente de otra forma dejará de ser utilizada. Sea cual sea el formato usado para el almacenamiento de la información debe cumplir las siguientes características:

- Debe realizar una reducción importante del volumen de datos pero conservando la información importante.
- Debe poseer un formato compacto, fácil de consultar, escribir y actualizar.
- Debe permitir la interrelación de todos los datos entre sí.

El formato *TCPQUAD* es una reducción compacta de la información contenida en los paquetes IP que se basa en almacenar una cuádruple tupla que contiene los siguientes campos (Fecha, Dirección origen, Dirección de destino, Tipo de protocolo).

Para almacenar los históricos de tráficos de red es doble, por un lado poder realizar informes y estadísticas sobre incidentes en nuestra red. Por otro lado se debe permitir conocer cuando un ataque presenta características similares o iguales a otro recibido anteriormente, ya que se puede obtener información de cómo reaccionar ante él de forma proactiva a tiempo, evitando ser sujetos pasivos y lamentarse posteriormente. De esta forma gran parte de las consultas a las bases de datos se basarán únicamente en buscar correlaciones entre los eventos de interés detectados y los datos históricos almacenados.

- Correlaciones por dirección de origen: se basan en encontrar similitudes entre conexiones provenientes de la misma fuente por ejemplo un escáner de puertos a nuestra red detectará que desde el mismo origen se realizan miles de peticiones a distintos puertos.
- Correlaciones por dirección de destino: considera las conexiones que tienen como destino la misma dirección IP por ejemplo un DOS. Se tiene miles de peticiones hacia un mismo destino.
- Correlaciones de firmas: se basan en buscar conexiones hacia un puerto determinado muchos virus y programas de *backdoor* basan su comunicación en puertos no *standards*. También se buscan configuraciones no *standards* de los distintos campos del paquete IP.
- Correlaciones de contenidos: estas correlaciones hacen referencia al contenido de datos de los distintos paquetes de información que circulan por la red. Buscar patrones como */etc/passwd* en conexiones TELNET o FTP, inspeccionar conexiones HTTP.

El sistema IDS debe permitir realizar estas consultas interactivamente al operador de la consola para investigar libremente en las bases de datos además deben realizarse de forma automática sólo para los eventos de interés de extrema criticidad. Existe una gran controversia sobre la cantidad de tiempo semanas, meses y años que se debe tener almacenada en la base de datos del IDS para poder realizar consultas tanto el operador como el propio sistema automáticamente lo deseable sería tener todo el histórico de la red sin embargo se debe tener en cuenta que:

- Más tiempo implica más espacio de disco crecimiento exponencial.
- Más tiempo implica una ralentización de las búsquedas pérdida de eficiencia.
- Más tiempo no implica necesariamente más seguridad.
- En caso de necesitar la informática forense nuestro histórico debe permitir la reconstrucción total los actos sucedidos en la red.
- También se debe tener en cuenta las leyes vigentes de protección de datos y almacenamiento de logs.

Por lo que una solución propuesta aboga por una ventana de al menos tres meses (90 días).

3. CRIPTOLOGÍA EN SEGURIDAD DE REDES DE TELECOMUNICACIONES

3.1. Historia

En el año 500 a.C, los griegos utilizaron un cilindro llamado *scytale* alrededor del cual enrollaban una tira de cuero. Al escribir un mensaje sobre el cuero y desenrollarlo se veía nuevamente en un cilindro de igual diámetro.

Durante el Imperio Romano Julio César empleó un sistema de cifrado consiste en sustituir la letra a encriptar por letra distanciada a tres posiciones más adelante. Durante se reinado, los mensajes de Julio César nunca fueron des encriptados. En el S. XII Roger Bacon y en el S. XV León Batista Alberti inventaron y publicaron algoritmos de encriptación basados en modificaciones del método de Julio César.

Durante la Segunda Guerra Mundial en un lugar llamado Bletchley Park (70 Km al norte de Londres) un grupo de científicos trabajaba en Enigma, la máquina encargada de cifrar los mensajes secretos alemanes. En este grupo se encontraban tres matemáticos polacos y un joven que había sido reclutado porque unos años antes había creado un ordenador binario.

Probablemente poca gente en los servicios secretos ingleses sabía lo que era un ordenador (y mucho menos binario), que sólo alguien realmente inteligente podía inventar algo así, cualquier cosa que eso fuese, era mucho más abstracto que todos sus antecesores y sólo utilizaba 0 y 1 como valores

posibles de las variables de su álgebra. Sería Turing el encargado de descifrar el primer mensaje de Enigma y cambiar el curso de la guerra, la historia y de la seguridad informática actual.

3.2. Criptografía

La palabra criptografía proviene etimológicamente del griego *Κρυπτοζ* (Kriptos– Oculto) y *Γραφειν* (Grafo–Escritura), que significa arte de escribir con clave secreta o de un modo enigmático. La criptografía hace años que dejó de ser un arte para convertirse en una técnica que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica. La criptografía es el fundamento de todas las tecnologías de seguridad de las redes.

La criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es mediante claves que sólo el emisor y el destinatario conocen, como se muestra en la figura 18.

Figura 18. **Criptograma**



Fuente: Borghello, Cristian Fabián. Seguridad Informática p. 171.

La importancia de la criptografía radica en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática, mantener la privacidad, integridad, autenticidad y hacer cumplir con el No rechazo, relacionado a no poder negar la autoría y recepción de un mensaje enviado.

3.3. Criptoanálisis

Es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.

Analiza los algoritmos criptográficos, con el fin de poder obtener el texto nativo a partir de un texto cifrado. Hay ciertos algoritmos simples que son fáciles de romper, sin embargo un buen algoritmo de encriptación sólo puede ser roto por medio de ataques de fuerza bruta o de diccionario.

El ataque de fuerza bruta consiste en probar cada posible clave sobre un fragmento de texto cifrado hasta que se obtenga un mensaje legible de texto nativo, el ataque de diccionario se basa en estudiar la naturaleza del algoritmo junto a algún conocimiento de las características generales del texto nativo con el fin de deducir un texto nativo concreto o encontrar la clave que se esté utilizando. Si la clave es descubierta, todos los mensajes cifrados con esta clave quedan seriamente amenazados.

3.4. Criptosistema

Es un método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado o criptograma, el proceso de transformar un texto en claro en texto cifrado se denomina cifrado y el proceso inverso, es decir la

transformación del texto cifrado en texto en claro, se denomina descifrado, ambos procesos son controlados por una o más claves criptográficas.

Un criptosistema se define como la quintupla (m,C,K,E,D) , donde:

- m : representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- C : representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- K : representa el conjunto de claves que se pueden emplear en el criptosistema.
- E : es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de C . Existe una transformación diferente E_K para cada valor posible de la clave K .
- D : es el conjunto de transformaciones de descifrado, análogo a E .

Todo criptosistema cumple la condición $D_K(E_K(m)) = m$ es decir, que si se tiene un mensaje m , se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m .

Existen 2 tipos fundamentales de criptosistemas utilizados para cifrar datos e información digital y ser enviados posteriormente después por medios de transmisión libre.

- Simétricos o de clave privada. Se emplea la misma clave K para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave. El mayor inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.
- Asimétricos o de llave pública. Se emplea una doble clave conocidas como K_p (clave privada) y K_P (clave pública). Una de ellas es utilizada para la transformación E de cifrado y la otra para el descifrado D . En muchos de los sistemas existentes estas claves son intercambiables, es decir que si se emplea una para cifrar se utiliza la otra para descifrar y viceversa.

Los sistemas asimétricos deben cumplir con la condición que la clave Pública (al ser conocida y sólo utilizada para cifrar) no debe permitir calcular la privada. Como puede observarse este sistema permite intercambiar claves en un canal inseguro de transmisión ya que lo único que se envía es la clave pública.

Los algoritmos asimétricos emplean claves de longitud mayor a los simétricos, por ejemplo suele considerarse segura una clave de 128 bits para estos últimos pero se recomienda claves de 1024 bits (como mínimo) para los algoritmos asimétricos. Esto permite que los algoritmos simétricos sean considerablemente más rápidos que los asimétricos.

En la práctica actualmente se emplea una combinación de ambos sistemas ya que los asimétricos son computacionalmente más costosos (mayor tiempo de cifrado). Para realizar dicha combinación se cifra el mensaje m con un sistema simétrico y luego se encripta la clave K utilizada en el

algoritmo simétrico generalmente más corta que el mensaje con un sistema asimétrico.

Después de estos criptosistemas modernos se puede encontrar otros no menos importantes utilizados desde siempre para cifrar mensajes de menos importancia o domésticos, que han ido perdiendo su eficacia por ser fácilmente criptoanalizables y por tanto reventables. Cada uno de los algoritmos clásicos descritos a continuación utiliza la misma clave K para cifrar y descifrar el mensaje.

3.4.1. Transposición

Son aquellos que alteran el orden de los caracteres dentro del mensaje a cifrar. El algoritmo de transposición más común consiste en colocar el texto en una tabla de n columnas. El texto cifrado serán los caracteres dados por columna (de arriba hacia abajo) con una clave K consistente en el orden en que se leen las columnas. Ejemplo: Si $n = 4$ columnas, la clave K es (4, 2, 3,1) y el mensaje a cifrar SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES, como se muestra en la tabla 5.

Tabla IV. **Transposición**

1	2	3	4
S	E	G	U
R	I	D	A
D		E	N
L	A	S	
R	E	D	E
S		D	E
	T	E	L
E	C	O	M
U	N	I	C
A	C	I	O
N	E	S	

Fuente: elaboración propia, con programa Microsoft Excel.

El mensaje cifrado será:

uan eelmco ei ae tcncegdesdeoiissrdlrs euan.

3.4.2. Cifrados mono alfabéticos

Sin desordenar los símbolos del lenguaje, se establece una correspondencia única para todos ellos en todo el mensaje. Es decir que si al carácter A le corresponde carácter D, esta correspondencia se mantiene durante todo el mensaje.

3.4.2.1. Algoritmo de César

Es uno de los algoritmos criptográficos más simples consiste en sumar 3 al número de orden de cada letra. De esta forma a la A le corresponde la D, a la B la E, y así sucesivamente. Puede observarse que este algoritmo ni siquiera posee clave, puesto que la transformación siempre es la misma. Obviamente,

para descifrar basta con restar 3 al número de orden de las letras del criptograma, el algoritmo de cifrado es:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Entonces el mensaje cifrado será:

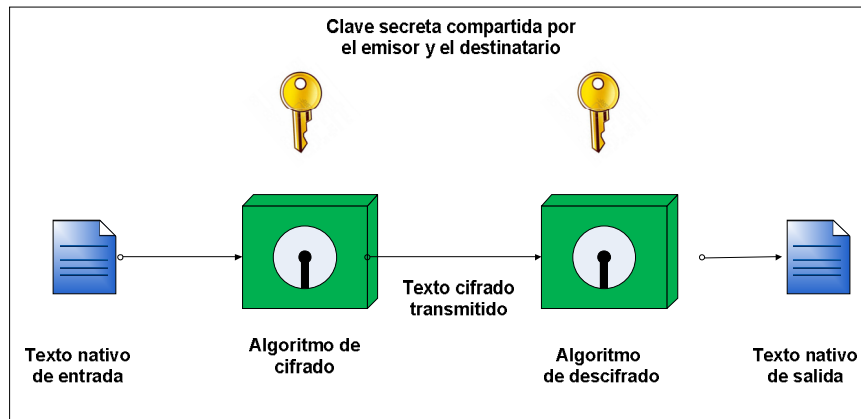
seguridad en las redes de telecomunicaciones
vhjxulgdg hq odv uhghv gh whohfrpxqlfdflrqhv

Es el caso general del algoritmo de César. El sistema consiste en sustituir cada letra por otra aleatoria. Esto supone un grado más de complejidad aunque como es de suponer las propiedades estadísticas del texto original se conservan en el criptograma y por lo tanto el sistema sigue siendo criptoanalizable.

3.5. Algoritmos simétricos modernos o llave privada

La técnica más utilizada para la privacidad a los datos transmitidos es el cifrado simétrico o de clave privada. En el cifrado simétrico, las entidades de comunicación establecen y comparten una clave secreta que se utiliza después para cifrar y descifrar los mensajes. Un esquema de cifrado simétrico tiene los siguientes elementos, como se muestra en la figura 19.

Figura 19. **Modelo de cifrado simétrico**



Fuente: González Morales Alexandro, Redes Privadas Virtuales p. 78.

- Texto nativo: es el mensaje original que va a ser cifrado y que constituye la entrada del algoritmo.
- Algoritmo de cifrado: es un algoritmo que realiza varias transformaciones del texto nativo en base a operaciones simples sobre patrones de bits.
- Clave secreta: es una entrada del algoritmo de cifrado. Los cambios que realice el algoritmo al texto nativo dependen de la clave.
- Texto cifrado: es el mensaje alterado que produce el algoritmo de cifrado. Claves diferentes producen cifrados diferentes para un mismo mensaje.
- Algoritmo de descifrado: es esencialmente el algoritmo de cifrado ejecutado inversamente.

Una clave es un código secreto que utiliza el algoritmo de encriptación para crear una única versión de texto cifrado. Mientras mayor sea la longitud de la clave, será más difícil averiguar, por ejemplo una clave de 56 bits puede proporcionar 256 diferentes combinaciones.

Los algoritmos de encriptación simétrica más importantes son los llamados cifradores de bloque. Un cifrador de bloque procesa una entrada de texto nativo en bloques de tamaño fijo y produce un texto cifrado de igual tamaño por cada bloque de texto nativo. Los principales algoritmos de este tipo son:

- Redes de feistel
- DES
- IDEA
- *BlowFish*

3.5.1. Redes de Feistel

Este algoritmo se basa en dividir un bloque de longitud n (generalmente el texto a cifrar) en dos mitades, L y R. Luego se define un cifrado de producto interactivo en el que la salida de cada ronda es la entrada de la siguiente.

3.5.2. Estándar de cifrado de datos (*Data Encryption Standard DES*)

Data Encryption Standard es el algoritmo simétrico más extendido mundialmente. Fue diseñado por la NSA (*National Security Agency*) para ser implementado en hardware, pero al extenderse su algoritmo se comenzó a implementar en software.

DES utiliza bloques de 64 bits, los cuales codifica empleando claves de 56 bits y aplicando permutaciones a nivel de bit en diferentes momentos (mediante tablas de permutaciones y operaciones XOR). Es una red de Feistel de 16 rondas, más dos permutaciones, una que se aplica al principio y otra al final. La flexibilidad de DES reside en que el mismo algoritmo puede ser utilizado tanto para cifrar como para descifrar, simplemente invirtiendo el orden de las 16 subclaves obtenidas a partir de la clave de cifrado.

En la actualidad no se ha podido romper el sistema DES criptoanalíticamente (deducir la clave simétrica a partir de la información interceptada). Sin embargo una empresa española sin fines de lucro llamado *Electronic Frontier Foundation* (EFF) construyó en Enero de 1999 una máquina capaz de probar las 2^{56} claves posibles en DES y romperlo sólo en tres días con fuerza bruta.

A pesar de su caída DES sigue siendo utilizado por su amplia extensión de las implementaciones vía hardware existentes en cajeros automáticos y señales de video, se evita tener que confiar en nuevas tecnologías no probadas. En vez de abandonar su utilización se prefiere suplantar a DES con lo que se conoce como cifrado múltiple, es decir aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave.

3.5.3. *International data encryption algorithm (IDEA)*

El *International Data Encryption Algorithm* fue desarrollado en Alemania trabaja con bloques de 64 bits de longitud empleando una clave de 128 bits y, como en el caso de DES, se utiliza el mismo algoritmo tanto para cifrar como para descifrar. El proceso de encriptación consiste ocho rondas de cifrado idéntico, excepto por las subclaves utilizadas (segmentos de 16 bits de los

128 de la clave), en donde se combinan diferentes operaciones matemáticas (XORs y Sumas Módulo 16) y una transformación final.

3.5.4. *Blowfish*

Este algoritmo fue desarrollado para la encriptación bloques de 64 bits y permite claves de encriptación de diversas longitudes hasta 448 bits.

Generalmente, utiliza valores decimales de π (aunque puede cambiarse a voluntad) para obtener las funciones de encriptación y desencriptación. Estas funciones emplean operaciones lógicas simples y presentes en cualquier procesador. Esto se traduce en un algoritmo liviano, que permite su implementación, vía hardware, en cualquier controlador.

3.5.5. Criptoanálisis de algoritmos simétricos

El Criptoanálisis comenzó a extenderse a partir de la aparición de DES por sospechas (nunca confirmadas) de que el algoritmo propuesto por la NSA contenía puertas traseras. Entre los ataques más potentes a la criptografía simétrica se encuentran:

- Criptoanálisis Diferencial. Ideado por Biham y Shamir en 1990, se basa en el estudio de dos textos codificados para estudiar las diferencias entre ambos mientras se los está codificando. Luego puede asignarse probabilidades a ciertas claves de cifrado.

- Criptoanálisis Lineal. Ideado por Mitsuru Matsui, se basa en tomar porciones del texto cifrado y porciones de otro texto plano y efectuar operaciones sobre ellos de forma tal de obtener probabilidades de aparición de ciertas claves.

Estos métodos, no han podido ser muy eficientes en la práctica. En el momento después de que un sistema criptográfico es publicado y se muestra inmune a estos dos tipos de ataques (y otros pocos) la mayor preocupación es la longitud de las claves.

3.6. Algoritmos asimétricos o llave privada pública

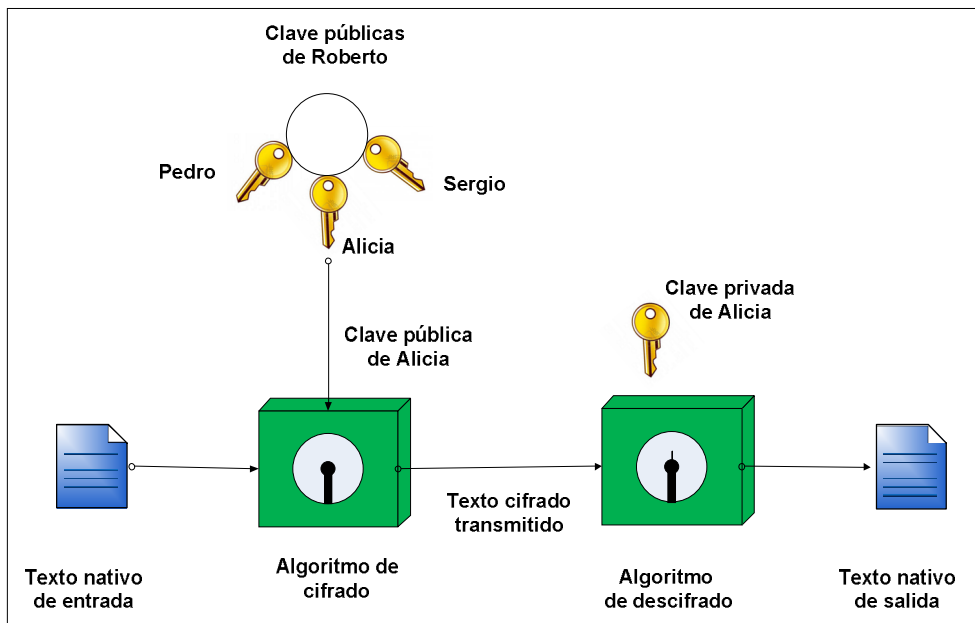
El cifrado asimétrico es un método donde cada usuario posee una pareja de claves relacionadas matemáticamente, donde se utiliza una clave para cifrar la información y la otra para descifrarla. Una de las claves se denomina clave pública, la cual puede darse a conocer ante todos los que quieran intercambiar información de forma segura con el usuario. La otra es la clave privada, la cual el usuario es dueño y no debe darla a conocer.

Estos algoritmos han demostrado su seguridad en comunicaciones inseguras como Internet. Su principal característica es que no se basa en una única clave sino en un par de ellas: una conocida (pública) y otra privada. Un esquema de cifrado asimétrico tiene los siguientes elementos:

- Texto nativo
- Algoritmo de cifrado
- Clave pública y privada
- Texto cifrado
- Algoritmo de descifrado

El procedimiento para cifrar mensajes utilizando claves públicas, como se muestra en la figura 20.

Figura 20. **Modelo de cifrado de clave pública**



Fuente: González Morales Alexandro, Redes Privadas Virtuales p. 80.

- Cada usuario genera un par de claves que van a ser utilizadas para el cifrado y descifrado de los mensajes.
- Cada usuario publica una de las dos claves de cifrado en un registro público. Esta clave se convierte en pública y la otra permanece privada. Cada usuario puede tener las claves públicas de todos los usuarios con los que mantiene comunicación.
- Si un usuario (Roberto) desea enviar un mensaje cifrado a otro (Alicia), él cifra el mensaje utilizando la clave pública de Alicia.

- Cuando Alicia recibe el mensaje, lo descifra utilizando su clave privada. Nadie más puede descifrar el mensaje, ya que solamente Alicia conoce su propia clave.

Así, todos los participantes tienen acceso a las claves públicas y cada uno de ellos genera localmente su propia clave privada. Mientras la clave privada permanezca en secreto, las comunicaciones serán seguras.

Los algoritmos de cifrado de clave pública más importante son el RSA y Diffie- Hellman.

3.6.1. RSA

Es un sistema de cifrado de llaves públicas que se usa tanto para cifrado de datos como para autenticación de llaves públicas. Fue inventado por Ronald Rivest, Adi Shamir y Leonard Adleman en 1977. De las iniciales del apellido de sus creadores RSA tomó su nombre.

Este algoritmo es el más empleado en la actualidad, sencillo de comprender e implementar, aunque la longitud de sus claves es bastante considerable (ha pasado desde sus 200 bits originales a 2048 actualmente).

Se emplean las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo, emplea la función exponencial discreta para cifrar y descifrar, y cuya inversa, el logaritmo discreto es muy difícil de calcular.

Los cálculos matemáticos de este algoritmo emplean un número denominado Módulo Público, N , que forma parte de la clave pública y que se

obtiene a partir de la multiplicación de dos números primos, p y q , diferentes y grandes (del orden de 512 bits) y que forman parte de la clave privada. La gran propiedad de RSA es que mientras que N es público, los valores de p y q se pueden mantener en secreto debido a la dificultad que entraña la factorización de un número grande.

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable.

El algoritmo RSA trabaja de la siguiente manera:

- Se toman dos números primos de gran tamaño, a los que se les llama p y q .
- Se calcula su producto $n=p*q$ y se le denomina módulo.
- Se escoge un número e , menor que n , y relativamente primo al producto $(p-1)*(q-1)$. Este valor es llamado el exponente público.
- Se encuentra otro número d tal que $(ed-1)$ es divisible por $(p-1)*(q-1)$. Este valor es llamado el exponente privado.
- La llave pública la conforman la pareja (n,e) .

- La llave privada la conforman la pareja (n,d) . Los factores p y q pueden ser destruidos o guardados junto con la llave privada.
- Una vez obtenidas las dos llaves se usan las siguientes fórmulas para encriptar y desencriptar el mensaje original:

Para encriptar:

$$c = m^e \text{ mod } n$$

Donde c es el mensaje encriptado y m el mensaje original

Para desencriptar:

$$m = c^d \text{ mod } n$$

La dificultad para poder obtener la llave privada a partir de la pareja (n,e) radica en el tamaño tan grande de los números primos p y q , que en la actualidad son del orden de los 512 a 1024 bits de tamaño. Cuanto más grande se escojan estos números mayor será el tiempo que se tome un intruso en calcular las llaves privadas de las partes que se comunican.

Observar el siguiente ejemplo: se escogen dos números primos⁹, $p=5$ y $q=11$. Se calcula el módulo $n = p*q = 5*11 = 55$. Se calcula e , tal que:

- $e < n$ y
- Relativamente primo¹⁰ a $(p-1)*(q-1) = (5-1)*(11-1) = 4*10 = 40$

Se escoge $e=3$, y se cumple que 3 es menor que $n=55$ y relativamente primo a 40, Se escoge d que cumpla con las condiciones dadas

anteriormente es decir que $ed-1$ sea divisible por $(p-1)*(q-1)$, para esto se puede aplicar la fórmula:

$$e*d \bmod [(p-1)*(q-1)] = 1$$

Se escoge entonces $d=27$, ya que:

$$3*27 \bmod [(5-1)*(11-1)] = 81 \bmod [(4)*(10)] = 81 \bmod [40] = 1$$

De lo anterior se concluye que la llave pública, es decir el par $(n,e) = (55,3)$ y la llave privada es el par $(n,d) = (55,27)$.

Ahora asúmase que A quiere enviar el mensaje 25 a B, para lo cual usa el par de la llave pública y la fórmula de cifrado dada anteriormente:

$$c = m^e \bmod n$$

$$c = 25^3 \bmod 55 = 5$$

$c=5$, es el número que se envía por el medio inseguro

En el otro lado B quiere recuperar el mensaje que le ha llegado, para lo cual usa la llave privada y la fórmula de descifrado dada anteriormente:

$$m = c^d \bmod n$$

$$m = 5^{27} \bmod 55 = 25$$

$m = 25$, el mensaje original enviado por A

3.6.1.1. Ataques a RSA

Si un atacante quiere recuperar la clave privada a partir de la pública debe obtener p y q a partir de N , lo cual actualmente es un problema intratable si los números primos son lo suficientemente grandes (alrededor de 200 dígitos).

Vale decir que nadie ha demostrado que no pueda existir un método que permita descifrar un mensaje sin usar la clave privada y sin factorizar N . El algoritmo es bastante seguro conceptualmente, existen algunos ataques que pueden ser efectivos al apoyarse sobre deficiencias en la implementación y uso del mismo. El ataque que con mayores probabilidades de éxito es el ataque de intermediario, que en realidad puede darse sobre cualquier algoritmo de clave pública. Supongamos:

Que A quiere establecer una comunicación con B, y que C quiere espiarla. Cuando A le solicite a B su clave pública K_B , C se interpone, obteniendo la clave de B y enviado a A una clave falsa K_C , creada por él. Cuando A codifique el mensaje, C lo intercepta de nuevo, lo decodifica con su clave propia y emplea K_B para codificarlo y enviarlo a B. ni A ni B sospecharán nunca de lo sucedido.

La única manera de evitar esto consiste en asegurar a A que la clave pública de B es auténtica. Para ello esta debería ser firmada por un amigo común como Autoridad Certificadora que certifique su autenticidad.

Otros ataques (como el de claves débiles, el de texto plano escogido, el de módulo común y el de exponente bajo) aprovechan vulnerabilidades específicas de algunas implementaciones.

3.6.2. Protocolo de acuerdo de llaves exponenciales (Diffie – Hellman)

El protocolo Diffie-Hellman también llamado (protocolo de acuerdo de llaves exponenciales), permite a dos usuarios intercambiar una llave secreta sobre un medio inseguro sin tener acuerdos preestablecidos.

Diffie-Hellman no se usa para encriptar datos, como se piensa generalmente. Se usa para intercambiar de forma segura las llaves que encriptan los datos. Esto lo logra generando un secreto compartido, también llamado llave de cifrado de la llave (*key encryption key* en inglés) entre las dos partes. Este secreto compartido luego encripta la llave simétrica (usando DES, 3DES, CAST, IDEA, Blowfish), que asegura la transmisión.

Los sistemas de llaves asimétricas (la base de la infraestructura de llaves públicas) usan dos llaves la llave privada y la llave pública desafortunadamente estos sistemas tornan lenta la transmisión de datos. Lo práctico hoy en día, es usar un sistema simétrico para encriptar los datos y un sistema asimétrico para cifrar las llaves a usar en el proceso de cifrado de los datos.

Cada lado de la comunicación tiene su llave privada y la llave pública del otro lado. *Diffie-Hellman* tiene la capacidad de generar llaves compartidas idénticamente iguales en ambos lados de la comunicación con la llave privada local y la llave pública del lado remoto.

Así trabaja el criptosistema de intercambio de llaves Diffie-Hellman:

- Se tienen dos parámetros públicos q y p , tal que ambos son primos y $p < q$.
- Dos partes quieren iniciar el cifrado de sus datos, y por lo tanto necesitan tener primero un secreto compartido, las dos partes son A y B.

- A genera una llave privada X_a , tal que X_a es un valor aleatorio, menor que q .
- B genera una llave privada X_b , tal que X_b es un valor aleatorio, menor que q .
- A genera su llave pública, Y_a , a partir de su llave privada X_a , con la siguiente fórmula: $Y_a = p^{X_a} \bmod q$
- De igual manera, B genera su llave pública, Y_b , a partir de su llave privada X_b , con la siguiente fórmula: $Y_b = p^{X_b} \bmod q$
- A y B intercambian sus llaves públicas, Y_a y Y_b , entre sí.
- Con Y_b en su poder, A está en capacidad de calcular el secreto compartido K , con la siguiente fórmula: $K = (Y_b)^{X_a} \bmod q$
- De igual manera, B puede calcular K , con Y_a en su poder:
 $K = (Y_a)^{X_b} \bmod q$

Observar el siguiente ejemplo: Carlos y Julián, necesitan un secreto compartido para iniciar su sesión de comunicación encriptada usando un sistema asimétrico. Los valores iniciales son:

- $q = 11$ y $p = 5$
- Carlos escoge su llave privada $X_c = 9$
- Julián escoge su llave privada $X_j = 3$
- Carlos calcula su llave pública $Y_c = p^{X_c} \bmod q$

$$Y_c = 5^9 \bmod 11 = 9$$

- Julián calcula su llave pública $Y_j = p^{x_j} \bmod q$
 $Y_j = 5^3 \bmod 11 = 4$
- Carlos le envía su llave pública Y_c a Julián, y Julián le envía su llave pública Y_j a Carlos. Ahora, Carlos calcula el secreto compartido
 $K = (Y_j)^{x_c} \bmod q$
 $K = 4^9 \bmod 11$
 $K = 3$
- Julián calcula el secreto compartido
 $K = (Y_c)^{x_j} \bmod q$
 $K = 9^3 \bmod 11$
 $K = 3$
Por tanto el secreto compartido es $K = 3$.

Una vez, cada lado de la comunicación tiene su secreto compartido idéntico al remoto, se inicia un proceso de cifrado de datos simétrico que es mucho más liviano que un mecanismo asimétrico, por tanto no disminuye sensitivamente la velocidad del enlace. Algunos algoritmos de cifrado simétricos son DES, 3DES, IDEA, CAST y Blowfish. Se tiene que hacer especial énfasis en el hecho que la llave compartida nunca se trasmite de un lado a otro, lo cual es muy importante.

El intercambio de llaves usando *Diffie-Hellman* es vulnerable a ataques tipo el hombre en la mitad, ya que el intruso podría interceptar la comunicación, hacerse pasar por el lado remoto y enviarle al emisor su llave pública haciéndose pasar por el receptor. La solución para evitar este

problema es usar firmas digitales que aseguren que la persona con la cual se está estableciendo la comunicación es efectivamente quien dice ser.

3.7. Autenticación

Se entiende por autenticación cualquier método que permita garantizar alguna característica sobre un objeto dado. Interesa comprobar la autenticación de:

- Un mensaje mediante una firma: se debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se lo conoce como Firma Digital y consiste en asegurar que el mensaje M proviene del emisor E y no de otro.
- Un usuario mediante una contraseña: se debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta.
- Un dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo una llave electrónica.

3.7.1. Funciones de dispersión unidireccionales (hash)

Las funciones de dispersión unidireccionales (*one-way hash function*), son muy utilizadas para la autenticación de datos, para la creación de firmas digitales y también son muy utilizadas por las tecnologías de autenticación de usuarios. Un conjunto de datos está autenticado si verdaderamente proviene del lugar de origen pretendido. La autenticación verifica que el mensaje sea auténtico y que no haya sido alterado.

Existen tres formas para autenticar un mensaje. La primera es utilizando cifrado simétrico. Si se supone que sólo el emisor y el receptor comparten la clave, se asegura la autenticación. El resumen del mensaje se puede cifrar usando cifrado de clave pública. Esto proporciona una firma digital, así como la autenticación de los mensajes y no requiere distribuir las claves a las partes que se comuniquen. La tercer forma es utilizando una función de dispersión.

Las funciones de dispersión operan sobre un mensaje de longitud variable y produce un resumen del mensaje de longitud fija (*hash signature*), estas funciones crean una huella digital electrónica única para un mensaje dado. Para autenticar un mensaje se envía con él un resumen del mensaje de forma que el resumen sea auténtico. Una función de dispersión tiene las siguientes propiedades y atributos:

- La función puede ser aplicada a un bloque de datos de cualquier tamaño.
- La función produce una salida de longitud fija.
- Para cualquier valor dado, es relativamente fácil calcular su función por lo que la función se puede implementar en software y hardware.
- La función es unidireccional porque es fácil generar un código dado un mensaje, pero prácticamente imposible generar un mensaje a partir de un código. De esta forma, el mensaje se mantiene secreto.
- No se puede encontrar un mensaje alternativo que produzca el mismo valor que un mensaje dado. Con esto se impide la falsificación de un mensaje.

- Una función de dispersión es fuerte si resiste un ataque llamado ataque del cumpleaños. Las funciones de dispersión más importantes son MD5 y SHA-1.
- Resumen de mensaje versión 5 (MD5, *Message Digest version 5*). Es un algoritmo de dispersión que autentica los datos de los paquetes. Este algoritmo toma un mensaje de longitud variable y produce un resumen del mensaje (hash) de 128 bits. MD5 es muy utilizado por IPSec para la autenticación de datos.
- Algoritmo de Dispersión Segura versión 1 (*SHA-1, Security Hash Algorithm*). Este algoritmo toma como entrada un mensaje con una longitud máxima de 264 bits y produce un resumen del mensaje (hash) de 160 bits. La entrada se procesa en bloques de 512 bits. IPSec y los certificados utilizan ampliamente SHA-1 para la autenticación y las firmas digitales.

3.7.2. Firma digital

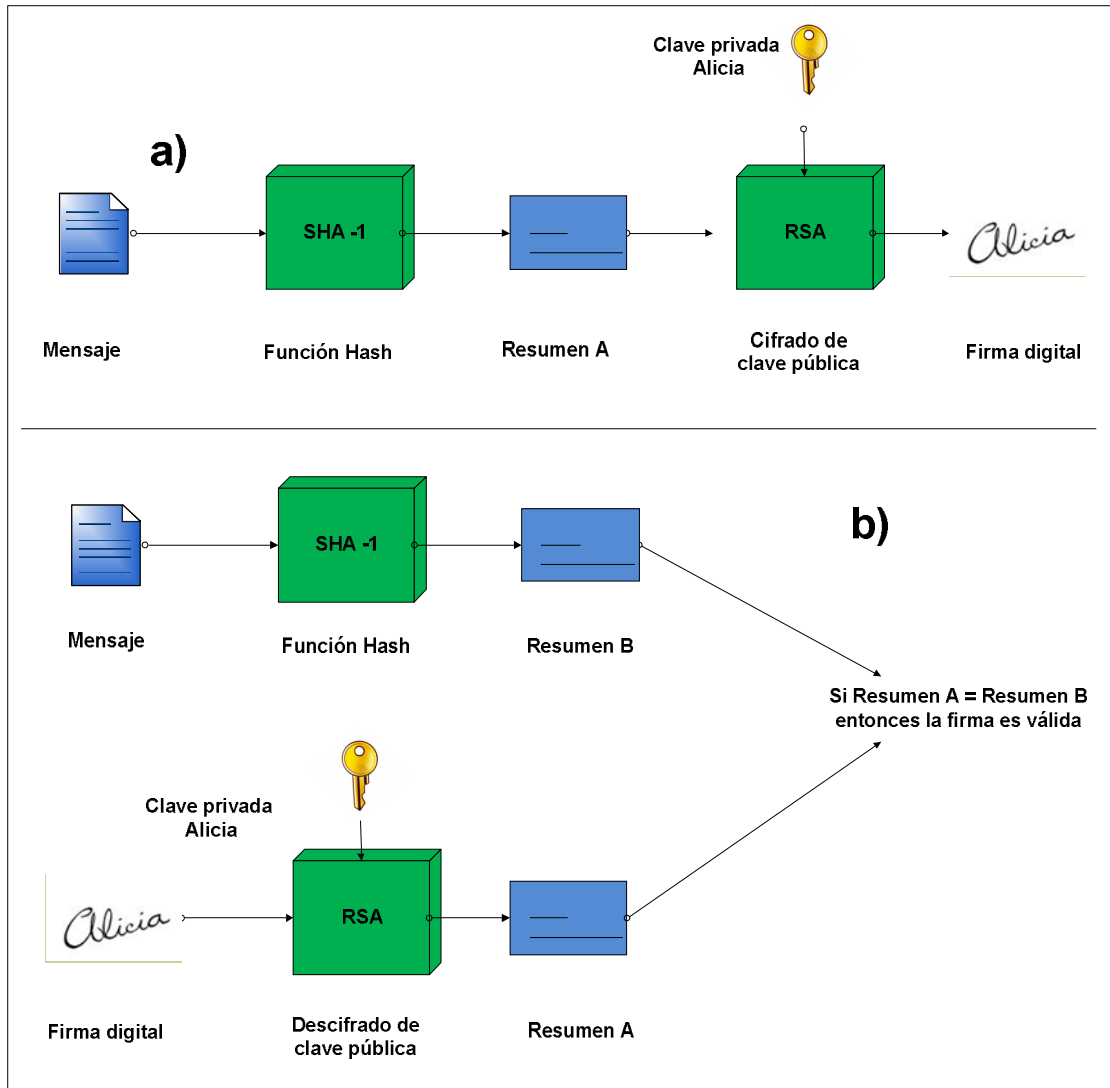
Una firma digital es utilizada con las claves públicas y se trata de un medio por el que los autores de un mensaje, archivo u otro tipo de información codificada digitalmente enlazan su identidad a la información. El proceso de firmar información digitalmente implica la transformación de la misma y de algunos datos secretos que guarda el remitente en una etiqueta denominada firma.

Una firma digital es el equivalente electrónico de una firma manuscrita y tiene el mismo propósito. Las firmas digitales no deben ser falsificables, los receptores deben ser capaces de verificarlas y los firmantes no deben

poder negarlas después. Una diferencia entre una firma manuscrita y una firma digital electrónica es que ésta última no debe ser constante y debe ser función de los datos que acompaña, de lo contrario una misma firma podría ser utilizada en cualquier mensaje y también se podría alterar cualquier mensaje firmado.

El cifrado de clave pública puede operar en conjunción con las funciones de dispersión unidireccionales para poder crear una firma digital el proceso de creación de una firma digital y la verificación de su autenticidad usando estas técnicas criptográficas, como se muestra en la figura 21.

Figura 21. Firma digital a) Creación b) Validación



Fuente: González Morales Alexandro, Redes Privadas Virtuales p. 84.

El inciso a) muestra la creación de la firma digital. Alicia crea la firma cifrando el resumen del mensaje producido por la función de dispersión usando su clave privada.

El inciso b) se muestra la validación de la firma. Cuando Alicia le envía un mensaje firmado a Roberto, éste lo valida comparando el resumen del mensaje que él genera localmente con el resumen obtenido al descifrar la firma usando la clave pública de Alicia. Si ambos resúmenes son exactamente iguales, entonces la firma es válida.

Es necesario tomar en cuenta que una firma digital no ofrece privacidad, ya que un mensaje firmado puede ser leído por cualquier persona. Incluso si se cifra el mensaje completo, cualquier intruso puede descifrar el mensaje utilizando la clave pública del autor. Lo único que hace la firma digital es demostrar que el mensaje pertenece al verdadero autor que lo creó.

Las funciones Hash están basadas en que un mensaje de longitud arbitraria se transforma en un mensaje de longitud constante dividiendo el mensaje en partes iguales, aplicando la función de transformación a cada parte y sumando todos los resultados obtenidos. Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor más utilizado.

4. SEGURIDAD DE VPN EN LAS REDES DE TELECOMUNICACIONES APLICADA A PEQUEÑAS Y MEDIANAS EMPRESAS

El concepto de VPN es una red que soporta transporte de datos privados sobre infraestructura IP pública por excelencia es Internet, la red de datos más pública que existe. De esta forma el término VPN se está aplicando cada vez más a las redes privadas que transportan datos utilizando Internet.

4.1. Definición de red privada virtual (VPN)

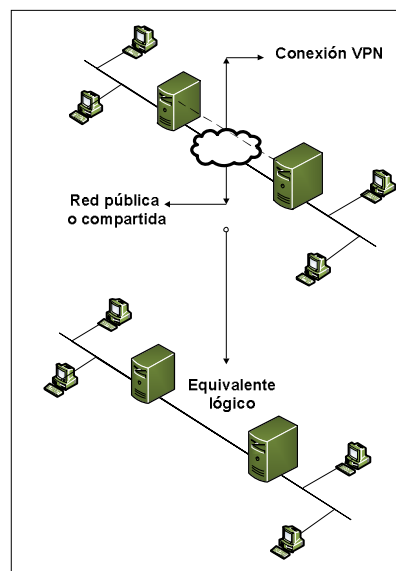
Los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos. Puesto que las redes públicas resultan ser mucho más económicas que las privadas se buscaron maneras de poder establecer una red privada dentro de una red pública. El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa. Se puede definir a una VPN de la siguiente.

Una Red Privada Virtual (VPN, *Virtual Private Network*) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Una VPN combina dos conceptos: redes virtuales y redes privadas.

- En una red virtual los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla. Un usuario de una red virtual no será capaz de detectar la red física, sólo podrá ver la red virtual. Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado, como se muestra en la figura 22.

Figura 22. **Una red virtual de VPN**



Fuente: González Morales, Alejandro. Funcionamiento de las VPN Capítulo 2.

- Las redes privadas son definidas como redes que pertenecen a una misma entidad administrativa. Un ejemplo típico de esta clase de red es una intranet corporativa, la cual puede ser utilizada sólo por

los usuarios autorizados. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual.

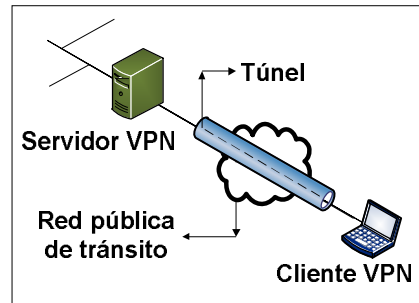
- Debido al hecho de ser una red privada que utiliza una red pública, la cuestión de la seguridad en una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones, en una red pública como Internet existen muchas personas malintencionadas que siempre están dispuestas a robar información. Es por eso que una VPN debe de poseer excelentes mecanismos de autenticación y de encriptación de la información para que ésta viaje segura a través de una red pública.

4.1.1. Componentes de una VPN

Los componentes básicos de una VPN, consisten hardware y software, son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener, como se muestra en la figura 23.

- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de tránsito
- Cliente VPN

Figura 23. **Componentes de una VPN**



Fuente: González Morales, Alejandro. Funcionamiento de las VPN Capítulo 2.

Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino. Para emular un vínculo privado los datos se cifran para asegurar la confidencialidad los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la cual los datos privados son encapsulados es conocida como túnel. La parte de la conexión en la que se encapsulan y cifran los datos privados se denomina conexión VPN.

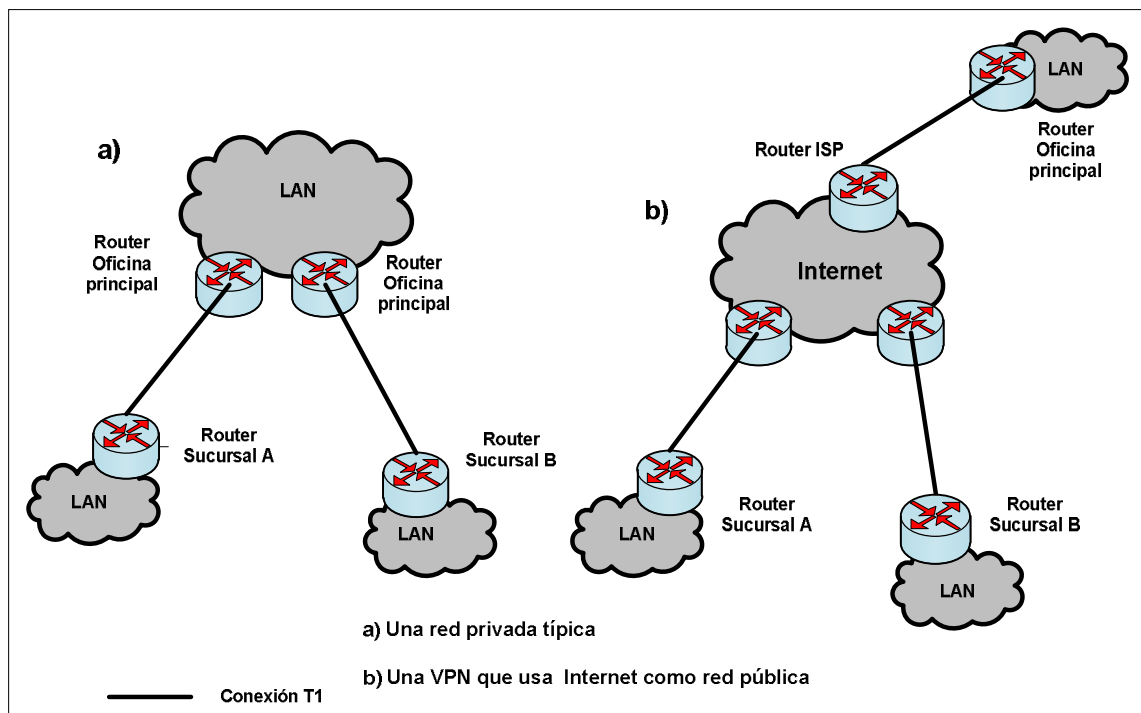
4.1.2. Utilizar Internet para crear una VPN

El uso de Internet como una VPN permitió a los usuarios remotos acceder a la red corporativa utilizando a un ISP. Puesto que ahora muchos ISP ofrecen acceso ilimitado a Internet por un precio accesible al mes, para conexiones de módem el uso de Internet puede proporcionar muchos beneficios económicos comparados con las tarifas de hacer llamadas de larga

distancia. La VPN es utilizada como un mecanismo para reemplazar redes privadas, también se pueden obtener bastantes beneficios económicos.

En el inciso a y b muestra a dos sucursales conectadas con la oficina corporativa, como se muestra en la figura 24.

Figura 24. El uso de Internet para crear una VPN



Fuente: González Morales, Alejandro. Funcionamiento de las VPN Capítulo 2.

4.2. Arquitectura de una VPN

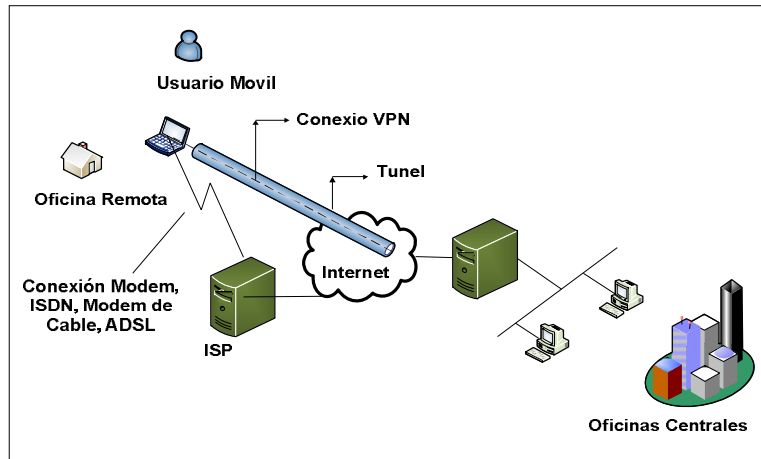
Existen básicamente 2 tipos de arquitectura para una VPN. La VPN de sitio a sitio, también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet. Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas.

- VPN de acceso remoto
- VPN de sitio a sitio

4.2.1. VPN de acceso remoto

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la organización siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre, como se muestra en la figura 25.

Figura 25. VPN de acceso remoto



Fuente: González Morales, Alexandro. Funcionamiento de las VPN Capítulo 2.

Las VPN de acceso remoto ahorran costos a las empresas ya que los usuarios sólo necesitan establecer una conexión con un ISP local, pagándose solamente la llamada local y olvidándose de realizar llamadas de larga distancia. El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa.

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

- VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. Aunque se trata de una conexión lenta es todavía muy común. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.

- VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad, tales como DSL y módem de cable las cuales ya ofrecen muchos ISP. Este tipo de VPN en la red se puede encontrar principalmente entre los tele trabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

4.2.2. VPN de sitio a sitio

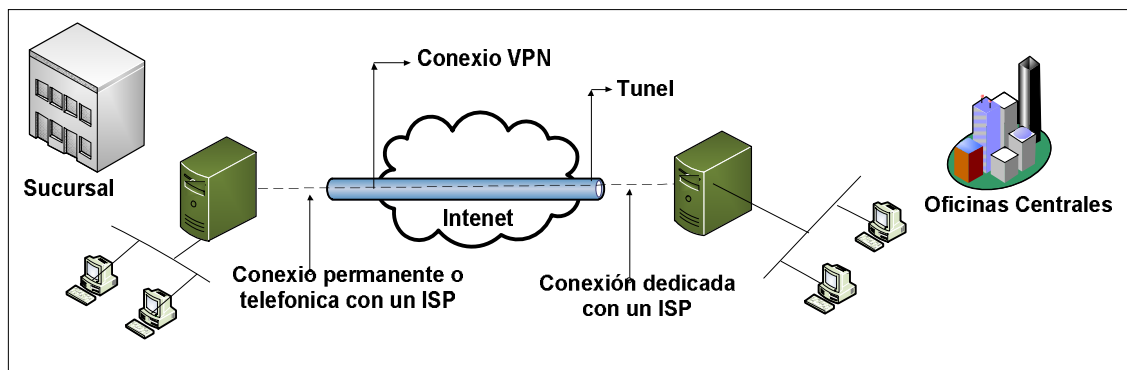
Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. En las redes tradicionales las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o Frame Relay. Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.

Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales.

La VPN de sitio a sitio puede dividirse a su vez en VPN intranet y VPN extranet.

- VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una organización, enlazan una oficina central con todas sus sucursales se disfrutan de las mismas normas que en cualquier red privada. Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN, como se muestra en la figura 26.

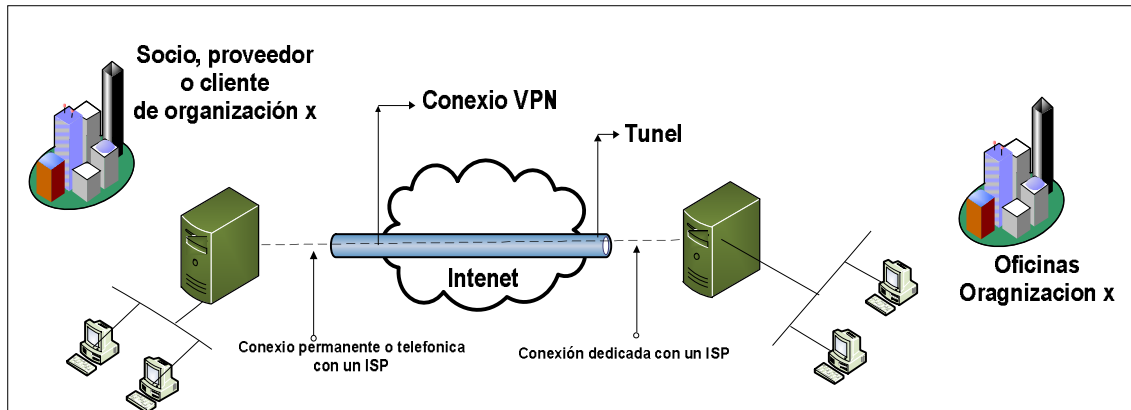
Figura 26. **VPN intranet**



Fuente: González Morales, Alexandro. Funcionamiento de las VPN Capítulo 2.

- VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa, se pueden implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Las amenazas a la seguridad en una extranet son mayores que en una Intranet, porlo que una VPN extranet debe ser cuidadosamente diseñada con muchas pólizas de control de acceso y acuerdos de seguridad entre los miembros de la extranet, como se muestra en la figura 27.

Figura 27. VPN extranet



Fuente: González Morales, Alejandro. Funcionamiento de las VPN p. 53.

4.3. Tipos de VPN

Existen diferentes formas de que una organización puede implementar una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más le convenga.

Los tipos diferentes de VPN son:

- VPN de *firewall*
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación
- VPN de proveedor de servicios

4.3.1. VPN de *firewall*

Un *firewall* llamado también cortafuegos o servidor de seguridad es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes. Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el *firewall* examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el *firewall* decide si lo permite o no. Además, el *firewall* examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un *firewall* puede ser un dispositivo software o hardware.

Es muy común que se utilice un *firewall* para proporcionar servicios VPN. Una VPN basada en *firewall* tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad.

Entre los inconvenientes se puede mencionar que tener la VPN en un *firewall* convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red.

Otra desventaja ocurre debido a que tener *firewall* y VPN juntos, se ejerce presión al rendimiento del *firewall*. Esto ocurre principalmente cuando se tienen conectados cientos o incluso miles de usuarios.

4.3.2. VPN de router y de concentrador

Es la VPN integrados dentro de un router o un dispositivo llamado concentrador VPN. Tanto el router como el concentrador VPN, están especialmente diseñado para las conexiones VPN sitio a sitio y acceso remoto. Cuenta con las tecnologías VPN más importantes y los métodos de autenticación y cifrado para proteger los datos transmitidos.

Este dispositivo está especialmente diseñado para las VPN, por lo que se trata de la solución VPN más rápida. Resulta ser más fácil agregarles tarjetas con el fin de incrementar el rendimiento. Dependiendo de la implementación, estas VPN pueden configurarse para utilizar certificados, servicios de autenticación externos o claves de seguridad.

4.3.3. VPN de sistema operativo

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,...) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios de servidor Web, de nombres de dominio, acceso remoto, VPN y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto.

4.3.4. VPN de aplicación

Una VPN de aplicación es un programa que añade posibilidades VPN a un Sistema operativo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

4.3.5. VPN de proveedor de servicios

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como FrameRelay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.

El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser FrameRelay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, *Service Level Agreements*). Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.

4.4. Topologías de VPN

La topología VPN que necesita una organización debe decidirse en función de los problemas que va a resolver. Una misma topología puede ofrecer distintas soluciones en diferentes organizaciones. En una VPN se puede encontrar las siguientes topologías:

Para las VPN de sitio a sitio:

- Topología radial
- Topología de malla completa o parcial
- Topología híbrida

Para las VPN de acceso remoto:

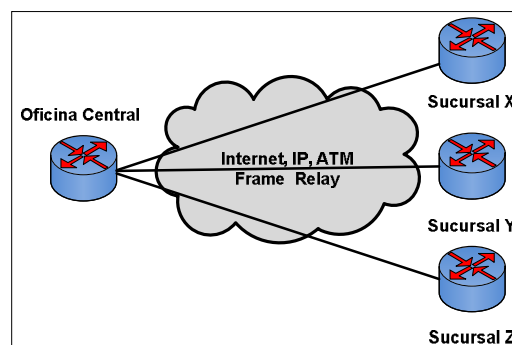
- Topología de acceso remoto

En las VPN basadas en ATM y *Frame Relay*, los enlaces que conectan las oficinas centrales con sus sucursales son circuitos virtuales (VC), mientras que en las VPN basadas en IP como Internet, estos enlaces son los túneles que se establecen a través de Internet.

4.4.1. Topología radial

En una VPN de sitio a sitio, esta es la topología más común, las sucursales remotas se conectan a un sitio central, las sucursales podrían intercambiar datos entre ellas, este tipo de datos resulta ser muy insignificante. La mayor parte del intercambio de datos se da con las oficinas centrales de la compañía. Los datos intercambiados entre las sucursales siempre viajan a través del sitio central, como se muestra en la figura 28.

Figura 28. Topología radial

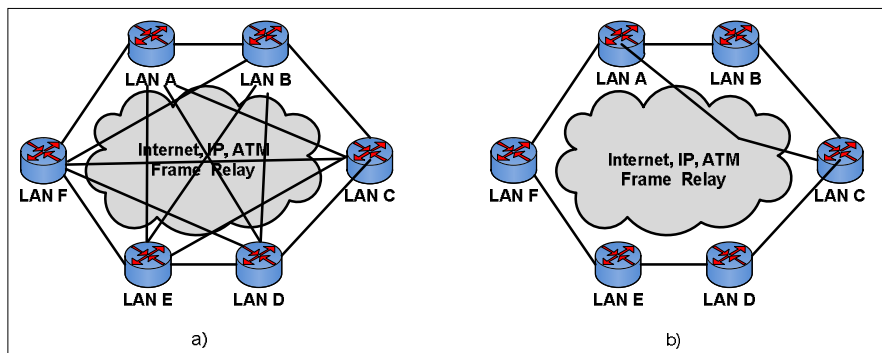


Fuente: González Morales, Alejandro. Funcionamiento de las VPN p. 58.

4.4.2. Topología de malla completa o parcial

Esta topología es implementada en corporaciones que no tienen una estructura demasiado jerárquica. Las diversas LAN de la compañía pueden realizar un intercambio constante de datos entre ellas. Dependiendo de sus necesidades, una organización de empresa puede utilizar una topología de malla completa si todas las LAN se comunican entre sí o una topología de malla parcial, si sólo algunas LAN mantienen intercambio de datos. En la gran mayoría de los casos se utiliza sólo malla parcial, como se muestra en la figura 29.

Figura 29. Topología de malla: a) completa b) parcial



Fuente: González Morales, Alejandro. Funcionamiento de las VPN p. 58.

4.4.3. Topología híbrida

Las redes VPN grandes combinan la topología radial con la topología de malla parcial, una organización de una empresa multinacional podría tener acceso a redes implementadas en cada país con una topología radial, mientras que la red principal internacional estaría implementada con una tecnología de malla parcial.

4.4.4. Topología de acceso remoto

Esta topología consiste en un enlace punto a punto entre el usuario remoto y la oficina central utilizando tramas *tunneling* PPP intercambiadas entre el usuario remoto y el servidor VPN. El usuario y el servidor establecen conectividad usando un protocolo de capa 3, siendo el más común IP, sobre el enlace PPP entunelado e intercambian paquetes de datos.

4.5. Requerimientos de una VPN

Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda

4.5.1. Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí

misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, *Public Key Infrastructure*), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se autentica intercambiando los certificados de cada uno, los cuales están garantizados por una autoridad de certificación (CA, *Certification Authority*) en la que todos confían.

El proceso de autenticación también involucra el intercambio de información secreta, como una clave o un desafío ante un Servidor de Acceso a Red (NAS, *Network Access Server*), el cual consultará a un servidor RADIUS administra la autenticación en una red que lo requiere.

4.5.2. Control de acceso

El control de acceso en una red está definido como el conjunto de pólizas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de *firewalls*, sistemas operativos; son responsables de gestionar el estado de la conexión del usuario. La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

El conjunto de reglas y acciones que definen el control de acceso se denomina póliza de control de acceso. Un servidor RADIUS (*RADIUS, Remote*

Authentication Dial In User Service), que es el Servicio de Usuario de Marcación para Autenticación Remota es un estándar para un sistema de autenticación de acceso remoto. Puede administrar el control de acceso basándose en la póliza, una regla de control de acceso sería que el servidor permitiera el acceso sólo los usuarios de acceso remoto que no han rebasado un determinado uso de horas de la red.

El principal propósito de una VPN es permitir acceso seguro y selectivo a los recursos de una red. Con un buen sistema de cifrado y autenticación pero sin control de acceso, la VPN sólo protege la integridad del tráfico transmitido y evita que usuarios no autorizados ingresen a la red, pero los recursos de ésta no quedan protegidos. Es por eso que el control de acceso es importante.

4.5.3. Administración de direcciones

Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el *tunneling* es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. El contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet. Existen muchas tecnologías de *tunneling*, cada una de ellas con sus ventajas y desventajas, otra

tecnología alterna al *tunneling* es *MPLS*, donde se hace uso de un sistema de etiquetas para transmitir información.

4.5.4. Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información. El cifrado es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. El texto sin cifrar se le denomina texto nativo, mientras que el texto cifrado se le denomina texto cifrado. Antes de enviar la información el servidor VPN cifra la información convirtiéndolo en texto cifrado. El receptor de la información descifra la información y la convierte en texto nativo.

Al principio los algoritmos de encriptación se mantenían en secreto. Sin embargo, cuando el algoritmo era roto, toda la información protegida con dicho algoritmo se volvía vulnerable, actualmente los algoritmos se hacen públicos. Existen muchos tipos de algoritmos de cifrado muy fuertes utilizados en las VPN entre los que se pueden encontrar 3DES, *Diffie-Hellman*, MD5, RSA y SHA-1.

Puesto que el algoritmo de cifrado es conocido por todos, es necesario implementar técnicas para poder mantener los datos seguros. Esto se logra mediante el uso de claves.

Una clave es un código secreto que el algoritmo de encriptación utiliza para crear una única versión de texto cifrado. Mientras la longitud en bits de esta clave sea más grande, más difícil será descifrar una información. Las VPN requieren del uso de claves con una cierta longitud, de tal

manera que resulta prácticamente imposible descifrar los datos (teóricamente tardarían muchos años, a no ser que se posean cientos de procesadores trabajando al mismo tiempo para encontrar la clave y aunque ésta se encontrara, los algoritmos están diseñados de forma que no se garantizaría totalmente el éxito).

El uso de claves muy largas no es recomendable porque se afecta mucho el rendimiento de un procesador. Para eso se utilizan métodos como el uso de claves simétricas y asimétricas.

Con una clave simétrica, se usa la misma clave para cifrar y descifrar la información que viaja por un túnel. Tanto el emisor como el receptor de los datos poseen la misma clave privada. Con una clave asimétrica, la información se cifra con una clave y se descifra con otra diferente. Una de las claves sólo es conocida por el usuario, la cual es conocida como clave privada. La otra clave es conocida por todos y se le llama clave pública.

Las claves públicas permiten el uso de firmas digitales para autenticar información. Una clave pública es distribuida libremente a cualquiera que requiera enviar información cifrada o firmada. La clave privada debe ser bien resguardada por el usuario y no darla a conocer nunca.

4.5.5. Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado con su clave privada. Un usuario que

utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable.

En una VPN pequeña no es muy necesario establecer una infraestructura de administración de claves. Sin embargo, las grandes compañías obtendrán muchos beneficios si hacen crear una Infraestructura de Claves Públicas (PKI) para poder crear y distribuir certificados. Una corporación puede crear su propia CA o confiar en una CA de terceros. Una PKI es muy útil en aquellas organizaciones que requieren de mucha seguridad y acceso limitado a sus usuarios.

4.5.6. Ancho de banda

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente. Dicho concepto es la Calidad de Servicio, La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda. La calidad del servicio también se refiere al número de conexiones simultáneas (la cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio central) que puede soportar una VPN y la forma como ésta afecta al rendimiento de la VPN.

Es preciso también asegurarse que una VPN puede cifrar y descifrar los paquetes transmitidos a una velocidad adecuada, ya que algunos algoritmos de cifrado son lentos y si no se tiene un buen procesador el rendimiento se verá afectado. Es importante mencionar que el valor nominal de velocidad de los dispositivos de redes (por ejemplo 100 Mbps) nunca se cumple en la

realidad y que eso habrá que tomarse en cuenta a la hora de implementar una VPN Para una organización.

La calidad de las conexiones a Internet también es importante las técnicas de encriptación que incrementan el deterioro del rendimiento de la comunicación por las sobrecargas. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afecta más al rendimiento, que la carga añadida por la encriptación.

4.6. Túnel (*Tunneling*)

El *tunneling* es un método utilizado para encapsular paquetes (conocidos como datos de usuario) dentro de otros paquetes los cuales son enviados utilizando la tecnología de la red por la que viaja. Esto ofrece grandes ventajas, ya que permite el transporte de protocolos con diferente esquema de direccionamiento y que por lo tanto no son compatibles con una red que utiliza otros protocolos de direccionamiento dentro de paquetes que sí reconoce la red.

4.6.1. Funcionamiento del *tunneling*

Un paquete IPX o *AppleTalk* no puede ser transportado en una red basada en IP, como Internet. Sin embargo, si este paquete es encapsulado dentro de un paquete IP, entonces podrá ser transportado como cualquier otro paquete IP. Lo que hace este proceso es simplemente agregarles un encabezado adicional.

Después de agregar el encabezado, se envía el paquete encapsulado a través de una ruta lógica denominada túnel. El túnel es la ruta de información

lógica a través de la cual viajan los paquetes encapsulados. Para los interlocutores de origen y de destino originales, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. A estos puntos que están en cada extremo del túnel se les denomina interfaces de túnel. Los interlocutores desconocen los *routers*, *switches*, servidores proxy u otras puertas de enlace de seguridad que pueda haber entre los extremos del túnel.

Cuando el paquete llega a su destino, éste es desencapsulado para que pueda ser utilizado. El *tunneling* es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación. El túnel envuelve o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes observen el tráfico en la red. De los paquetes encapsulados llegan a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final.

4.6.2. Protocolo pasajero, encapsulador y portador

El proceso de *tunneling*, involucra 3 protocolos diferentes el protocolo pasajero, encapsulador y portador, para la seguridad en las redes de telecomunicaciones que brinda la protección de la información.

- Protocolo pasajero: representa el protocolo que debe encapsularse. Como ejemplos de protocolos pasajeros tenemos PPP y SLIP.
- Protocolo de encapsulamiento: es el que será empleado para la creación, mantenimiento y destrucción del túnel. Ejemplos de protocolo de encapsulamiento son L2F, L2TP, PPTP.
- Protocolo portador: es el encargado de realizar el transporte del protocolo de encapsulamiento. El principal ejemplo de protocolo portador es IP puesto que este tiene amplias capacidades de direccionamiento y es en el que está basado Internet.

4.6.3. Tunneling y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el *tunneling* para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el *tunneling* involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del *tunneling* pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual. Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como Internet.

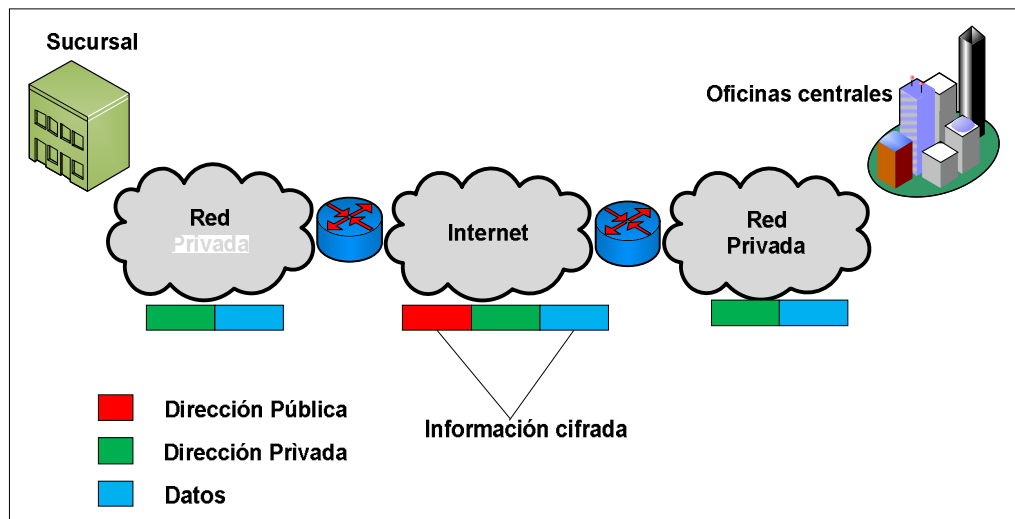
Puesto que los contenidos del paquete entunelado sólo pueden ser interpretados por las interfaces de túnel, las direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del paquete permanecen protegidos de acceso no autorizado. Además, el *tunneling* opcionalmente puede proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Tres protocolos de túnel son los más usados para la creación de una VPN:

- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio, como se muestra en la figura 30 .

Figura 30. **Tunneling en un VPN**



Fuente: González Morales, Alexandro. Funcionamiento de las VPN p. 68.

4.6.4. Tipos de túneles

Los túneles se clasifican de acuerdo a cómo se establece la conexión entre 2 *hosts*. En base a esto, existen dos tipos de túneles en la VPN en las redes de telecomunicaciones. Éstos son:

- Túnel voluntario
- Túnel obligatorio

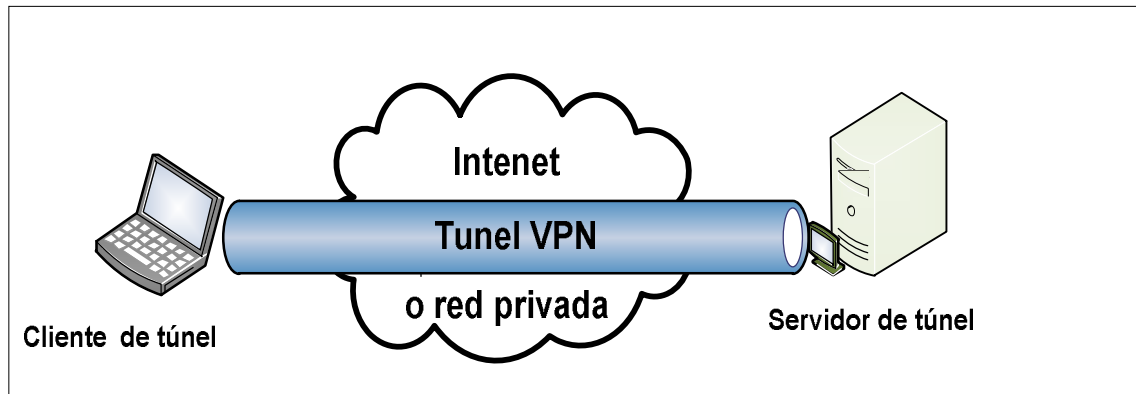
4.6.4.1. Túnel voluntario

Un usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario, el usuario está un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un *router* utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalarse el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión dial-up o a través de una LAN.

A través de una conexión *dial-up*, en este caso el usuario primero hace una llamada a su ISP para conectarse a Internet y entonces posteriormente podrá ser creado el túnel. La conexión a Internet es un paso preliminar para crear el túnel pero no forma parte del proceso de creación del túnel.

A través de una LAN, en este caso el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN. Como se muestra en la figura 31.

Figura 31. **Túnel voluntario**



Fuente: González Morales, Alexandro. Funcionamiento de las VPN p. 69.

4.6.4.2. **Túnel obligatorio**

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (*gateway*) de Seguridad IP en IPSec. Para realizar su función, el dispositivo que proporciona el túnel debe tener

instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión.

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizar el túnel creado por el dispositivo que proporciona el túnel. Una vez que se realiza la conexión inicial, todo el tráfico de la red y el cliente se envía automáticamente a través del túnel.

En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente se conecta en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un el dispositivo que proporciona el túnel para hacer un túnel a todos los clientes hacia un servidor específico del túnel. De manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

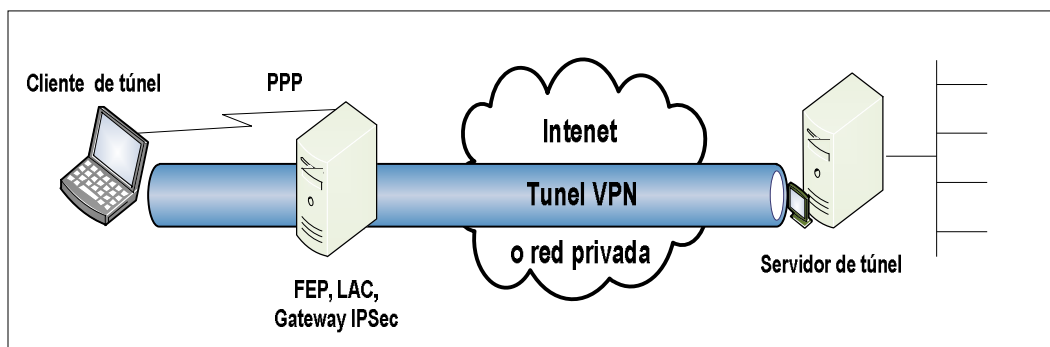
A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

Una organización puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la organización. Estos dispositivos pueden establecer

túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización. Existen dos formas de crear túneles obligatorios.

- En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel.
- En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso, como se muestra en la figura 32.

Figura 32. Túnel obligatorio



Fuente: González Morales, Alexandro. Funcionamiento de las VPN p. 71.

4.7. Seguridad en una VPN

Cuando se diseñaron los primeros protocolos para redes, la seguridad no era un punto importante puesto que las redes sólo eran utilizadas por universidades e investigadores. Nadie pensaba en que alguien pudiera

interceptar mensajes. Sin embargo, conforme las redes pasaron a tener un propósito comercial cuando las empresas las adoptaron y con la llegada de Internet, la seguridad pasó a ser una cuestión de vital importancia al momento de implementar redes.

Con la llegada de Internet, toda computadora conectada es susceptible de ser atacada por personas que no deben ingresar a ellas los ataques a redes provocan muchas pérdidas económicas a las empresas, la seguridad cobra especial importancia al momento de implementar una VPN. Puesto que la información privada de una organización atraviesa una red pública, es necesario proveer a la VPN de mecanismos que aseguren la confidencialidad y la integridad de los datos transmitidos y también para evitar el acceso a la red privada.

La seguridad de una VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de una red. También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una VPN. Es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red de la organización corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general.

La autenticación de usuarios y la encriptación de datos son características de seguridad muy fuertes. Y en una VPN la tecnología que podrá ofrecer mejor seguridad será IPSec.

4.7.1. Clasificación de las amenazas a redes

La amenaza de la seguridad de las redes de VPN, se clasificación en 4 posibles amenazas a la seguridad de las redes de telecomunicaciones las cuales son descritas a continuación.

- Amenazas no estructuradas. Esta clase de amenazas suelen ser originadas por personas inexpertas que utilizan herramientas de piratería en Internet. Aunque algunos actúan de forma malintencionada, la gran mayoría de ellos lo hace por puro reto intelectual. Se les conoce comúnmente como script kiddies.
- Amenazas estructuradas. Estas amenazas son causadas por personas que sí tienen conocimientos de redes. Saben cómo están constituidas y conocen sus puntos débiles. Como conocen mucho de programación pueden crear programas que penetren en los sistemas. Son conocidos como *hackers* y si tienen malas intenciones se les llama *crackers*. Estas personas pueden ser contratadas por el crimen organizado para cometer robos y fraudes, por una empresa para dañar a la competencia o por agencias de inteligencia con el fin de desestabilizar un gobierno enemigo.
- Amenazas externas. Son las amenazas causadas por personas ajenas a la red de una empresa. Son personas no autorizadas a ingresar a estos sistemas, pero pueden entrar a través de Internet o por medio de un RAS.
- Amenazas internas. Son amenazas causadas por personas que sí tienen acceso autorizado a la red. Puede ocurrir que algún empleado despedido

o descontento con la compañía introduzca un virus a la red como venganza. Este tipo de amenazas son las más frecuentes que existen.

4.7.2. Clasificación de los ataques a redes

Los ataques de la seguridad de las redes de VPN, se clasifican en 7 posibles ataques a la seguridad de las redes de telecomunicaciones las cuales son descritas a continuación.

- Husmeadores (*sniffers*) de red. Este ataque tiene lugar cuando el usuario no autorizado utiliza un programa llamado husmeador o sniffer el cual puede leer todos los paquetes que circulan por una red con lo que se puede tener acceso a información privada. Si los paquetes no están cifrados, el *sniffer* proporciona una vista completa de los datos contenidos en el paquete. Incluso los paquetes encapsulados (enviados por un túnel) se pueden abrir y leer si no están cifrados.
- Integridad de datos. Una vez que un atacante ha leído los datos entonces podrá tener la capacidad de modificarlos. Este ataque tiene lugar cuando alguien modifica o corrompe los datos que circulan por una red. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan.
- Ataques de contraseña (diccionario). Un problema típico de seguridad tiene que ver con el control de acceso basado en contraseñas. El problema es que un sistema no puede saber quien está frente al teclado escribiendo la contraseña. Una forma de obtener una contraseña es si los nombres de usuario y contraseña no son cifrados al enviarse por una red, cualquier atacante podría apoderarse de ella y

obtener acceso a una red haciéndose pasar por un usuario legítimo. Otra forma que se utiliza para obtener una contraseña es utilizar ciertas técnicas de criptoanálisis llamadas ataques de diccionario o fuerza bruta.

- Ataque de denegación de servicio (DoS). Este ataque tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Se puede lograr enviando datos no válidos a aplicaciones o servicios de red, lo que puede hacer que el servidor se bloquee. Otro ataque DoS consiste en inundar de tráfico toda una red hasta hacer que se sature y sea imposible utilizarla o también se puede estropear un *router* con el fin de que los usuarios legítimos no puedan acceder a la red.
- Ataque hombre en medio. Este ataque se produce cuando alguien se interpone entre dos usuarios que se están comunicando. El atacante observa activamente, captura y controla los paquetes sin que los usuarios lo adviertan. Por ejemplo, un atacante puede negociar claves de cifrado con ambos usuarios. A continuación, cada usuario enviará datos cifrados al atacante, quien podrá descifrarlos.
- *Spoofing*. Este ataque se basa en el uso de las direcciones IP. La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en una red. En algunos casos, es posible utilizar una dirección IP falsa. Esta práctica se conoce como suplantación. Un atacante podría utilizar programas especiales para construir paquetes IP que parezcan provenir de direcciones válidas dentro de la intranet de una organización. Una vez obtenido el acceso a

la red con una dirección IP válida, el atacante podrá modificar, desviar o eliminar datos.

- **Ataque de clave comprometida.** Una clave es un código o un número secreto necesario para cifrar, descifrar o validar información protegida. Averiguar una clave es un proceso difícil y que requiere grandes recursos por parte del atacante, pero no deja de ser posible. Cuando un atacante averigua una clave, ésta se denomina clave comprometida. El atacante puede utilizar la clave comprometida para obtener acceso a una comunicación protegida sin que el remitente ni el receptor lo perciban. La clave comprometida permite al atacante descifrar o modificar los datos. El atacante también puede intentar utilizar la clave comprometida para calcular otras claves que podrían suponer el acceso a otras comunicaciones protegidas.

4.8. Configuración de una VPN en un *firewall*

La configuración de IPSec en el *firewall* PIX de Cisco, El *firewall* PIX es un dispositivo que puede funcionar también como un activador de servicios VPN, el cual cumple con los estándares y es fácil de configurar. Los PIX 515, 520 y 525 pueden tener una tarjeta aceleradora VPN opcional (VAC). Esta tarjeta ofrece un rendimiento de cifrado 3DES a 100 Mbps sin necesidad de software adicional y sin tener que modificar la configuración del PIX. Como se muestra en la figura 33.

Figura 33. El *firewall* PIX de Cisco



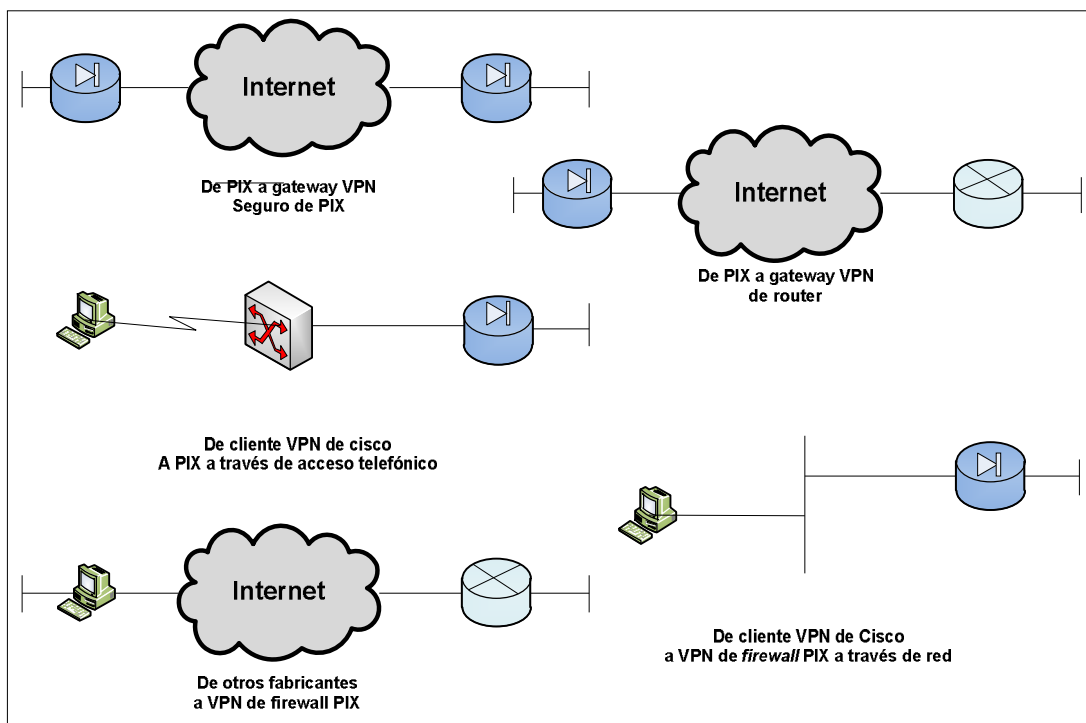
Fuente: González Morales, Alejandro. Funcionamiento de las VPN p. 153.

El firewall PIX crea VPN en varias topologías, las cuales se presentan en la siguiente lista y como se muestra en la figura 34.

- De PIX a *gateway* VPN seguro de PIX. Dos o más *firewalls* PIX pueden habilitar una VPN, que protege el tráfico entre los dispositivos colocados detrás de los *firewalls* PIX. La topología de *gateways* VPN seguros impide que el usuario tenga que implementar dispositivos o software VPN dentro de la red, haciendo que el *gateway* seguro sea transparente para los usuarios.
- De PIX a *gateway* VPN seguro de router Cisco IOS. El *firewall* PIX y el router Cisco, que ejecutan software VPN de Cisco Secure, pueden interactuar para crear un *gateway* VPN seguro entre redes.
- De cliente VPN de Cisco a PIX a través de acceso telefónico. El *firewall* PIX puede convertirse en un punto final para el cliente VPN de Cisco a través de una red de acceso telefónico.

- De cliente VPN de Cisco a PIX a través de red. El *firewall* PIX puede convertirse en un punto final VPN para el cliente VPN 3000 de Cisco Secure a través de una red IP.
- De productos de otros fabricantes a PIX. Los productos de otros fabricantes pueden conectarse con el *firewall* PIX si se adaptan a los estándares VPN abiertos.

Figura 34. **Topologías VPN con el *firewall* PIX**



Fuente: González Morales, Alexandro. Funcionamiento de las VPN p. 154.

Cualquier *firewall* PIX que ejecute el sistema operativo 5.0 y posterior del PIX utiliza el conjunto de protocolos IPSec para activar las opciones VPN. El *firewall* PIX soporta los estándares IPSec tales como IKE,

DES, 3DES, MD5, SHA-1, RSA, CA, SA. Se puede configurar IPsec en el *firewall* PIX por medio de claves previamente compartidas para la autenticación el uso de estas claves IKE para la autenticación de sesiones IPsec es relativamente fácil de configurar, aunque no escala bien cuando hay un gran número de iguales IPsec, habrá que usar certificados digitales.

5. IMPLEMENTACIÓN DE LA SEGURIDAD EN LAS REDES DE TELECOMUNICACIONES A PEQUEÑAS Y MEDIANAS EMPRESAS

5.1. Diseño de la gestión de seguridad

Una vez definidas las bases de un plan de seguridad de la empresa, puede comenzar a implementar medidas y controles para el resguardo de la información. El lugar donde se comienza a implementar la seguridad es en los controles técnicos es en la infraestructura de la organización.

5.1.1. Infraestructura

Se denomina infraestructura de red a todo componente informático disponible para la ejecución de las operaciones diarias de la empresa pequeñas y medianas empresas comprende no solo las computadoras de los usuarios; sino también *routers*, *switches*, cableado de red, impresoras, dispositivos móviles, servidores.

En una estructura de red empresarial de tamaño medio es posible separar los componentes de la infraestructura en dos grandes grupos: los internos (denominados LAN, del inglés *Local Area Network* en español, Red de Área Local) y los externos (denominados WAN, del inglés *Wide Area Network* en español, red de área extensa).

El perímetro de la red está formado por todos los elementos que actúan como frontera entre el mundo exterior y los componentes internos de la

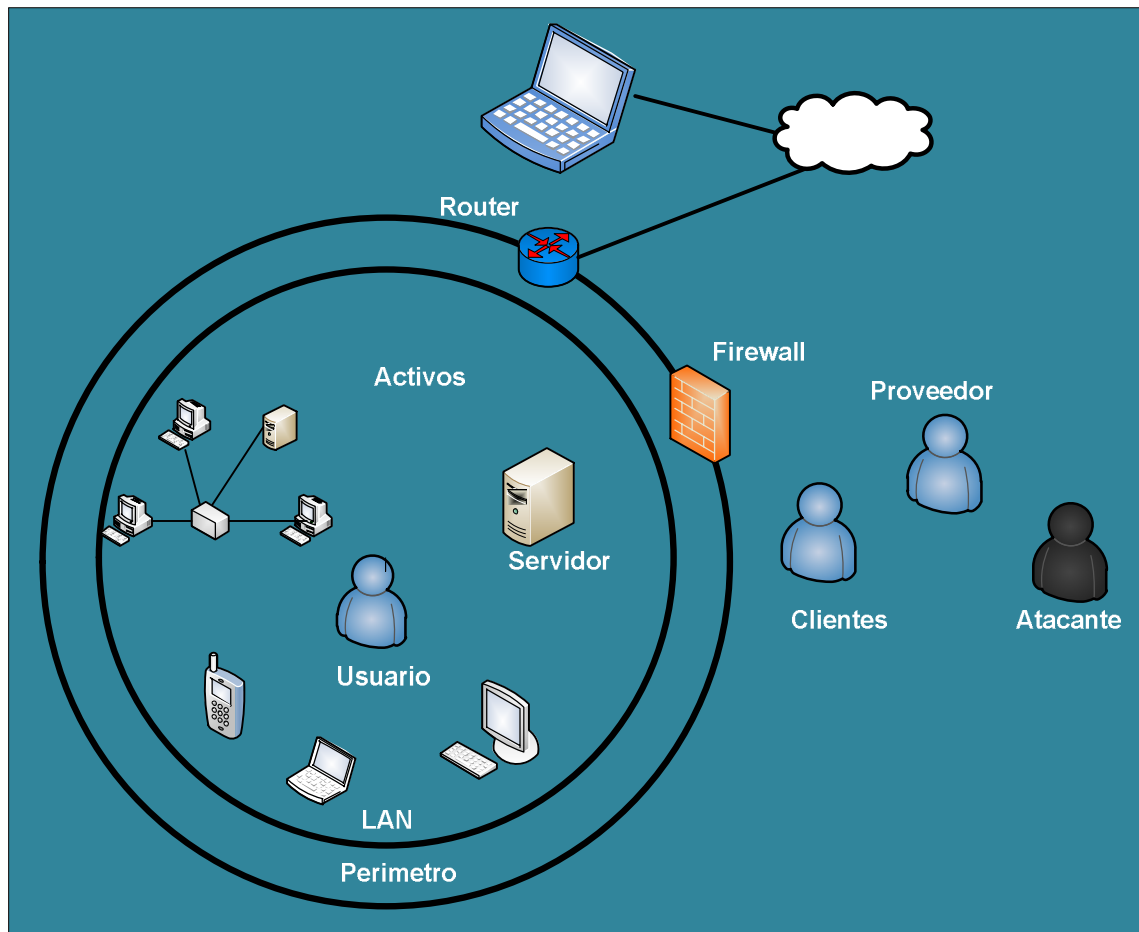
organización. Por lo general en una PyME es posible definir una comunicación según la necesidad de acceder a Internet: una transmisión se considera del tipo LAN si para comunicarse ambos extremos (emisor y destinatario) no es necesario utilizar Internet; en caso contrario se la considera una conexión WAN, que deberá extenderse por fuera del perímetro de la organización.

Los equipos que forman parte del perímetro son comúnmente *routers* (de conexión a Internet) y/o *firewalls*, aunque también pueden ser *gateways* o *proxys*, entre otros. A través de estos dispositivos se brinda la seguridad perimetral, es decir la posibilidad de controlar qué entra y qué sale en la infraestructura LAN de las pequeñas y medianas empresas.

En los últimos años la aparición de dispositivos móviles, utilidades de acceso remoto y otros, han logrado que el perímetro sea difuso, dificultando la definición de éste a la hora de implementar medidas de seguridad.

Para el establecimiento de la seguridad, en el perímetro se consideran como confiables los dispositivos LAN. Todo acceso desde la red WAN a la LAN es denegado por defecto, excepto los explícitamente permitidos, como se muestra en la figura 35.

Figura 35. **Infraestructura**



Fuente: Seguridad para PyMEs Infraestructura y comunicaciones p 4.

La política a utilizar es análoga a las reglas de seguridad que se aplican a las personas dentro de la empresa, quienes forman parte de la organización y están dentro de las instalaciones (área interna) son considerados confiables, no se ejerce control sobre ellos respecto a la salida de la empresa. El ingreso de personas ajenas a la organización (área externa), es asegurado de cierta forma a través de controles (en el perímetro), ya que no se considera confiable el ingreso desde el exterior al interior de la empresa sin un control previo.

5.1.1.1. Seguridad por capas

Los riesgos que está expuesta una organización son diversos, existe el modelo de seguridad por capas, para administrar y gestionar la seguridad perimetral, consiste en organizar las medidas de seguridad en diferentes niveles, garantizando que si resultara comprometido un nivel, el intruso o atacante deberá traspasar otra capa de seguridad para vulnerar los sistemas de la red. El concepto es análogo a las capas de una cebolla, para llegar al corazón (el activo) es necesario atravesar todas las capas previas.

Si un atacante externo deseara comprometer un servidor, primero deberá atravesar el *firewall* perimetral. Posteriormente, deberá poder autenticarse en el servidor, finalmente deberá poder comprometer el servicio deseado. En este caso, existen 3 niveles de seguridad (perimetral, en el sistema operativo, y medidas de seguridad del servicio o aplicación) que un intruso deberá comprometer para cumplir sus fines con éxito.

5.1.1.2. Acceso remoto

Una de las tendencias de mayor crecimiento en los últimos años es la posibilidad de acceder a recursos internos de la red, desde ubicaciones remotas (fuera de la red LAN). En las PyMEs, esta funcionalidad es útil, especialmente para cargos jerárquicos o personal que viaja frecuentemente, que desean continuar su trabajo (y disponer de los recursos apropiados) desde sus hogares, o desde sus laptops en ubicaciones remotas (bares, hoteles, oficinas distantes).

Las tecnologías para acceder remotamente son variadas, aunque no todas ofrecen las mismas características de seguridad. En entornos corporativos el acceso remoto seguro debe ser implementado a través de Redes Privadas

Virtuales (VPN), ya que estas cifran la información. Al transmitirse los datos por fuera de la LAN, en redes públicas, la confidencialidad de la información debe resguardarse cifrando la comunicación entre los extremos.

El protocolo predilecto para la utilización de acceso remoto por VPN es IPSEC1. El mismo puede ser implementado, sin mayores complejidades, tanto por hardware (muchos *routers* y *firewalls* incluyen dicha funcionalidad) como por software.

5.1.2. Comunicaciones *Networking*

Los usuarios de una PyMEs, hacen uso de recursos informáticos tanto de hardware como de software, las computadoras de los puestos de trabajo, los servidores, las *notebooks*, los medios de almacenamiento, las aplicaciones que se utilizan, el sitio web de la organización de las PyMEs, servicios en red.

Para que todos estos recursos se comuniquen entre sí, y trabajen coordinadamente en la red, existen una serie de componentes principalmente de hardware, que conforman las comunicaciones en la red. Estos dispositivos se llaman dispositivos de Comunicaciones o *Networking*, y los más utilizados en redes de tamaño medio son: router, switch, hub, cableado UTP.

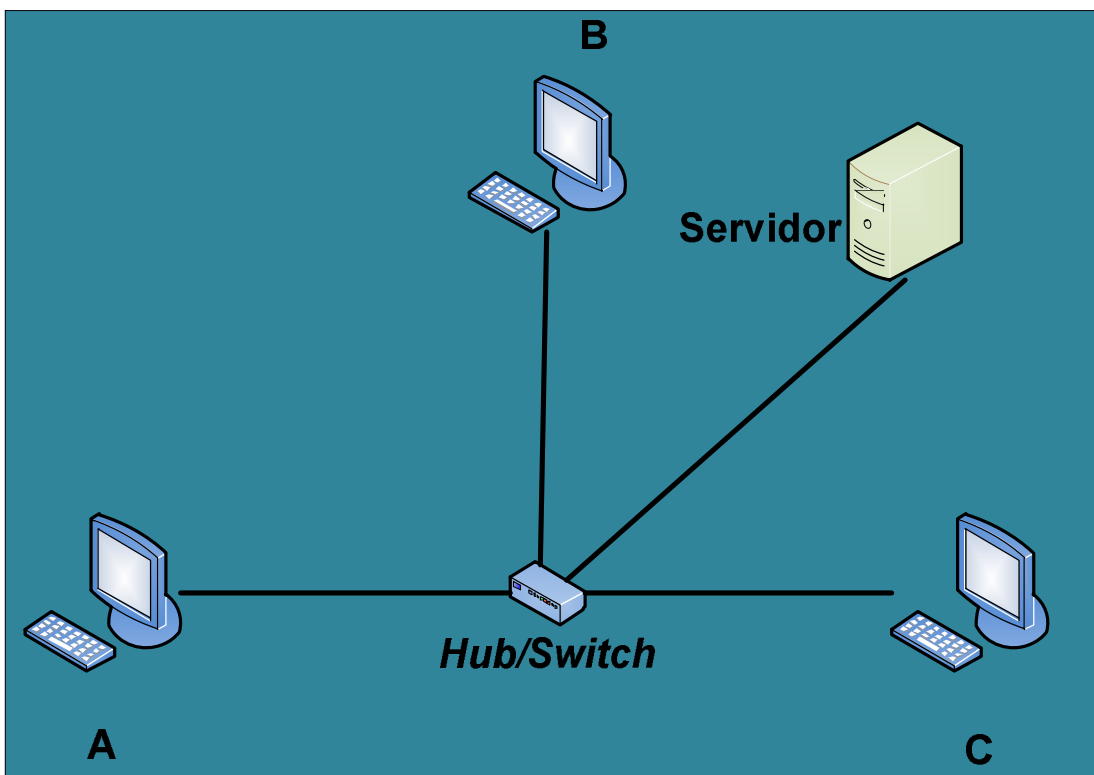
5.1.2.1. ¿*Switch* o *Hub*?

Las redes en empresas PyME están compuestas por una única red LAN donde todos los equipos están conectados a través de cables de red UTP existen ciertos dispositivos de red que permiten inter conectar todos los equipos entre sí, a través de las instalaciones de la red de las PyMEs, los hubs y los *switches*.

El *hub* (en español, concentrador), es un dispositivo de red que permite conectar varios equipos (según su capacidad) y que retransmite los paquetes recibidos en todos sus puestos, menos en el que recibió los datos.

Un *switch* (en español, conmutador), es un dispositivo de interconexión de equipos en red que retransmite los paquetes de acuerdo a la dirección de la placa de red (MAC) de destino leída en la trama del paquete de datos.

Figura 36. **Switch y Hub**



Fuente: Seguridad para PyMEs Infraestructura y comunicaciones p 7.

Como se muestra en la figura 36, tanto un *hub* y *switch* cumplen un mismo objetivo: conectar equipos en una red LAN. Sin embargo, su forma de operar difiere tecnológicamente.

Un *Hub* al recibir un paquete de datos replica la información en todos sus puertos. Es decir, si el equipo A envía cierta información al equipo B, el hub replicará la información en todos los puertos y serán posteriormente las computadoras las encargadas de recibir o rechazar el paquete. Es decir, el equipo B recibirá la información y ésta será dirigida por el sistema operativo hasta la aplicación correspondiente. En cambio, el equipo C recibirá los paquetes de datos pero estos serán rechazados, dado que estaban dirigidos a la dirección IP del equipo B.

Un *hub* tiene un funcionamiento similar a un dispositivo de múltiples enchufes donde la energía recibida es replicada en todas sus bocas, sin importar si ésta será utilizada o no posteriormente por cada una de ellas.

Un *switch* tiene una memoria interna que le permite direccionar el paquete de datos únicamente al puerto donde está conectada la PC destino, al llegar los paquetes al *switch*, los mismos serán retransmitidos únicamente en la boca donde se encuentra el equipo B.

Es por ello que los *hubs* representan un problema desde el punto de vista de la seguridad. Dada su naturaleza, un intruso conectado a un *hub* puede monitorear todos los datos que circulen por dicho segmento, utilizando programas *sniffers* que permiten capturar los paquetes en una red. Dada la naturaleza del *hub*, desde cualquier equipo es posible leer todos los paquetes que circulen por el *hub*, incluso aquellos que estén dirigidos a otros equipos de

la red en un *switch* instalado, un atacante en el equipo C no podrá monitorear las comunicaciones entre los equipos A y B.

Al mismo tiempo, por la retransmisión de paquetes en todos los puertos, los *hubs* generan tráfico innecesario y disminuyen la performance de la red.

A pesar de que los *switches* llevan años en el mercado, aún existen gran cantidad de empresas, particularmente del tipo PyME, que utilizan *hubs* en sus redes LAN, es recomendable utilizar únicamente *switches* como dispositivos de interconexión en la LAN, tanto por sus características de performance (afectando la disponibilidad de la información) como de transmisión (confidencialidad de la información).

Existen formas de comprometer un *switch* de forma tal que éste se comporte como *hub* y así monitorear el tráfico de red. De todas formas, la naturaleza de los dispositivos es diferente; no es posible vulnerar cualquier *switch* caso de ser posible, el atacante deberá tener amplios conocimientos de redes TCP/IP y herramientas de *networking*, *hacking* y *sniffing*.

5.1.2.2. Segurización de dispositivos de red

Dadas las características de las PyMEs, el armado de la red, sus dispositivos y el cableado son comúnmente realizados por personal interno de la organización, sin considerar normas o estándares internacionales de cableado estructurado.

Sin embargo es aconsejable considerar ciertas medidas de simple implementación a la hora del armado de la red, que brindan a los administradores nuevas capas de seguridad de alta efectividad.

5.1.3. Almacenamiento

Una de las cuestiones más críticas respecto a la información digital de las PyME empresas es su almacenamiento. Toda la información debe ser almacenada de forma tal que queden resguardados los tres principios de la seguridad:

- Disponibilidad (que cualquier usuario pueda acceder a la información que necesite en el momento que lo desee).
- Integridad (garantizar que esta información esté libre de alteraciones no autorizadas).
- Confidencialidad (que la información sea accedida sólo por las personas autorizadas).

5.1.3.1. Esquema cliente servidor

Uno de los errores más frecuentes en entornos corporativos y particularmente en PyMEs es la descentralización de la información. Entre las desventajas de tener la información distribuida en muchos equipos de la red y particularmente en puestos de trabajo se encuentran:

- Problemas de disponibilidad: algunos usuarios de la red pueden necesitar información y no saber dónde encontrarla o cómo ubicar en dónde está almacenada.
- Confidencialidad: alguna información no controlada podría ser accedida por personas no autorizadas.

- Dificultad para hacer *backup*: es extremadamente complejo mantener un *backup* completo de la información disponible en todos los puestos de trabajo. Puede darse el caso de que información valiosa no tenga copias de respaldo.

Para entornos corporativos de las PyMEs es recomendable mantener un esquema cliente servidor, donde toda la información sea almacenada en unos servidores de archivos (*File Server*).

La implementación de un *File Server* incluye no sólo la adquisición de hardware para tal fin y la instalación de un sistema operativo, sino también la creación de políticas de uso, la configuración de los puestos de trabajo y la capacitación de los usuarios para que éstos puedan acceder al servidor.

Todos los usuarios deben estar informados de la existencia del *File Server* y alertados de que toda la información de la organización será responsabilidad del Área de red y sistemas, excepto aquella que se encuentre almacenada en otro lugar que no sea el servidor de archivos. Se pueden configurar los puestos de trabajo para limitar las capacidades de almacenamiento local que tengan los usuarios.

5.1.3.2. Políticas de almacenamiento

La existencia de un servidor de archivos, no significa que cualquier tipo de archivos deben ser almacenados allí por cualquier tipo de personas. Es por ello que es necesario definir las políticas de almacenamiento para el servidor de archivos. Las mismas deben ser definidas en conjunto con los responsables de cada área y la alta gerencia de la organización.

Las preguntas que deben responderse para la realización de una política de almacenamiento son las siguientes:

- ¿Qué se desea almacenar? Se debe definir cuál es la información importante para la empresa y que deba ser almacenada en el *File Server*. Por ejemplo, archivos temporales que utilicen los usuarios (para llevar un control de sus tareas) o archivos de MP3 que utilicen los usuarios en su jornada laboral, no siempre será necesario almacenarlos en un servidor central.
- ¿Quién podrá almacenar? Una vez definida qué información se debe almacenar, se deberá evaluar qué usuarios hacen uso de esa información. Probablemente haya usuarios que no necesiten almacenar archivos importantes. Por ejemplo, usuarios que solo utilicen una aplicación de negocios. Se debe dar acceso al servidor sólo a aquellos usuarios que necesiten utilizar sus archivos.
- ¿Cuánto podrá almacenar? El espacio en disco tiene un costo y un límite una vez adquiridos los discos de almacenamiento. Es por ello que es necesario definir y calcular qué capacidad de almacenamiento podrá disponer cada usuario.

Los sistemas operativos más utilizados en la actualidad a nivel servidor ofrecen alternativas para hacer uso de estas configuraciones. Por ejemplo, prohibir los archivos de extensión, WAV, MP3 o limitar a cada usuario para que no pueda almacenar más de 500 MB de archivos. La utilización de estas opciones de configuración permite optimizar el uso y mantenimiento del *File Server*.

Las políticas de almacenamiento deben darse a conocer a todos los usuarios de la empresa directamente, o a través de las Políticas de Seguridad.

5.1.3.3. Redundancia

Cuando todos los datos están almacenados en un servidor de archivos la criticidad de dicho servidor aumenta. Respecto a los discos duros, el lugar donde está almacenada la información, es necesario contar con un *backup* de la misma, existen métodos de redundancia que permiten la continuidad en caso que un disco rígido presente una falla.

RAID (*Redundant Array of Independent Disks*, en español Conjunto Redundante de Discos Independientes), es una tecnología que permite almacenar información en múltiples discos duros y disponer de ella de manera redundante. Si se detecta un error al acceder a cierto dato del disco, el mismo será leído al menos desde otra ubicación sin afectar la operatoria de las PYMEs.

Existen múltiples técnicas para aplicar RAID en discos y cada una de ellas ofrece mayor o menor nivel de performance y redundancia. Para una PYME es recomendable utilizar en el servidor de archivos, al menos el más simple de éstos el RAID 1.

Un RAID 1 consiste en dos discos espejados, donde se replica la información en tiempo real y el operador los ve funcionar como si fueran un único disco. De esta forma un fallo en uno de los discos permite continuar con el acceso a los datos. Para la adquisición de un disco para un servidor de archivos, se recomienda evaluar bien el tamaño y comprar dos discos de igual capacidad para configurar el RAID 1. Existen otros sistemas de RAID, que

permiten niveles de seguridad más avanzados y para esquemas más complejos de organización de discos.

5.1.3.4. Medios extraíbles

Además del empleo de los discos rígidos como medios de almacenamiento más frecuentes en las computadoras, es muy frecuente que los empleados cuenten con sus propios medios extraíbles, tales como Pen Drives, MP3 o memorias de cámaras y dispositivos móviles. Estos pueden representar un riesgo para la seguridad de la información, ya que el administrador pierde control sobre el uso y protección que se le brinde a dichos datos.

Por lo tanto las PyMEs deben definir una política respecto al uso de dispositivos de almacenamiento móviles. Deberá establecerse si estos están permitidos o prohibidos y para quién. En caso de ser necesario, los administradores deberán deshabilitar, por software, los puertos USB de las computadoras. En caso de no implementar dichas medidas es una buena práctica inhabilitar los enchufes USB de las máquinas a fin de evitar la conexión de estos dispositivos.

Las políticas de uso de dispositivos de almacenamiento móviles deben darse a conocer a todos los usuarios de la empresa directamente, a través de las Políticas de Seguridad y de la concientización.

5.1.4. Política de *Backups*

La realización de copias de seguridad de la información es útil tanto para la recuperación total de información ante un desastre, si se perdiera toda la

información de un *File Server* o de una base de datos, es posible utilizar el *backup* para poner a disposición nuevamente la información, como para la recuperación parcial de información ante un incidente como el borrado no intencional de un archivo, archivos dañados. Si fuera necesario recuperar cierta información, ésta puede ser obtenida del último *backup* disponible.

Tener esquemas centralizados como un *File Server*, carece de total sentido si no se aprovechan dichas topologías para mantener un *backup* que resguarde la información corporativa.

5.1.4.1. Backup

Se denomina *backup* o copia de seguridad a la copia de información y su almacenamiento fuera de entornos de producción. Un esquema de *backup* debe contemplar las tres alternativas y definir cuáles son convenientes en cada caso, existen tres tipos de copias de seguridad.

- *Backup Full* (o completo): es el resguardo total de la información. En el caso de un servidor de correo, consiste en realizar la copia de seguridad de todos los correos y base de datos completa del servidor. Este tipo de *backup* es el de mayor complejidad y consumo de espacio, por lo que generalmente se debe realizar con baja periodicidad.
- *Backup Incremental*: es el resguardo solo de aquella información que ha sido modificada desde el último *backup* completo. En el caso de un servidor de archivos, consiste en almacenar solo los archivos cuya fecha de modificación sea superior al último *backup*. Este tipo de *backup* consume mucho menos espacio y tiempo, que el *backup full*, y puede ser realizado en períodos más cortos de tiempo.

- *Backup* Diferencial: aumenta el tamaño de datos hasta la realización de un nuevo *backup* full. Es decir, si se hace un *backup* el primer día del mes, el segundo día se almacenarán los archivos que hayan sido modificados ese día; y el cuarto día se almacenarán los archivos de los tres días posteriores al *backup* full.

En el caso del *backup* diferencial, solo se almacenan los archivos modificados desde el último *backup* diferencial. De esta forma, cada *backup* independiente ocupa menos espacio en disco.

5.1.4.2. Consideraciones

Es necesario definir sobre qué información se va a realizar el *backup*, definir sobre cada tipo de datos, cada cuánto tiempo y qué tipos de *backups* se aplicarán en cada caso. Finalmente, es necesario definir dónde será almacenado el *backup*; las copias de seguridad completas, teniendo en cuenta que proveen protección ante desastres, deben ser guardadas en instalaciones distantes del lugar donde se aloja diariamente la información.

Es necesario considerar todo tipo de información para la realización de copias de seguridad, no solo el servidor de archivos. También deben realizarse copias de respaldo del correo electrónico, las bases de datos, las configuraciones de los sistemas operativos, los logs. Cada organización deberá evaluar la criticidad de la información y los recursos para realizar los *backups*.

5.2. Mejores prácticas

Para mitigar los riesgos que los dispositivos móviles representan, en la implementación para la seguridad de las redes de telecomunicaciones aplicada a las Pequeñas y Medianas Empresas (PyMEs), deben intervenir con tres tipos de medidas.

- En primer término, limitar el uso de dispositivos móviles en la red. Es decir dar permisos solo aquellos usuarios para los cuales el uso del dispositivo suma valor a su trabajo, puedan conectarse a la red de las PyMEs. Es una buena práctica limitar las redes wireless en cuanto al acceso que éstas brinden a la red. Los usuarios con mayores permisos pueden conectarse a la red inalámbrica y luego establecer una VPN.
- En segundo término, establecer políticas de seguridad para los dispositivos móviles en la red, controlando con el consentimiento del usuario las medidas de seguridad que estos poseen y denegando su utilización en las PyMEs si no se cumplen requisitos mínimos de seguridad.
- En último lugar, las PyMEs puede tomar el control de aquellos usuarios que necesiten explícitamente de un dispositivo móvil para trabajar, otorgando el mismo al usuario definiendo las medidas de seguridad y permisos que el usuario tendrá.

5.2.1. Establecer la política de seguridad de la empresa

Es el responsables del desarrollo, implantación y gestión de la política de las PyMEs es el director de Política de Seguridad. Personal encargado de

realizar, supervisar, inspeccionar, modificar las normas y reglas establecidas en la política de seguridad.

Política de seguridad establecida, es asignar acceso a la información, proveer de permisos y soportes informáticos, controlar la entrada y salida de información, identificación y resolución de incidencias.

Crear una directiva de uso aceptable, es un documento en el que se informa a los empleados de lo que pueden y no pueden hacer en los equipos de las PyMEs. Ponga por escrito las normas que espera que se cumplan. Puede describir su política sobre la creación de contraseñas, indicar la frecuencia de cambio de contraseñas o mencionar el riesgo que supone abrir archivos adjuntos de correo electrónico de remitentes desconocidos, la prohibición de instalar software no autorizado en los equipos. En este documento, que debe ser firmado por todos los empleados, tienen que constar las sanciones en casos extremos, incluso el despido por contravenir esas normas.

En su calidad de propietario o director del negocio, también deberá firmar una copia de la directiva. Si la directiva es larga y detallada, ayude a los empleados a recordar los puntos principales con un resumen de una página que puede distribuir y colocar cerca de sus estaciones de trabajo.

5.2.1.1. Conciencia a sus empleados

Distribuya proactivamente a través de comunicaciones periódicas las actualizaciones en las políticas de seguridad en los empleados para la seguridad de la información de las Pequeñas y Medianas Empresas.

5.2.2. Proteja sus equipos de escritorio y portátiles

La protección de los equipos de escritorio y portátiles, es proteger de los virus y software espía. Realizando actualización de software, configuración de *firewall*, evitar correo no deseado, utilice software legal, navegación segura para la protección de los equipos de escritorio y portátiles.

5.2.2.1. Protéjase de los virus y el software espía

Los virus así como los gusanos y los troyanos son programas maliciosos que se ejecutan en su equipo. Entre las acciones que pueden provocar este tipo de código malicioso se encuentran: borrado o alteración de archivos, consumo de recursos del equipo, acceso no autorizado a archivos, infección de los equipos de los clientes con los que se comunique mediante correo electrónico, el virus se puede extender por los equipos de su empresa y producir momentos de inactividad y pérdidas de datos muy graves. Existen herramientas de eliminación de software malintencionado que comprueban infecciones por software malintencionado específico y ayuda a eliminarlas.

Instale software antivirus. Debe disponer de protección antivirus en todos sus equipos de escritorio y portátiles. El software antivirus examina el contenido de los archivos en su PC en busca de indicios de virus. Cada mes aparecen cientos de virus nuevos, por lo que hay que actualizar periódicamente los antivirus con las últimas definiciones para que el software pueda detectar los nuevos virus. Asegúrese que el antivirus esta actualizado.

5.2.2.2. Actualizaciones software

A los piratas informáticos les gusta encontrar y aprovechar cualquier error de seguridad en los productos de software más populares. Cuando Microsoft u otra compañía descubren una vulnerabilidad en su software, suelen crear una actualización que se puede descargar de Internet (tanto para el Sistema Operativo como cualquier aplicación que se tenga instalada). Es necesario instalar las actualizaciones tan pronto se pongan a la disposición del público.

5.2.2.3. Configure un *firewall* para PyMES

Un *firewall* es un programa encargado de analizar tanto el tráfico entrante como saliente de un equipo, con el fin de bloquear determinados puertos y protocolos que potencialmente podrían ser utilizados por las aplicaciones.

5.2.2.4. Evite el correo electrónico no deseado

El spam son mensajes de correo electrónico comercial no solicitado si recibe un correo electrónico de un remitente desconocido elimínelo sin abrirlo, puede contener virus y tampoco responda al mismo, ya que estaría confirmando que su dirección es correcta y está activa. No realice envío de publicidad a aquellas personas que no hayan autorizado previamente el consentimiento de recibir publicidad.

Adopte medidas de protección frente al correo electrónico no deseado. Como filtros de correo electrónico actualizados.

5.2.2.5. Utilice solamente software legal

El uso de software ilegal además de generar riesgos de carácter penal, también puede generar problemas en la seguridad en la red de la información en las PyMEs, lo que lo que conlleva a pérdidas en la rentabilidad y productividad de las PyMEs. El software legal ofrece garantía y soporte del fabricante.

5.2.2.6. Navegación segura

La navegación segura por Internet, protege los equipos dqe escritorios o portátiles de las redes de las Pequeñas y Medianas Empresas (PyMES) ante amenazas o ataques externos de la red, se tiene los siguientes recomendaciones:

- Acceda únicamente a sitios de confianza.
- Analice con un antivirus todo lo que descarga antes de ejecutarlo en su equipo.
- No explore nunca sitios Web desde un servidor. Utilice siempre un equipo o portátil cliente.
- Mantenga actualizado su navegador a la última versión.
- Configure el nivel de seguridad de su navegador según sus preferencias.
- Descargue los programas desde los sitios oficiales para evitar suplantaciones maliciosas.

- Configure su navegador para evitar pop-ups emergentes.
- Utilice un usuario sin permisos de Administrador para navegar por Internet, así impide la instalación de programas y cambios en los valores del sistema.
- Borre las cookies, los ficheros temporales y el historial cuando utilice equipos ajenos para no dejar rastro de su navegación.
- Observe en la barra de navegación de su navegador, que la dirección Web comienza por https: indica que se trata de una conexión segura y el contenido que transfiera será cifrado por la Red.
- Observe que aparece un candado () en la parte inferior derecha de su navegador. Esto significa que la entidad posee un certificado emitido por una autoridad certificadora, el cual garantiza que realmente se ha conectado con la entidad destino y que los datos transmitidos son cifrados.

5.2.3. Proteja su red

Para la protección de la red de las Pequeñas y Medianas Empresas (PyMES), es utilizar contraseñas seguras, protección de la red WIFI, configurar el *firewall* a nivel de la red, se realiza para proteger la información que desea mantener confidencial, preste atención a las siguientes reglas.

5.2.3.1. Utilice contraseñas seguras

Informar a los empleados de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red, ya que dificultan la suplantación de su usuario. Es decir no se debe dejar en cualquier parte ni se debe compartir. Características de una contraseña segura.

- Una longitud de ocho caracteres como mínimo; cuanto más larga, mejor.
- Una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Se debe cambiar cada 30 días como mínimo y, al cambiarla, debe ser muy distinta de las contraseñas anteriores.
- No utilice datos personales.

5.2.3.2. Proteger una red WIFI

Para proteger una red WIFI y maximizar seguridad en la redes de la Pequeñas y Medianas Empresas (PyMEs) para la protección de la información, es necesario usar la siguiente lista de consejos en conjunto.

- Ocultar el SSID (identificador de redes inalámbricas) al exterior es una buena medida para evitar las intrusiones, aunque este dato puede descubrirse fácilmente aunque este se presente oculto.
- Cambiar el nombre SSID.

- Cifrado WEP Se basa en claves de 64 o 128 bits. La encriptación WEP no es la opción más segura.
- Encriptación Wi-Fi *Protected Access*.

Surgió como alternativa segura y eficaz al WEP, se basa en el cifrado de la información mediante claves dinámicas, que se calculan a partir de una contraseña.

5.2.3.3. Configure un *firewall* a nivel de Red

Un *firewall* es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Un *firewall* puede ser un dispositivo software o hardware.

5.2.4. Proteja sus servidores

La protección de los servidores en las redes de las Pequeñas y Medias Empresas (PyMES), es de gran importancia, en el momento que los servidores están en peligro, también lo está toda la red es necesario seguir las siguientes instrucciones.

5.2.4.1. Certificados de servidor

Identifican a los sitios Web. Requiere de la existencia de una autoridad certificadora (CA) que afirme, mediante los correspondientes certificados de servidor, que éstos son quienes dicen ser antes del establecimiento del canal seguro. Le permitirá establecer comunicaciones seguras con sus clientes,

cifrando la conexión usando la tecnología SSL para que no pueda ser leída por terceros.

5.2.4.2. Mantenga sus servidores en un lugar seguro

Las empresas deben asegurarse de que sus servidores no son vulnerables a las catástrofes físicas. Coloque estos equipos en una sala segura y con buena ventilación. Haga una relación de los empleados que tienen las llaves de la sala de servidores.

5.2.4.3. Práctica de menos privilegios

Asigne distintos niveles de permisos a los usuarios. En vez de conceder a todos los usuarios el acceso Administrador, debe utilizar los servidores para administrar los equipos cliente. Los servidores se pueden configurar para conceder a cada usuario acceso únicamente a programas específicos y para definir los privilegios de usuario que se permiten en el servidor. De este modo se garantiza que los usuarios no pueden efectuar cambios que son fundamentales en el funcionamiento del servidor o equipo cliente.

5.2.4.4. Conozca las opciones de seguridad

Los servidores actuales son más seguros que nunca, pero las sólidas configuraciones de seguridad que se encuentran en los productos de servidor sólo son eficaces si se utilizan del modo adecuado y se supervisan estrechamente.

5.2.5. Proteja sus aplicaciones y recursos

La protección de aplicaciones y recursos de las redes de las Pequeñas y Medianas Empresa (PyMES), se establece el valor de un directorio activo, la gestión de aplicación, atención a la base de datos, cortafuegos de aplicaciones web, autorías y gestión de actualizaciones.

5.2.5.1. Valore la instalación del directorio activo

La implementación del directorio activo en las redes de las Pequeñas y Medianas Empresas (PyMES), facilita las tareas tanto de seguridad como de funcionalidad y ventajas:

- La propagación de permisos está centralizada desde el Controlador de Dominio.
- Posibilidad de escalabilidad según las necesidades particulares de la empresa.
- La integración con un servicio DNS.
- Sencillez en la estructuración de ficheros y recursos compartidos.
- Robustez en la seguridad del sistema.
- Establecimiento de políticas.

5.2.5.2. Gestione las aplicaciones a través del directorio activo

La gestión de las aplicaciones a través del directorio, activa en las redes de las Pequeñas y Medianas Empresas (PyMES), establece la política de la gestión en los permisos para usuario para hacer uso de los recursos de la red.

- Políticas
- Permisos usuario
- Impresoras
- Correo electrónico

5.2.5.3. Preste atención a la base de datos

Instale los últimos *Service Packs* de la base de datos. Asegúrese de instalar los *Service Packs* y las actualizaciones más recientes para mejorar la seguridad. Evalúe la seguridad de su servidor con MBSA (Microsoft *Baseline Security Analyzer*). Aísle el servidor y realice copias de seguridad periódicas del mismo.

5.2.5.4. Cortafuegos de aplicaciones Web

Protegiendo de ataques específicamente las comunicaciones en la que intervienen tanto las aplicaciones Web como todos los recursos a de las redes de las Pequeñas y Medianas Empresas (PyMES), para la protección de la información.

5.2.5.5. Auditorias técnicas

Una auditoría técnica de seguridad, puede identificar las vulnerabilidades de una aplicación web en la implementación de la seguridad en la redes de telecomunicaciones aplicada a las Pequeñas y Medianas Empresas (PyMES), para garantizar el funcionamiento de la red.

5.2.5.6. Gestión de las actualizaciones

La gestión de las actualizaciones en las redes de las Pequeñas y Medias Empresa (PyMES), se realiza para buen funcionamiento de la red en la actualización de software, hardware de actualizaciones oportunas, configuraciones especiales y supresión.

5.2.5.6.1. Actualizaciones oportunas

Las revisiones y las actualizaciones de errores, junto con nuevas versiones de software, se pueden implementar desde el servidor en los equipos y portátiles de los usuarios. Así sabe que se han realizado correctamente de forma oportuna y no tiene que depender de que los usuarios no se olviden.

5.2.5.6.2. Configuraciones especiales

Puede impedir que los usuarios instalen programas no autorizados si limita su capacidad para ejecutar programas desde CD-ROM y otras unidades extraíbles o para descargar programas de Internet.

5.2.5.6.3. Supervisión

Si se produce un acceso no autorizado en un equipo o si hay un error del sistema de red de algún tipo en algún equipo, se puede detectar inmediatamente mediante las capacidades de supervisión que están disponibles en un entorno de equipos y portátiles administrado.

CONCLUSIONES

1. El éxito de la seguridad de las redes de telecomunicaciones es proteger las pequeñas y medianas empresas de amenazas y riesgos, que impiden el desarrollo productivo.
2. Al realizar una política de seguridad esto garantiza la protección de los activos por medio de un análisis de riesgos que identifica los riesgos y clasificarlos en función de su grado.
3. La protección de la información transmitida se realiza por medio de la criptografía que utiliza algoritmos simétricos (modernos o llave privada), algoritmos asimétrico (llave privada pública), autenticación y firma digital, que garantiza la información sea original.
4. Las ventajas que ofrecen las redes privadas virtuales es que utiliza la infraestructura de una red pública para poder transmitir información que constituye un replazo indispensable a los métodos tradicionales caros de una red.
5. No solamente las grandes empresas necesitan considerar las medidas de seguridad en su red, sino también las pequeñas y medianas empresas deben implementarlo para mejorar desarrolla productivo y laboral.

RECOMENDACIONES

1. Para establecer la seguridad de las redes de telecomunicaciones aplicada a las pequeñas y medianas empresas es indispensable buscar que la tecnología sea de alta calidad y personal calificado para realizarlo, para garantizar la protección de la entidad, el desarrollo productivo y tener una buena imagen.
2. Se debe utilizar una planificación y una política de la seguridad a las redes de las pequeñas y medianas empresas para la protección de los activos.
3. Para la seguridad de la información debe utilizar la encriptación cuando se transmite por medio de la red.
4. Se debe utilizar una red de VPN en las pequeñas y medianas empresas para la seguridad la comunicación en la red y obtener beneficios de esta tecnología.
5. Al momento de implementar la seguridad en las redes de las pequeñas y medianas empresas es indispensable conocer de red, para implementar la seguridad correctamente.

BIBLIOGRAFÍA

1. ARÉVALO JIMÉNEZ, Fernando Andres. *Cómo escoger e implementar una VPN conceptos teóricos y prácticos*. Director. Ing. Fabio Guerrero Msc. Universidad del Valle Santiago de Cali. Facultad de Ingeniería Escuela de Ingeniería Eléctrica y Electrónica. Colombia: 2003. 25 p.
2. BELLO, Claudia E. *Manual de seguridad en redes. ArCERT (Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública)*. 2a ed. Argentina: 2000. 23 p.
3. BERTINE, Herb. *La seguridad de las telecomunicaciones y las tecnologías de la información*. 2a ed. Ginebra: 2006. 15 p.
4. DE LEÓN ESCOBAR, José Antonio. *Factibilidad económica y relación técnica en la implementación de una red de servicios de telecomunicaciones*. Trabajo de graduación de Ing. José Antonio De León Escobar. Universidad de San Carlos de Guatemala. Facultad de Ingeniería. 2006. 22 p.
5. DE LEÓN PAREDES, Diego Antonio. *Diseño de implementación de una red inalámbrica bluetooth, haciendo énfasis en la seguridad de la misma*. Trabajo de graduación de Ing. Diego Antonio De León Paredes. Universidad de San Carlos de Guatemala. Facultad de Ingeniería. 2007. 10 p.

6. GONZÁLEZ MORALES, Alexandro. *Redes privadas virtuales*. Coordinador. Lic. Elías Varela Paz. Universidad Autónoma del Estado de Hidalgo. Instituto de Ciencias Básicas e Ingeniería. México: 2006. 35 p.

7. VILLAGRÁ GONZÁLEZ, Víctor A. *Seguridad en redes de telecomunicación. Mateos Lanchas, Verónica (Grupo de Redes y Servicios de Telecomunicación e Internet Departamento de Ingeniería de Sistemas Telemáticos E.T.S.I. de Telecomunicación-UPM)*. Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones Ciudad Universitaria, Abril 2009. 10-18,103-153 P. ISBN (13): 978-84-7402-356-5. 60 p.

8. VIVAR ROJAS, Luis Fernando. *Implementación de los cursos de telecomunicaciones y redes locales y de proyectos computacionales aplicados a ingeniería electrónica para estudiantes en línea*. Universidad de San Carlos de Guatemala. Facultad de Ingeniería. 2007. 25 p.

ANEXOS

Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.

Se ha revisado recientemente la arquitectura de seguridad de redes define una arquitectura para garantizar la seguridad extremo a extremo. Esta arquitectura puede aplicarse a distintos tipos de redes en los que es importante garantizar la seguridad extremo a extremo, independientemente de la tecnología que utilice la red. Si bien los principios y definiciones generales allí tratados son válidos para todas las aplicaciones, los detalles relativos a, por ejemplo, las amenazas y vulnerabilidades y las medidas para contrarrestarlas o preverlas dependen de cada aplicación.

Esta arquitectura de seguridad se define teniendo en cuenta dos conceptos principales, a saber las capas y los planos. El concepto de capas de seguridad tiene que ver con los requisitos aplicables a los elementos de red y sistemas que constituyen la red extremo a extremo, el sistema de capas proporciona una perspectiva jerárquica de la seguridad extremo a extremo de la red basada en la seguridad capa por capa. Hay tres capas de seguridad: la capa de infraestructura, la capa de servicios, y la capa de aplicaciones.

Una de las ventajas del modelo de capas es que se garantiza la seguridad extremo a extremo aun cuando se utilicen diferentes aplicaciones. Cada capa tiene sus propias vulnerabilidades y se han de definir medidas para contrarrestarlas en cada una de ellas. La capa de infraestructura comprende los dispositivos de transmisión de red, así como los elementos que la componen.

Por ejemplo, son parte de dicha capa los encaminadores, los centros de conmutación y los servidores, así como los enlaces de comunicación entre ellos, la capa de servicios tiene que ver con la seguridad de los servicios de red

que los proveedores prestan a sus clientes desde servicios básicos de transporte y conectividad, como las líneas arrendadas, hasta los servicios de valor añadido como la mensajería instantánea. La capa de aplicaciones tiene que ver con la seguridad de las aplicaciones de red a las que acceden los usuarios, y que van desde las básicas como el correo electrónico hasta las sofisticadas como la colaboración en vídeo.

La seguridad de las actividades que se efectúan en una red, se definen tres planos de seguridad que representan los tres tipos de actividades protegidas que se realizan en ella:

- El plano de gestión
- El plano de control
- El plano usuario de extremo

Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como a las de usuario de extremo.

El plano de seguridad de gestión tiene que ver con las actividades, operaciones, administración, mantenimiento y aprovisionamiento, relacionadas. La configuración de un usuario o una red y otras.

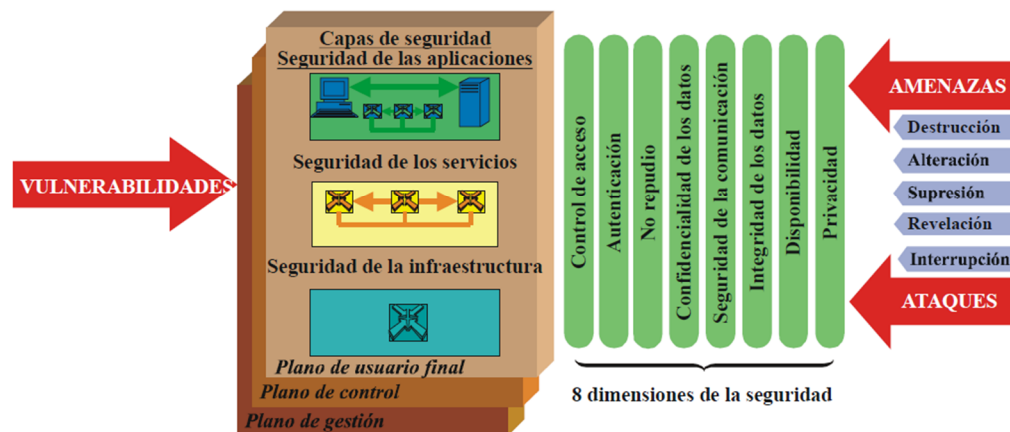
El plano de seguridad de control se relaciona con los aspectos de señalización necesarios para establecer y modificar la comunicación extremo a extremo a través de la red, sin importar el medio y la tecnología utilizados en ella.

El plano de seguridad de usuario de extremo tiene que ver con la seguridad cuando se accede y utiliza la red; en este plano también se considera la seguridad de flujos de datos del usuario extremo.

En la arquitectura se definen ocho dimensiones de seguridad, descritas a continuación que tratan la seguridad de red. Desde el punto de vista de la arquitectura, estas dimensiones se aplican a cada una de las componentes de la matriz 3 por 3 formada entre las capas y los planos, de tal manera que se puedan tomar medidas para contrarrestar los problemas de seguridad correspondientes.

En la figura 37 se indican los planos, capas y dimensiones de seguridad de la arquitectura de seguridad.

Figura 37. **Elementos de la arquitectura de seguridad**



Fuente: Vanegas, Orlando. Tendencias de Seguridad en Telecomunicaciones.

Las funciones de los servicios de seguridad básicos de (control de acceso, autenticación, confidencialidad de los datos, integridad de los datos y no repudio) reflejan las correspondientes funciones de las dimensiones de la seguridad de las comunicaciones, disponibilidad y privacidad que ofrecen nuevos tipos de protección para la red.

- La dimensión de seguridad control de acceso protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones.
- La dimensión de seguridad autenticación permite comprobar la identidad de las entidades comunicantes. La autenticación garantiza la validez de las identidades que anuncian las entidades que participan en la comunicación (persona, dispositivo, servicio o aplicación) y garantiza que ninguna de estas entidades ha usurpado una identidad o está reproduciendo una comunicación anterior sin autorización.
- La dimensión de seguridad no repudio impide que una persona o una entidad nieguen haber realizado una acción concreta en relación con los datos, presentando las pruebas de esas acciones en la red (prueba de obligación, intención o compromiso; prueba de origen de los datos, prueba de propiedad, prueba de utilización de recursos). Garantiza la disponibilidad de pruebas que pueden presentarse a terceros y que permiten demostrar que ha ocurrido algún tipo de evento o acción.

- La dimensión de seguridad confidencialidad de los datos impide la divulgación no autorizada de los datos. La confidencialidad de los datos garantiza que las entidades no autorizadas no pueden entender el contenido de los datos. A menudo se utilizan métodos tales como la criptación, listas de control de acceso y permisos de acceso a ficheros para garantizar la confidencialidad de datos.
- La dimensión de seguridad la comunicación garantiza que los flujos de información sólo tienen lugar entre puntos extremos autorizados (la información no puede desviarse ni ser interceptada cuando fluye entre estos dos puntos extremos).
- La dimensión de seguridad integridad de los datos garantiza que los datos son correctos y exactos. Los datos están protegidos contra las acciones no autorizadas de modificación, supresión, creación y copia, y en su caso se señalan estas acciones no autorizadas.
- La dimensión de seguridad disponibilidad garantiza que ningún evento que pueda ocurrir en la red impedirá el acceso autorizado a los elementos, la información almacenada, los flujos de información, los servicios y las aplicaciones de la red. Las soluciones de recuperación en caso de desastre y para restablecimiento de la red se incluyen en esta categoría.
- La dimensión de seguridad privacidad impide conocer información observando las actividades de la red, por ejemplo los sitios web que un usuario ha visitado, la ubicación geográfica del usuario y las direcciones IP y los nombres DNS de los dispositivos de una red del proveedor de servicios.

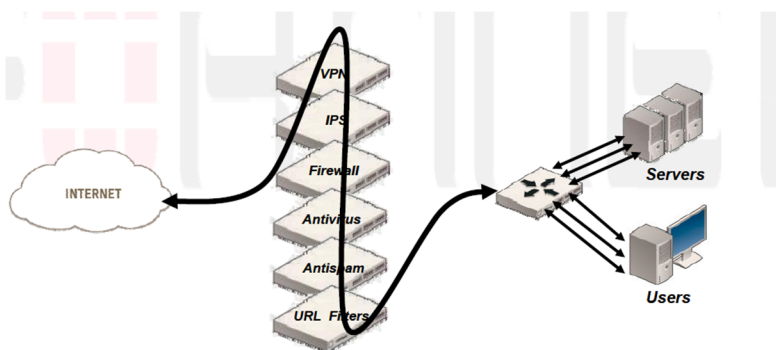
La arquitectura de seguridad de las redes es una referencia para definir políticas de seguridad globales, planes de respuesta ante incidentes y recuperación.

La arquitecturas tecnológicas ha teniendo en cuenta cada una de las dimensiones de seguridad en cada una de las capas y planos durante la fase de definición y planificación, puede servir de base para una evaluación de la seguridad, para determinar los efectos del programa de seguridad en las dimensiones, capas y planos de seguridad, cuando se aplican las políticas y procedimientos y se hace efectiva la tecnología. Una vez implantado, es necesario mantener el programa de seguridad, es decir adaptarlo al entorno de seguridad cambiante.

Tendencias en seguridad

La seguridad de la red de telecomunicaciones de pequeñas y medianas empresas con múltiples puntos aumenta la complejidad de solución como se observa en la siguiente figura 38.

Figura 38. **Tendencias en seguridad**



Fuente: Vanegas, Orlando. Tendencias de Seguridad en Telecomunicaciones.

