# ÍNDICE

# ÍNDICE

**INTRODUCCIÓN** 1

**ANTECEDENTES**

HISTORIA DE INTERNET 5

INTRODUCCIÓN AL SERVIDOR DE NOMBRE DE DOMINIO (DNS) 9

**CAPÍTULO 1 CRIPTOGRAFÍA**

1.1 CRIPTOGRAFÍA 18

1.2 CRIPTOGRAFÍA CLÁSICA 20

1.2.1 EVOLUCIÓN DE LOS MÉTODOS 21

1.3 CRIPTOGRAFÍA MODERNA 25

1.4. CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE SECRETA 27

1.4.1 ALGORITMO SIMÉTRICO EN BLOQUE 28

1.4.2 ALGORITMO SIMÉTRICO EN FLUJO 30

1.5 CRIPTOGRAFÍA ASIMÉTRICA O DE CLAVE PÚBLICA 31

**CAPÍTULO 2 EXTENSIONES DE SEGURIDAD A LOS SERVIDORES DE NOMBRE DE DOMINO (DNSSEC)**

2.1 DNSSEC 38

2.2 ORGANISMOS DE REGULACIÓN 38

2.2.1 ISOC 38

2.2.2 IETF 40

2.3 ORÍGENES DE DNSSEC 41

2.4 AMENAZAS DEL DNS 44

2.5 VULNERABILIDADES QUE TIENEN LOS DNS 45

2.5.1 INTERCEPTACIÓN DE PAQUETES 45

2.5.2 ID GUESSING AND QUERY PREDICTION 46

2.5.3 NAME CHAINING 48

2.5.4 BETRAYAL BY TRUSTED SERVER 50

2.5.5 DNS DENEAL OF SERVICE
("NEGACIÓN DE SERVICIO" O "DNS DOS") 52
2.6 ¿QUÉ ES DNSSEC? 52
2.7 RESOURCE RECORD SIGNATURE (RRSIG) 55
2.8 DNSKEY 57
2.9 NSEC 59
2.10 DELEGATION SIGNER (DS) 61
2.11 COMPARACIÓN DE MOVILIDAD REDUCIDA (CD) Y
AUTENTICACIÓN DE DATOS (AD) 61

**CAPÍTULO 3 DESARROLLO E IMPLEMENTACIÓN**

3.1 SISTEMA OPERATIVO 64
3.2 UNIX Y SUS DERIVADOS 66
3.3 CARACTERÍSTICAS DEL BIND 69
3.4 IMPLEMENTACIÓN DE EXTENSIONES DE SEGURIDAD 74
3.4.1 RNDC 75
3.4.2 OPCIONES DE RNDC 78
3.5 HERRAMIENTAS DE DIAGNÓSTICO 80
3.5.1 PING 80
3.5.2 DIG (DOMAIN INFORMATION GROPER) 82
3.5.3 NSLOOKUP (NAME SYSTEM LOOKUP 84
3.6 TSIG 86
3.6.1 GENERACIÓN DE LLAVES TSIG 87
3.7 GENERACIÓN DE LLAVES DNSSECBIS 91
3.7.1 DNSKEY 93
3.7.2 RRSIG 98

**CONCLUSIONES** 101

**ANEXOS**

ANEXO1 RAÍZ DE BASE DE DATOS DE ZONA 105
BIBLIOGRAFÍA 122