

Índice de contenido

Cap. 1. Un enfoque nuevo sobre la seguridad en computación: concepto de seguridad total **11**

1. Exigencias para incrementar la seguridad en computación, 11. **1.1.** Concentración del procesamiento de aplicaciones más grandes y de mayor complejidad, 12. **1.2.** Dependencia en el personal clave, 13. **1.3.** Desaparición de los controles tradicionales, 14. **1.4.** Huelgas, terrorismo urbano e inestabilidad social, 15. **1.5.** Mayor conciencia de los proveedores, 15. **2.** Enfoques tradicionales sobre la seguridad en computación, 16. **3.** Concepto de seguridad total en computación, 17. **4.** Resumen, 19.

PRIMERA PARTE. ELEMENTOS ADMINISTRATIVOS

Cap. 2. Definición de una política de seguridad en computación **23**

1. Limitaciones de la seguridad, 23. **2.** Equilibrio entre las medidas de seguridad y los niveles de riesgo, 23. **3.** Cuantificación de los riesgos para la seguridad en computación, 24. **3.1.** Clasificación general de las instalaciones, 25. **3.2.** Identificación de las aplicaciones de riesgo alto, medio y bajo, 26. **3.2.1.** Fase uno: elaboración de una lista de aplicaciones por orden de riesgo, 27. **3.2.2.** Fase dos: cuantificación del riesgo, 27. **3.2.3.** Fase tres: obtención del consenso sobre los niveles de riesgo, 28. **3.3.** Evaluación de las medidas de seguridad, 28. **3.4.** Justificación de las medidas de seguridad en cuanto al costo, 29. **4.** El logro del compromiso con la política de seguridad, 29. **5.** Resumen, 30.

Cap. 3. Organización y división de responsabilidades	32
<p>1. División de responsabilidades, 32. 2. Sistemas de control, interno, 34. 3. Asignación de responsabilidades en cuanto a la seguridad, 35. 4. Sustitución del personal clave, 36. 5. Resumen, 36.</p>	
Cap. 4. Seguridad física y contra incendios	37
<p>1. Ubicación y construcción del centro de cómputo, 37. 1.1. Ubicación, 37. 1.2. Construcción, 38. 1.3. Disposición, 38. 2. Aire acondicionado, 39. 3. Suministro de energía, 40. 4. Riesgo de inundación, 40. 5. Acceso, 41. 5.1. Controles de acceso durante las distintas horas del día o de la noche, 41. 5.2. Acceso de terceras personas, 41. 5.3. Estructura y disposición del área de recepción, 42. 5.4. Alarmas contra robos, 42. 5.5. Tarjetas de acceso y gafetes, 42. 6. Detección de incendios, 43. 7. Protección contra incendios, 44. 8. Extinción de incendios, 44. 9. Mantenimiento, 46. 10. Resumen, 46.</p>	
Cap. 5. Políticas hacia el personal	47
<p>1. Políticas de contratación, 47. 1.1. Verificación de referencias y antecedentes de seguridad, 48. 1.2. Pruebas psicológicas, 48. 1.3. Exámenes médicos, 49. 2. Procedimientos para evaluar el desempeño, 49. 3. Política sobre permisos, 50. 4. Rotación de puestos, 50. 5. Evaluación de las actitudes del personal, 51. 6. Resumen, 51.</p>	
Cap. 6. Los seguros	52
<p>1. Problemas tradicionales, 52. 2. Áreas de riesgo asegurables, 53. 2.1. Ambiente, 53. 2.2. Equipo, 54. 2.2.1. Responsabilidad del seguro, 54. 2.2.2. Riesgos por cubrir, 55. 2.3. Programas y datos, 55. 2.3.1. Definiciones, 55. 2.3.2. Seguros contra pérdida o daños, 56. 2.3.3. Programas de computadora, 56. 2.4. Interrupción comercial y su recuperación, 57. 2.4.1. Evaluación de las consecuencias, 57. 2.4.2. Efectos de la interrupción sobre el costo, 58. 2.5. El personal, 58. 2.5.1. Daños causados por el personal, 58. 2.5.2. Daños al personal, 59. 2.5.3. Actos deshonestos del personal, 59. 2.6. Responsabilidades de terceras personas, 59. 3. Servicios de seguro especializados, 59. 4. Seguimiento de los cambios en los riesgos, 60. 5. Resumen, 61.</p>	

SEGUNDA PARTE. ELEMENTOS TÉCNICOS Y DE PROCEDIMIENTO

- Cap. 7. Seguridad de los sistemas** **65**
1. Alcance del término, 65. 2. Equipo, 65. 3. Los programas, 66. 4. Redes, 67. 5. Terminales, 68. 6. Seguimientos del desempeño, 68. 7. Resumen, 69.
- Cap. 8. Seguridad de las aplicaciones** **70**
1. Alcance, 70. 2. El defecto común: la relación entre la computadora y el usuario, 70. 3. Controles del usuario, 72. 4. Controles de procesamiento de la computadora y seguridad de los archivos, 72. 4.1. Controles de procesamiento de la computadora, 72. 4.2. Seguridad de los archivos, 73. 4.2.1. Almacenamiento de las copias de seguridad en un lugar distante, 73. 4.2.2. Identificación y control de los archivos, 74. 4.2.3. Precisión de los archivos, 74. 4.2.4. Acceso físico a los archivos, 74. 5. Revisión regular de los controles de aplicación, 74. 6. Resumen, 75.
- Cap. 9. Estándares de programación y operación de sistemas** **76**
1. Sistemas y estándares de programación, 78. 1.1. Seguridad y planeación computacional a largo plazo, 78. 1.2. Garantía de calidad de la aplicación a corto plazo, 79. 1.2.1. Seguridad de los programas y del equipo, 80. 1.2.2. Controles de la aplicación, 80. 1.2.3. Supervisión y métodos de trabajo, 81. 1.2.4. Documentación, 82. 2. Operaciones, 83. 3. Resumen, 84.
- Cap. 10. Función de los auditores tanto internos como externos** **85**
1. Funciones generales de la auditoría, 85. 1.1. Auditores externos, 85. 1.2. Auditores internos, 86. 2. Funciones y seguridad de la auditoría en computación, 87. 2.1. Alcance de la auditoría interna respecto a la seguridad en computación, 87. 2.2. Relación entre los auditores internos y los externos, 88. 2.3. Función de la auditoría interna en el desarrollo, 88. 2.4. Función en los sistemas en operación, 89. 2.5. Instrucción y capacitación, 89. 3. Resumen, 91.
- Cap. 11. Planes y simulacros para la recuperación en caso de desastres** **92**
1. Tipos de desastres, 93. 2. Alcance de la planeación contra desastres, 94. 3. Aplicaciones en el proceso de desarrollo, 95. 4. Aplicaciones terminadas, 95. 4.1. Sistemas y programa-

ción, 95. **4.2.** Operaciones de procesamiento, 96. **4.2.1.** Equipo, 96. **4.2.2.** Datos y archivos, 97. **4.2.3.** Papelería, 97. **4.2.4.** Procedimientos en caso de desastres, 97. **5.** Simulacros de desastres, 98. **5.1.** Alcance de los simulacros de desastre, 99. **5.2.** Frecuencia de los simulacros de desastre, 99. **5.3.** Forma de simulacro de desastre, 99. **5.4.** Análisis del impacto, 100. **6.** Resumen, 100.

TERCERA PARTE. APLICACIÓN

Cap. 12. Aplicación de la seguridad efectiva en computación 103

1. Definición del alcance de la seguridad en computación, 103. **2.** Establecimiento de un comité de seguridad en computación, 104. **2.1.** Objetivos, 105. **2.2.** Formación, 105. **2.3.** Método de funcionamiento, 105. **3.** Revisión de la efectividad de la seguridad actual, 106. **4.** Aplicación de las medidas de seguridad, 107. **4.1.** Compromiso, 107. **4.2.** Continuidad, 108. **4.3.** Política, 109. **4.4.** Comunicaciones, 109. **4.5.** Gerencia de seguridad, 110. **4.6.** Tiempo necesario para la aplicación, 110. **4.7.** Prioridad de las actividades de seguridad, 110. **4.8.** Costos, 111. **4.8.1.** Seguridad física, 111. **4.8.2.** Auditoría y control de sistemas, 112. **4.8.3.** Aplicaciones existentes, 112. **5.** Integración de un plan de acción, 113. **6.** Planes y simulacros en caso de desastres, 113. **7.** Planeación y seguridad de largo plazo en computación, 113. **8.** Resumen, 114.

Apéndice 1. Inventario de riesgos de seguridad en computación 115

Apéndice 2. Revisión de la seguridad en computación 117

Apéndice 3. Revisión de la seguridad en computación 119

Apéndice 4. Un caso de estudio: seguridad en computación dentro de una instalación pequeña 120

1. Antecedentes, 120. **2.** Enfoque de la seguridad en computación, 120. **2.1.** Organización y división de responsabilidades, 121. **2.2.** Seguridad de los sistemas, 121. **2.3.** Seguridad física, 121. **2.4.** Seguridad contra incendios, 122. **2.5.** Seguridad de las aplicaciones, 122. **2.6.** Estándares, 122. **2.7.** Políticas hacia el personal, 123. **2.8.** Seguros, 123. **2.9.** Función de la auditoría, 123. **3.** Conclusión, 123. **3.1.** Costos y tiempo, 123.

ÍNDICE DE CONTENIDO

9

Apéndice 5. Glosario de términos de computación

124

Apéndice 6. Bibliografía complementaria

126

Índice analítico

127