



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER  
BIBLIOTECA EDUARDO COTE LAMUS



## RESUMEN – TESIS DE GRADO

**AUTORES:** ALBA MILENA MARTINEZ LOPEZ

**FACULTAD:** DE INGENIERIA

**PLAN DE ESTUDIOS:** INGENIERIA DE SISTEMAS

**DIRECTOR:** ING. JOSE MARTIN CALIXTO CELY

**TITULO DE LA TESIS:** ANALISIS DEL ESTANDAR IPsec INTERNET PROTOCOL SECURITY, ESTUDIO COMPARATIVO DE SUS DIFERENTES TECNOLOGIAS Y TIPOS DE APLICACIONES PRACTICAS.

### RESUMEN

IPSec esta definido en el RFC 2401 de la IETF Internet Engineering Task Force (Grupo de Trabajo en Ingeniería de Internet). Y consiste en un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), Algoritmos de *hash* (MD5, SHA-1) y certificados digitales X509v3.

IPSec es un estándar que cubre la carencia de seguridad del protocolo IP. Otorgándonos la posibilidad de usar redes IP para aplicaciones críticas.

### CARACTERÍSTICAS

PAGINAS 243 PLANOS        ILUSTRACIONES        CD-ROM 1

ANALISIS DEL ESTANDAR IPSec INTERNET PROTOCOL SECURITY,  
ESTUDIO COMPARATIVO DE SUS DIFERENTES TECNOLOGIAS Y  
TIPOS DE APLICACIONES PRÁCTICAS

ALBA MILENA MARTINEZ LOPEZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER  
FACULTAD DE INGENIERIA  
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS  
SAN JOSE DE CUCUTA  
2009

ANALISIS DEL ESTANDAR IPSec INTERNET PROTOCOL SECURITY,  
ESTUDIO COMPARATIVO DE SUS DIFERENTES TECNOLOGIAS Y TIPOS  
DE APLICACIONES PRÁCTICAS

ALBA MILENA MARTINEZ LOPEZ

Trabajo de grado presentado como requisito para optar al título  
de Ingeniero de Sistemas

Director  
JOSÉ MARTÍN CALIXTO CELY  
Ingeniero de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER  
FACULTAD DE INGENIERIA  
PLAN DE ESTUDIOS DE INGENIERIA DE SISTEMAS  
SAN JOSE DE CUCUTA  
2009



UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

## ACTA DE SUSTENTACION DE UN TRABAJO DE GRADO

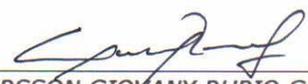
FECHA: 23 DE JULIO DE 2009 HORA: 2:30 p. m.  
LUGAR : AUDITORIO "J. J. MALDONADO" EDIFICIO AULAS SUR - UFPS  
PLAN DE ESTUDIOS: INGENIERIA DE SISTEMAS  
TITULO DE LA TESIS: "ANALISIS DEL ESTANDAR IPsec INTERNET PROTOCOL SECURITY, ESTUDIO COMPARATIVO DE SUS DIFERENTES TECNOLOGIAS Y TIPOS DE APLICACIONES PRACTICAS".  
JURADOS: ING. JEAN POLO CEQUEDA OLAGO  
ING. GERSSON RUBIO GONZALEZ  
ING. CARLOS EDUARDO PARDO GARCIA  
DIRECTOR: INGENIERO JOSE MARTIN CALIXTO CELY.

NOMBRE DE LOS ESTUDIANTES:	CODIGO	CALIFICACION
		NUMERO LETRA
ALBA MILENA MARTINEZ LOPEZ	0151436	3,9 TRES, NUEVE

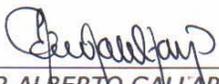
# A P R O B A D A

FIRMA DE LOS JURADOS

  
ING. JEAN POLO CEQUEDA OLAGO

  
ING. GERSSON GIOVANY RUBIO GONZALEZ

  
ING. CARLOS EDUARDO PARDO GARCIA

Vo.Bo.   
OSCAR ALBERTO GALLARDO PEREZ  
Coordinador Comité Curricular

Betty M.

## **AGRADECIMIENTOS**

La autora expresa sus agradecimientos a:

JOSE MARTIN CALIXTO CELY. Ingeniero de sistemas, por su colaboración y apoyo en todo.

A LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, cuyas aulas me brindaron la oportunidad de prepararme.

## CONTENIDO

	Pág.
INTRODUCCION	17
1. ASPECTOS GENERALES	19
2. INTERNET PROTOCOL SECURITY IPsec	22
2.1 ARQUITECTURA IPSEC	23
2.2.1 Seguridad IPsec en los modelos TCP/IP y OSI	25
2.3 MODOS DE FUNCIONAMIENTO DE IPSEC	26
2.4 ASOCIACIONES DE SEGURIDAD (SA)	29
2.4.1 Índice de parámetros de seguridad (security parameter index, spi)	30
2.4.2 Gestión de las SA	30
2.4.3 Parámetros	30
2.5 POLÍTICAS DE SEGURIDAD EN IPSEC	31
2.6 SERVICIOS DE SEGURIDAD OFRECIDOS POR IPSEC	32
2.7 IP ENCAPSULATING SECURITY PAYLOAD (ESP)	34

2.7.1 Funcionamiento ESP	37
2.8 AUTHENTICATION HEADER (AH)	38
2.8.1 Funcionamiento AH	41
2.9 INTERNET KEY EXCHANGE (IKE)	42
2.10 TECNOLOGIA PKI	45
2.11 IMPLEMENTACIÓN DE IPSEC	47
2.12 CONFIGURACIONES DE IPSEC	48
2.12.1 Configuración de IPsec en Windows 2000 Server	49
2.12.2 Como crear una directiva IPsec	51
2.12.3 Como crear una lista de filtro de la redA a la redB	52
2.12.4 Como crear una lista de filtros de la redB a la redA	55
2.12.5 Cómo configurar una regla para un túnel de la RedA a la RedB	56
2.12.6 Cómo configurar una regla para un túnel de la RedB a la RedA	61
2.12.7 Cómo asignar la nueva directiva IPsec a la puerta de enlace de Windows 2000	65
2.12.8 Cómo configurar el filtrado de RRAS	69

2.12.9	Cómo configurar rutas estáticas en RRAS	72
2.12.10	Probar el túnel IPSec	74
2.13	ESTABLECIENDO LA CONEXIÓN	76
2.13.1	Autenticación	76
2.13.2	Problemas Comunes	78
2.14	APLICACIONES PRÁCTICAS DE IPSEC	83
2.14.1	La interconexión segura de redes locales (intranet)	83
2.14.2	El acceso seguro de usuarios remotos	85
2.14.3	la extranet	87
3.	CONCLUSIONES	89
4.	RECOMENDACIONES	90
	BILBLOGRAFIA	90
	ANEXOS	93