

PROPUESTAS PARA IMPULSAR LA SEGURIDAD INFORMÁTICA EN MATERIA DE EDUCACIÓN

Índice general

Introducción

Panorama General	1
Objetivo General	2
Objetivos Particulares	3

Capítulo 1. Definiciones e historia de la seguridad informática5

1.1 Conceptos Básicos.....	6
1.1.1 Definición de Seguridad Informática	7
1.2 Principios.....	9
1.3 Antecedentes de la Seguridad Informática a nivel Nacional e Internacional.....	12
1.4 Desarrollo de la Seguridad Informática en México y en el Mundo	31
1.5 Importancia de la Seguridad Informática	38
1.6 Situación Actual de México con respecto al exterior.....	46

Capítulo 2. Amenazas y Vulnerabilidades de la seguridad informática49

2.1 Clasificación general de amenazas.....	50
2.1.1 Humanas.....	50
2.1.2 Lógicas (software).....	52
2.1.3 Físicos	56
2.2 Clasificación general de vulnerabilidades	57
2.3 Identificación de las principales amenazas y vulnerabilidades a nivel Nacional e Internacional.....	61

Capítulo 3. Tendencias de la seguridad informática en México85

3.1 Antecedentes	86
3.2 Situación actual	87
3.3 Tendencias.....	101

Capítulo 4. Análisis en materia de educación.113

4.1 Educación Básica (Primaria y Secundaria)	114
4.2 Educación Media.....	116
4.2.1 Escuela Nacional Preparatoria (ENP)	116
4.2.2 Colegio de Ciencias y Humanidades (CCH).....	118
4.3 Educación Superior	119

Capítulo 5. Propuesta.....	139
5.1 Propuesta para los diferentes niveles educativos	140
5.2 Modelo educativo.....	145
Capítulo 6. Contenidos desarrollados	151
6.1 Familia de Normas ISO / IEC 27000	156
6.2 Metodologías para el análisis de riesgo	162
6.3 Herramientas de seguridad	174
6.3.1 Monitoreo	175
6.3.2 Auditoría	183
6.3.3 Criptografía	185
6.3.4 Escaneo	187
6.3.5 Filtrado	187
6.3.6 Detección de intrusos	194
6.3.6.1 Tipos de intrusos	194
6.3.6.2 Composición de los IDS	195
6.3.6.3 Clasificación de los IDS	197
6.3.7 Autenticación	204
6.4 Auditoría	209
6.4.1 Definición	210
6.4.2 Auditoría interna y auditoría externa	211
6.4.3 Características de la Auditoría informática	211
6.4.4 Tipos y clases de auditorías	212
6.4.5 Fases de una auditoría	213
6.4.6 Auditoría de la seguridad de la información	217
6.4.7 Enfoques de la Auditoría Informática	219
6.4.8 Herramientas y técnicas para la auditoría informática	222
6.4.9 Perfil Profesional del auditor informático	223
6.5 Seguridad en redes inalámbricas	225
6.5.1 Definición de la seguridad inalámbrica	225
6.5.2 Implementación de los atributos de seguridad	228
6.5.3 Servicios de seguridad en redes inalámbricas	229
6.5.3.1 Confidencialidad	229
6.5.3.2 Autenticación	232
6.5.3.3 Integridad de datos en redes inalámbricas	234
6.5.3.4 Disponibilidad en redes inalámbricas	235
6.5.3.5 No repudio (rendición de cuentas)	236
6.5.4 Principales amenazas de seguridad en redes inalámbricas	236
6.6 Seguridad en bases de datos	238
6.6.1 Sistema de Gestión de Bases de Datos (SGBD)	239
6.6.2 Confidencialidad de la BD	240
5.6.2.1 Deducción de información confidencial de una BD	241
6.6.3 Disponibilidad de la BD	242
6.6.4 Integridad de la BD	246
6.6.5 Mecanismo de seguridad en SGBD	249
6.7 Ética Informática	250
6.7.1 Contenidos de la ética informática	252

6.7.2 Código deontológico	253
6.7.3 Objetivos del código deontológico	253
6.7.4 Funciones del código deontológico	254
6.7.5 Código Deontológico de los Ingenieros Informáticos	255
6.8 Legislación y delitos informáticos	256
6.8.1 Delitos Informáticos	256
6.8.2 Tipos de delitos informáticos	259
6.8.3 Legislación Internacional	260
Conclusiones	273
Anexos	279
Glosario de Términos	281
Bibliografía	309

Índice de Gráficas

Gráficas

Capítulo 1

1.1	Histórico de usuarios de Internet en México 2005-2010 (cifras en millones)	33
1.2	Usuarios de Internet por lugar de acceso 2000-2010	34
1.3	Distribución de usuarios de Internet por grupos de edad, 2010	35
1.4	Dispositivos usados por el Internauta Mexicano para conectarse a Internet	36
1.5	Conexión por día de la semana	36
1.6	Principales actividades sociales online	37
1.7	Uso de redes sociales	38
1.8	Principales preocupaciones de los usuarios	41
1.9	Amenazas percibidas de mayor riesgo	42
1.10	Importancia de la seguridad informática	43

Capítulo 2

2.1	Incidentes Anuales	63
2.2	Tipos de incidentes en el 2010	64
2.3	Tipos de incidente en el 2008	65
2.4	Tipos de incidente en el 2007	66
2.5	Volúmenes de Spam mundiales y el spam como un porcentaje de todo el correo	67
2.6	Nuevos zombis que envían spam por mes	68
2.7	Distribución de los sitios Web de Phishing	71
2.8	Crecimiento del Malware de robo de contraseñas	72
2.9	Tipos de Malware	73
2.10	Evolución de malware activo durante el primer semestre del 2009	74
2.11	Países con mayor porcentaje de malware (Enero – Junio) 2009	75
2.12	Países con mayor porcentaje de malware en la web	76
2.13	Reproducción de Spam por país	77
2.14	Spam por continente	78
2.15	Tipos de Malware detectados por mes	80

Capítulo 3

3.1	Índice de Competitividad en México (2004-2005/2009-2010)	86
3.2	Distribución del presupuesto para la GSI	95
3.3	Obstáculos para lograr una adecuada gestión de la SI	99

Índice de Tablas

Capítulo 1

1.1 Acontecimientos internacionales que marcaron el desarrollo de la seguridad informática	13
1.2 Acontecimientos relevantes de la seguridad informática en México	26
1.3 Países con el mayor número de usuarios de Internet	32
1.4 Situación actual de México con respecto al exterior	46

Capítulo 2

2.1 Las amenazas más peligrosas en los últimos 20 años	62
2.2 Países productores de nuevos zombis por trimestre	69
2.3 Países con mayor producción de spam	69
2.4 Resumen de los informes analizados por las diferentes empresas	82

Capítulo 3

3.1 Responsabilidad de la seguridad informática	94
3.2 Casos de violaciones a la seguridad informática	96
3.3 Entidad de notificación de denuncia	96
3.4 Frecuencia de pruebas de seguridad en la organización	97
3.5 Mecanismos utilizados para la protección de los sistemas de información	98
3.6 Clasificaciones de personal, dedicado al tema de la SI	100

Capítulo 4

4.1 Conectividad de las escuelas públicas de educación básica del DF.....	115
4.2 Planes y Programas de Estudio 1996	116
4.3 Mapa curricular del plan de estudios del CCH	118
4.4 Taller de Cómputo I y II	119
4.5 Plan de Estudios de la carrera de Arquitectura	120
4.6 Plan de Estudios de la carrera Medico Cirujano	121
4.7 Plan de Estudios de la carrera de Derecho	122
4.8 Plan de Estudios de la carrera de Contaduría.....	123
4.9 Plan de Estudios de la carrera de Ciencias Políticas y Administración Pública	124
4.10 Plan de Estudios de la carrera de Economía	125
4.11 Plan de Estudios de la carrera de Química.....	126
4.12 Plan de Estudios de la carrera Trabajo Social	127
4.13 Plan de Estudios de la carrera en Lengua y Literatura Hispánicas	128
4.14 Plan de Estudios de la carrera de Medicina y Veterinaria.....	129
4.15 Plan de Estudios de la carrera de Cirujano Dentista	130

4.16 Plan de Estudios 2009 de la Facultad de Ingeniería de la UNAM	131
4.6 Módulo: Redes y Seguridad	133

Capítulo 6

6.1 Divisiones de Auditoría Informática	213
6.2 Perfil Profesional del auditor informático	224
6.3 Las 10 amenazas más relevantes	236

Índice de Figuras

Capítulo 1

1.1 Datacenter o Centro de Cómputo	39
--	----

Capítulo 2

2.1 Principales Vulnerabilidades	58
--	----

Capítulo 3

3.1 Enciclomedia	89
3.2 Telemedicina	90

Capítulo 5

5.1 Cuadro resumen de la educación en México	145
5.2 Modelo educativo de seguridad informática	90

Capítulo 6

6.1 Historia de ISO 27001	157
6.2 Análisis y Gestión de MAGERIT	164
6.3 Modelo MAGERIT	165
6.4 Etapas del Submodelo de procesos MAGERIT	166
6.5 Modelo de Análisis y gestión de riesgos CRAMM.....	170
6.6 Principales actividades de análisis y gestión de riesgos CRAMM	172
6.7 Esquema de protección mediante un firewall	188
6.8 Firewall.....	189
6.9 Proxy	192
6.10 Ejemplo	199
6.11 Mecanismo de autenticación en Kerberos.....	207
6.12 Uso de herramientas de seguridad.....	209
6.13 Enfoques de la auditoría informática	221
6.14 Bases de datos espejo	246
6.15 Ejemplo de control de acceso basado en roles	248