

Figuras

CAPÍTULO 1. Conceptos Básicos

Figura 1.1 Clasificación de las redes por alcance, topología y estándar.....	3
Figura 1.2 Dirección física (MAC Address).....	4
Figura 1.3 Resolución de direcciones.....	6
Figura 1.4 Capas del modelo OSI.....	8
Figura 1.5 Arquitectura TCP/IP.....	14
Figura 1.6 Encapsulado de los datos.....	15
Figura 1.7 Estructura de datos.....	16
Figura 1.8 Equivalencia de la capa de acceso a red del modelo TCP/IP con las tres primeras capas del modelo OSI.....	16
Figura 1.9 Protocolo ARP.....	17
Figura 1.10 Datagrama IP.....	18
Figura 1.11 Protocolo ICMP.....	19
Figura 1.12 Cabecera TCP.....	20
Figura 1.13 Cabecera UDP.....	21
Figura 1.14 Three-way handshake.....	21
Figura 1.15 Protocolo HTTP.....	23
Figura 1.16 Traducción DNS.....	24
Figura 1.17 DNS.....	24
Figura 1.18 DHCP.....	25
Figura 1.19 Protocolo SNMP.....	26

CAPÍTULO 2. Conceptos Generales de Seguridad

Figura 2.1 Principios de seguridad.	30
Figura 2.2 Diagrama amenaza, vulnerabilidad y activo.	33
Figura 2.3 Vulnerabilidades de los sistemas de cómputo.	34
Figura 2.4 Fases de un ataque.	36
Figura 2.5 Tipos de ataques.....	37
Figura 2.6 Envenenamiento ARP.....	42
Figura 2.7 Pharming.....	43
Figura 2.8 Phishing.....	44
Figura 2.9 Botnet.....	44
Figura 2.10 Man in the middle.	45

CAPÍTULO 3. Mecanismos de seguridad en red

Figura 3.1 Modelo de seguridad.....	54
Figura 3.2 Modelo simplificado de cifrado simétrico.	60
Figura 3.3 Criptografía de clave pública.	61
Figura 3.4 Ubicación relativa de las herramientas de seguridad en la pila de protocolos TCP/IP....	63
Figura 3.5 Pila de protocolos SSL.....	64



Figura 3.6 Handshake de SSL.....	64
Figura 3.7 SSH.....	65
Figura 3.8 VPN Host to Host.....	66
Figura 3.9 VPN Host to Network.....	66
Figura 3.10 VPN Network to Network.....	66
Figura 3.11 Protocolos VPN en el modelo OSI.....	67
Figura 3.12 Diagrama de funcionamiento de un NAT.....	68
Figura 3.13 Matriz de acceso ejemplo.....	72
Figura 3.14 Autenticación Unilateral.....	76
Figura 3.15 Autenticación mutua.....	77
Figura 3.16 Autenticación por medio de un tercero confiable.....	77
Figura 3.17 Firewall.....	83
Figura 3.18 Esquema general de un Sistema Detector de Intrusos.....	88
Figura 3.19 Hotspot.....	92

CAPÍTULO 4. Buenas Prácticas de Seguridad

Figura 4.1 modelo PDCA.....	107
-----------------------------	-----

CAPÍTULO 5. Propuesta de implementación, caso práctico

Figura 5.1 Organigrama Dirección General Colegio de Ciencias y Humanidades.....	127
Figura 5.2 Análisis de Riesgos NIST 800-30.....	128
Figura 5.3 Diagrama de red, antes de la implementación del esquema de seguridad.....	134
Figura 5.4 Propuesta de esquema de seguridad para la red.....	147

Apendice B.

Figura B.1 Clasificación software malicioso.....	164
Figura B.2 Símbolo de cifrado en sitios Web, protección contra phishing.....	169

Apéndice C.

Figura C.1 Cifrado criptografía de clave pública.....	178
Figura C.2 Firewall con dos interfaces de red.....	181
Figura C.3 Screened host firewall.....	182
Figura C.4 Screened subnet firewall.....	183
Figura C.5 Filtrado de paquetes.....	185
Figura C.6 Firewall de aplicación.....	187
Figura C.7 Firewall basado en hardware.....	188
Figura C.8 IDS.....	189
Figura C.9 NIDS.....	191
Figura C.10 DIDS.....	192

Tablas

CAPÍTULO 1. Conceptos Básicos

Tabla 1.1 Direcciones IP.....	5
Tabla 1.2 Direcciones IP privadas.....	5
Tabla 1.3 Mensajes ICMP.....	19

CAPÍTULO 2. Conceptos Generales de Seguridad

Tabla 2.1 Amenazas Físicas.....	38
Tabla 2.2 Amenazas Lógicas.....	40

CAPÍTULO 3. Mecanismos de seguridad en red

Tabla 3.1 Amenazas en la web.....	62
Tabla 3.2 Herramientas útiles para el monitoreo.....	94
Tabla 3.3 Suite B criptografía.....	99

CAPÍTULO 4. Buenas Prácticas de Seguridad

Tabla 4.1 Escala de gravedad de un incidente.....	105
Tabla 4.2 Herramientas de análisis de vulnerabilidades.....	114

CAPÍTULO 5. Propuesta de implementación, caso práctico

Tabla 5.1 Lista de documentos solicitados para revisión	129
Tabla 5.2 Resumen de infraestructura.....	130
Tabla 5.3 Relación de equipos críticos para la institución.....	131
Tabla 5.4 Relación de costos de infraestructura crítica.....	132
Tabla 5.5 Servicios críticos para la institución.....	133
Tabla 5.6 Identificación de vulnerabilidades.....	135
Tabla 5.7 Matriz de nivel de atención de riesgos.....	140
Tabla 5.8 Probabilidad de impacto y ocurrencia.....	140
Tabla 5.9 Controles recomendados, con base en el análisis de riesgo.....	144
Tabla 5.10 Riesgos residuales.....	153

Apéndice C.

Tabla C.1 Comparación de funciones hash seguras.....	175
Tabla C.2 Algoritmos de cifrado simétrico convencionales.....	176
Tabla C.3 Aplicaciones para criptosistemas de clave pública.....	177
Tabla C.4 Comparación de funciones hash seguras.....	180
Tabla C.5 Uso y Nivel de Seguridad de Firewall.....	184
Tabla C.6 Estados de una conexión.....	186
Tabla C.7 HIDS.....	190
Tabla C.8 IDS por software.....	193