

Tabla de Contenido

1	<i>Introducción</i>	1
2	<i>Antecedentes y consecuencias de la falta de Seguridad</i>	4
2.1	Antecedentes	4
2.2	Consecuencias de la Falta de Seguridad	5
2.3	Causas que pueden originar dichas consecuencias	7
3	<i>Elementos Administrativos de la Seguridad</i>	10
3.1	Política de Seguridad	10
3.1.1	Cuantificación de Riesgos	11
3.1.2	Compromiso Gerencial	12
3.1.3	Políticas de Respaldos	13
3.1.4	Políticas Antivirus	14
3.2	Organización y División de responsabilidades	15
3.3	Seguridad Física y Contra Incendios	17
3.4	Políticas de Personal	23
3.5	Seguros	24
3.5.1	Problemas tradicionales	24
3.5.2	Áreas de Riesgo Asegurables	24
3.5.3	Servicios de Seguro Especializados en el ramo de la Computación.	26
3.5.4	Seguimiento de los cambios en los riesgos	27
4	<i>Elementos Técnicos y Procedimentales de la Seguridad</i>	28
4.1	Seguridad de los Sistemas	28
4.2	Seguridad de la Aplicación	31
4.3	Estándares	33
4.4	Función de Auditoría	36
4.5	Planes de Contingencia	37
4.5.1	Tipos de desastre	37
4.5.2	Procedimientos en caso de desastres	37
4.5.3	Simulacros de desastres	39
4.5.4	Análisis de Impacto	39
5	<i>Auditoría de Sistemas</i>	41
5.1	Conceptos básicos de Auditoría	41
5.1.1	Tipos de Auditoría	41
5.1.2	Clasificación por Naturaleza del Equipo	42

5.2	Auditoría de Sistemas	42
5.2.1	Clasificación de acuerdo a su enfoque	42
5.2.2	Clasificación de acuerdo al alcance	42
5.2.3	Herramientas y Técnicas utilizadas	43
5.3	Análisis de los delitos a través del computador	43
5.3.1	Por qué pueden cometerse delitos por computador	43
5.3.2	Cómo puede cometerse el delito por computador	44
5.3.3	Perfil de los que comenten delitos por computador	46
5.3.4	Factores que han permitido el incremento de delitos por computador	46
5.3.5	Informe de Auditoría (elementos)	46
6	<i>Criptografía</i>	48
6.1	¿De dónde viene y qué es?	48
6.2	Componentes	48
6.3	Propiedades	49
6.4	Evolución	50
6.5	Clasificación	58
6.6	¿Cómo encriptar el correo electrónico?	58
7	<i>Los Cortafuegos o Firewalls</i>	60
7.1	¿Qué son los Cortafuegos en Informática?	60
7.2	Historia de los Cortafuegos	61
7.2.1	Primera generación – cortafuegos de red: filtrado de paquetes	63
7.2.2	Segunda generación – cortafuegos de estado	65
7.2.3	Tercera generación - cortafuegos de aplicación	65
7.2.4	Acontecimientos posteriores	66
7.3	Tipos de cortafuegos	68
7.3.1	Nivel de aplicación de pasarela	68
7.3.2	Circuito a nivel de pasarela	68
7.3.3	Cortafuegos de capa de red o de filtrado de paquetes	69
7.3.4	Cortafuegos de capa de aplicación	69
7.3.5	Cortafuegos personal	70
7.4	Recordatorio de las Capas del modelo OSI	70
7.5	Opciones en el mercado	71

8	<i>Ingeniería Social</i>	72
8.1	¿Qué es Ingeniería Social?	72
8.2	¿Cómo se hace Ingeniería Social?	76
8.2.1	Suplantación de identidad o <i>Phishing</i>	79
8.2.2	Spear Phishing	85
8.2.3	Simple embaucamiento	87
8.2.4	Envío de archivos adjuntos en el correo electrónico	87
8.2.5	Recolección de hábitos de las víctimas potenciales	88
8.2.6	Revisión de desperdicios o basura	89
8.2.7	Vishing	91
8.3	¿Hasta dónde es ético hacer Ingeniería Social?	91
8.4	Proliferación de Redes Sociales y sus implicaciones en la Ingeniería Social	92
8.5	¿Cómo se evita la Ingeniería Social?	96
9	<i>Normas Iso 27000</i>	100
9.1	Qué es ISO?	100
9.2	¿Qué es la norma ISO 27000?	103
9.3	Quiénes conforman la familia de la Norma ISO 27000?	104
9.4	¿Qué obtengo si implanto ISO 27000 en mi organización?	106
9.5	¿En qué tipo de empresas puede implantarse ISO 27000?	106
9.6	Ventajas de implantar ISO 27000	108
9.7	¿Qué hacer para implantar ISO 27000?	109
10	<i>Misceláneas</i>	113
10.1	Navegación segura	113
10.2	Contraseñas seguras	113
10.3	Amenazas potenciales	115
10.4	Medidas de protección	119
11	<i>Referencias Bibliográficas</i>	120
11.1	Bibliografía	120
11.2	Webgrafía	120