

Contenido

Introducción.....	i
A. Antecedentes.....	ii
B. Definición del problema.....	iii
C. Objetivos.....	iv
D. Contribuciones.....	iv
E. Estructura de la tesis.....	v
CAPÍTULO 1. Conceptos Básicos	1
1.1. Redes de datos	2
1.1.1. Conceptos básicos.....	3
a) Dirección física	3
b) Dirección IP	4
c) Resolución de direcciones	5
d) Definición de protocolo	6
e) Definición de puertos	7
f) Definición de puerta de enlace	7
1.2. Modelo OSI y TCP/IP.	8
1.2.1 Modelo OSI	8
1.2.1.1 Esquema del modelo OSI	8
a) Capa física	9
b) Capa de enlace	9
c) Capa de red	11
d) Capa de transporte	11
e) Capa de sesión	12
f) Capa de presentación	12
g) Capa de aplicación	13
1.2.2 Modelo TCP/IP	13
1.2.2.1 Introducción al modelo TCP/IP	13
1.2.2.2 Arquitectura del protocolo TCP/IP	14
a) Capa de acceso a red	16
1. Protocolo ARP	17
b) Capa de internet	17
1. Protocolo IP	18
2. Protocolo ICMP	19
c) Capa de transporte	19
1. Protocolo TCP	20
2. Protocolo UDP	20
3. Three-Way Handshake	21



d) Capa de aplicación	22
1. Protocolo TELNET	22
2. Protocolo FTP	22
3. Protocolo HTTP	23
4. Protocolo SMTP	23
5. Protocolo DNS	24
6. Protocolo DHCP	25
1.3 Protocolo de administración SNMP	25
1.4 Protocolo de administración RMON	27
1.5 Protocolos utilizados en menor volumen.....	28
CAPÍTULO 2. Conceptos Generales de Seguridad	29
2.1. Principios básicos de seguridad.....	30
1. Integridad.....	31
2. Disponibilidad	31
3. Confidencialidad.....	32
2.2. Vulnerabilidades, amenazas, riesgo y control	32
2.3. Ataques	35
2.3.1. Fases de un ataque.	36
2.3.2. Ataques físicos	38
2.3.3. Ataques lógicos	39
2.3.4. Ingeniería social	47
2.4. Controles de seguridad	48
2.5. Análisis de riesgo	49
CAPÍTULO 3. Mecanismos de seguridad en red	52
3.1. Planeación de la seguridad en red.....	53
3.2 Estrategias de seguridad.....	54
1. Defensa perimetral.....	55
2. Seguridad en profundidad.....	55
3. Eslabón más débil.....	56
4. Seguridad basada en red	56
5. Seguridad basada en host.....	56
6. Principio de menor privilegio	57
7. Seguridad por oscuridad	57
8. Simplicidad.....	58
9. Punto de ahogo	58
10. Diversidad de la defensa	58
3.3 Servicios seguros	59
1. Cifrado.....	60
2. Seguridad en servidores web	61
3. SSL	63
4. TLS	65
5. SSH.....	65
6. VPN	66



7. NAT	68
8. Kerberos.....	69
9. Active Directory	69
3.4. Control de acceso	70
3.4.1 Modelos de control de acceso	72
a) Matriz de acceso	72
b) Bell-Lapadula	72
3.4.2 Métodos de autenticación	73
a) Algo que se sabe	74
b) Algo que se tiene	75
c) Algo que se es	75
d) Ubicación física	76
3.4.3 Por la manera de autenticar	76
a) Unilateral	76
b) Mutua	77
c) Tercero confiable	77
3.4.4 Autorización	77
3.5 Seguridad física	79
3.5.1 Factores que afectan la seguridad física	80
3.6. Mecanismos de monitoreo, de control y seguimiento	82
3.7 Firewall	83
a) Firewall de red	84
b) Firewalls de host	85
3.8 Auditoría, monitoreo y detección de intrusos	85
a) Auditoría	86
b) Sistema detector de intrusos	87
3.9. Seguridad en redes inalámbricas	88
a) WEP	89
b) WPA	90
c) WPA2	91
d) Hotspot	91
3.10. Sensores y herramientas	92
a) Snort	92
b) Cacti	93
c) Nagios	93
d) Ntop	93
e) Herramientas útiles para el monitoreo	94
3.11. Seguridad en equipos finales	94
3.11.1 Actividades de fortalecimiento	95
3.12. Estándares internacionales	97
a) Serie ISO 27000.....	98
b) Recomendaciones NIST serie 800.....	98
c) Suite B de criptografía	99



3.13. Políticas de seguridad	100
3.14 Planes de contingencia y recuperación	102
CAPÍTULO 4. Buenas Prácticas de Seguridad	104
4.1. Justificar por qué invertir en seguridad	105
4.2. Buenas prácticas en la administración de la seguridad con base en estándares	106
4.3. Buenas prácticas de seguridad en redes.....	110
4.4. Respaldo de información	112
4.5. Seguridad en aplicaciones	113
4.6. Seguridad en sistemas operativos	114
4.6.1. Hardening en plataformas Microsoft	115
4.6.2. Hardening en Unix y Linux	116
4.7. Buenas prácticas de seguridad en servidores.....	117
4.8. Seguridad en dispositivos removibles y verificaciones regulares al sistema	118
4.9. Concientizar a los usuarios finales	119
4.10. Controles críticos de seguridad.....	120
4.11. Pruebas de penetración	122
4.12. Implementar un Plan de Continuidad y Recuperación de Desastres (DRP).....	123
CAPÍTULO 5. Propuesta de implementación, caso práctico	126
5.1. Obtención de información de los activos y la infraestructura	127
5.2. Análisis de riesgo de la situación actual	134
5.3. Alcance y requerimientos de la propuesta	143
5.4. Desarrollo de la implementación	149
5.5. Limitantes de la implementación	152
5.6. Posibilidades de crecimiento	154
Conclusiones.....	156
Apéndice A. Clasificación de atacantes	160
Apéndice B. Ataques lógicos	162
Apéndice C. Mecanismos de seguridad en red	174
Apéndice D. Análisis de controles, políticas de uso de red y acceso a internet, encuestas aplicadas y sus resultados	195
Glosario	233
Referencias	246
Índice de figuras y tablas.....	254