

Índice General

Capítulo I

La Auditoría de Sistemas de Información

1.		La Auditoría de Sistemas de Información	25
2.		Nacimiento de la Auditoría	27
3.		El alcance de la Auditoría de Sistemas de Información	28
	3.1.	Control de integridad de registros	28
	3.2.	Control de validación de errores	28
4.		Características de la Auditoría de Sistemas de Información	28
5.		Síntomas de necesidad de una Auditoría de Sistemas de Información	29
	5.1.	Síntomas de descoordinación y desorganización	29
	5.2.	Síntomas de mala imagen e insatisfacción de los usuarios	29
	5.3.	Síntomas de debilidades económico-financiero	30
	5.4.	Síntomas de Inseguridad: Evaluación de nivel de riesgos	30
	5.5.	Continuidad del Servicio.	30
	5.6.	Centro de Proceso de Datos fuera de control.	30
	5.7.	Planes de Contingencia	30
6.		Tipos y clases de Auditoría de Sistemas de Información	31
7.		Auditoría Informática de Explotación	32
	7.1.	Control de Entrada de Datos	32
	7.2.	Planificación y Recepción de Aplicaciones	33
	7.3.	Centro de Control y Seguimiento de Trabajos	33
	7.4.	Operación. Salas de Ordenadores	33
	7.5.	Centro de Control de Red y Centro de Diagnosis	34
8.		Auditoría Informática de Desarrollo de Proyectos o Aplicaciones	34

9.		Auditoría Informática de Sistemas	37
	9.1.	Sistemas Operativos	37
	9.2.	Software Básico	37
	9.3.	Software de Teleproceso (Tiempo Real)	38
	9.4.	Tunning	38
	9.5.	Optimización de los Sistemas y Subsistemas	38
	9.6.	Administración de Base de Datos	39
	9.7.	Investigación y Desarrollo	39
10.		Auditoría Informática de Comunicaciones y Redes	40
11.		Auditoría de la Seguridad Informática	41
	11.1.	Elementos que comprenden el Sistema Integral de Seguridad	42
	11.2.	Pruebas en la Auditoría Informática	43
	11.3.	Principales herramientas de las que dispone el auditor informático	44
12.		Perfil del Auditor de Sistemas de Información	44
13.		Escenarios de la Auditoría de Sistemas de Información	45
	13.1.	Ambiente de Informática	45
	13.2.	Organización	45
	13.3.	Aplicativos	45
	13.4.	Base de datos	46
	13.5.	Redes de comunicación y micro computadores	46
	13.6.	Desarrollo de sistemas	46
14.		Elementos de la Informática	46
	14.1.	Elemento Físico (Hardware)	46
	14.2.	Elemento lógico (Software)	46
	14.3.	El elemento humano (personal informático)	47
	14.4.	Sistemas de Información	48
	14.5.	Usos de los Sistemas de Información	50

Capítulo II

Auditoría en el Ambito Judicial - Auditoría Forense

1.		Definición y alcance de la auditoría forense	51
2.		Auditoría forense: ¿Quiénes demandan este servicio?	52
3.		Evidencia Digital	52
4.		Características de una evidencia digital	53

Capítulo III

Estandares Internacionales - COBIT (Control Objectives for Information and related Technology), Cobit versión 4.1 - Derechos de autor (Copyright ©) 2007 por el IT Governance Institute.

1.		COBIT, Misión y Visión	54
	1.1.	Misión	54
	1.2.	Visión	55
2.		COBIT cubre cuatro dominios	55
	2.1.	Planificación y Organización	55
	2.2.	Adquisición e Implementación	56
	2.3.	Servicios y Soporte	56
	2.4.	Monitoreo	57
3.		Aceptabilidad General del COBIT	58
	3.1.	Usuarios interesados en COBIT	59
4.		Marco de Trabajo completo de COBIT	60
5.		Navegación en el marco de trabajo de COBIT	61
6.		Introducción a los componentes esenciales de COBIT	61
	6.1.	Formas de visualizar el contenido del desempeño del proceso	62
	6.2.	Usuarios de los Componentes de COBIT	63
7.		Areas de Enfoque del Gobierno de TI	64
	7.1.	Directrices Gerenciales	64

Capítulo IV

ITIL (Biblioteca de Infraestructuras de Tecnologías de Información)

1.		Concepto	66
2.		El alcance de ITIL	66
3.		Niveles de certificación ITIL para profesionales	67

Capítulo V

MCIIEF - Manual de Control Interno Informático para Entidades Financieras de la Superintendencia de Bancos, del Banco Central del Paraguay

1.		Planificación y Organización	68
2.		Adquisición e Implementación	70
3.		Producción y Servicios	71
4.		Monitoreo	73
5.		Índice del Manual de Control Interno Informático para Entidades Financieras de la Superintendencia de Bancos	73

Capítulo VI

Modelo de Redacción de NCI

1.		Modelo de NC 01 - Evaluación de Estructura de TI	76
	1.1.	Ubicación estructural del área de servicios de TI	76
2.		Organización de la Estructura de TI	77
	2.1.	Inexistencia de un responsable del área de TI de la dependencia Jefe/Encargado	77
	2.2.	Inexistencia de un Administrador de BD	78
	2.3.	Inexistencia de un Administrador de Redes	78
	2.4.	Inexistencia de un Administrador de Sistemas	79
	2.5.	Inexistencia de una estructura de soporte técnico/asistencia a usuarios	79

	2.6.	Inexistencia de una estructura de desarrolladores internos de sistemas	80
	2.7.	Nombramiento del administrador de seguridad de TI	80
	2.8.	Separación de funciones - Personal clave de tecnología de información	81
	2.9.	Definición de propietario de datos, determinación de responsabilidades	82
3.		Evaluación de Gestión de TI - Gerenciamiento	82
	3.1.	Plan de TI a largo plazo, enfoque y estructura, aprobación	82
	3.2.	Plan de TI a corto plazo, planificación de la capacidad de la infraestructura tecnológica	84
	3.3.	Cambios al plan de TI a largo plazo	84
	3.4.	Evaluación permanente del plan estratégico de tecnología de información	85
	3.5.	Metodología de Control de Adquisiciones - Procedimientos	85
4.		Sistemas de Información	86
	4.1.	Integración de módulos – ERP (Los Sistemas del tipo ERP (Enterprise Resource Planning) se han definido como un sistema global de planificación de los recursos y de gestión de la información)	86
	4.2.	Control de versiones del código fuente y autorización para el traspaso al entorno de producción	87
	4.3.	Pruebas del sistema en forma paralela antes del traspaso a producción	87
	4.4.	Prueba de aceptación final antes del traspaso a producción	88
	4.5.	Estructura de desarrollo paralelo – servidor independiente	88
	4.6.	Procedimientos aplicados ante la eventual caída del sistema	89
	4.7.	Mecanismo para el cierre diario del sistema – participantes – aprobación	89
	4.8.	En casos de ajustes eventuales de registros ya procesados, ¿cómo se realiza y quien autoriza?	90

5.		Evaluación del desarrollo y mantenimiento de sistemas - Equipo Interno	91
	5.1.	Procedimientos de controles de seguridad aplicados en la etapa de análisis y diseño del sistema	91
	5.2.	Seguridad en los sistemas de aplicación, validación de datos de entrada	91
	5.3.	Política de utilización de controles criptográficos, encriptación	92
	5.4.	Protección de los datos de prueba del sistema, aplicación de otras BD para pruebas	93
	5.5.	Control de cambios a datos operativos, manipulación de datos a través de un MGBD	94
	5.6.	Mecanismo, registro y control de acceso a las bibliotecas de programas fuentes	94
6.		Evaluación del desarrollo y mantenimiento de sistemas – consultoría externa	95
	6.1.	Acuerdos de licencias, propiedad de código y derechos conferidos	95
	6.2.	Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.	96
	6.3.	Procedimientos de certificación de la calidad, que incluyan auditorías internas de sistemas.	97
	6.4.	Acuerdos de custodia de las fuentes del software.	97
7.		Seguridad Física	98
	7.1.	Disponibilidad de los planes de continuidad de las actividades de TI (plan de contingencia)	98
	7.2.	Ensayo, Mantenimiento y Evaluación de los Planes de Continuidad de Ti (Pruebas)	99
	7.3.	Aprobación por la alta gerencia del plan de contingencias	100
	7.4.	Disponibilidad del plan de seguridad TI	101
	7.5.	Aprobación del Plan de Seguridad de TI	102
8.		Evaluación de la Sala de Servidores - Data Center y Alta Disponibilidad	103

	8.1.	Sala de servidores independiente y restricción de accesos, controles de acceso físico.	103
	8.2.	Restricción de accesos a la sala de servidores, bitácora de accesos	104
	8.3.	Evidencia del mantenimiento de equipos preventivos	104
	8.4.	Lista de Servidores	105
	8.5.	Servidor espejado - Fuera del recinto principal	106
	8.6.	Arquitectura Servidor - Clon	106
	8.7.	Sistema Operativo Server - Propietario - Libre	107
	8.8.	Rack de protección, protegido con llave	107
	8.9.	Cableado de red ordenado, identificado por usuarios	108
	8.10	Certificado del Cableado de Red	108
	8.11.	Identificación de materiales inflamables, en el recinto del Data Center	109
	8.12.	Disponibilidad de detectores de humo y calor	110
	8.13.	Extintores especiales contra incendios	110
	8.14.	Licencias de los sistemas operativos de redes	110
	8.15.	Disponibilidad del Sistema de puesta a tierra	111
	8.16.	Suministro de energía eléctrica, UPS	111
	8.17.	Suministro de energía eléctrica, generador de electricidad	112
9.		Relevamiento de Inventarios y manuales técnicos	113
	9.1.	Manuales de usuarios - Impresos - Interactivos	113
	9.2.	Manuales DFD, UML, AOO – Disponibles - Actualizados	113
	9.3.	Manuales de ER – Disponibles - Actualizados	114
	9.4.	Disponibilidad de inventario de activos – Hardware - Actualizado	114
10.		Evaluación de la Administración de Proyectos	115
	10.1	Definición y esquema de Administración de Proyectos de TI	115
	10.2	Evidencia de solicitud de prórroga	115
	10.3.	Solicitud de reajustes	116

10.4.	Solicitud de recepción técnica provisoria	116
10.5.	Solicitud de recepción técnica definitiva	117
10.6.	Contrato de mantenimiento hardware- vencimiento- cronograma	117
10.7.	Contrato de mantenimiento software- vencimiento	118
10.8.	Contrato de licencias de software propietario	118

Capítulo VII

Ejercicios Prácticos

1.	Caso: Omega Engineering INC:	119
1.1.	Tema: Fallas en la seguridad y el delito computacional	119
1.2.	Preguntas del estudio del caso	121
2.	Otros casos de fraudes y abusos computacionales	121
2.1.	Presentación del ejercicio	121
2.2.	El Caso del Guardia Honesto	122
2.3.	El Caso de la Cinta baleada	122
2.4.	El Caso del Ataque Terrorista	123
2.5.	El caso de las Cintas de Hewlett Packard	123
2.6.	El caso del computador que se iba al agua	123
2.7.	El caso de la lista de clientes robada	124
2.8.	El caso del sobre tiempo	124
2.9.	El Caso del Historial Clínico	125
2.10.	El caso del Seguro de Cesantía	125
2.11.	El caso de la Demanda a la Víctima	126
2.12.	El caso del fraude a Texaco	127
2.13.	El caso del SUPERZAP	127
2.14.	El Empleado Inexistente	128
2.15.	El Caso del Ataque Terrorista	128
2.16.	El caso de los negocios extras	129

	2.17.	El Caso del Correo de Votantes	129
3.		Práctica de auditoría de sistemas de información	130
	3.1.	Fallas en la seguridad y el delito computacional	130
	3.2.	Trabajo a desarrollar	131
4.		Ejercicio Práctico de Proceso de Auditoría	132

Capítulo VIII

Directrices y papeles de trabajo para la realización de una Auditoría Informática

1.		Pasos a seguir para recomendación de soluciones	136
2.		Modelo de Nota de Control Interno	136
3.		Papeles de trabajo de controles de TI	137
4.		Modelo de Propuesta de Servicios	154
	4.1.	Objetivo	154
	4.2.	Aspectos relevantes del plan de auditoría	155
	4.3.	Alcance de los servicios	155
	4.4.	Metodología	156
	4.5.	Presentación de Informes	156
	4.6.	Validéz de la oferta	156
	4.7.	Honorario y forma de pago	157
5.		Modelo de Carta Gerencial	157
	5.1.	Objetivo General	157
	5.2.	Objetivo Específico	157

Capítulo IX

Glosario de Términos Técnicos

1.		Glosario de Términos Técnicos	159
----	--	-------------------------------	-----

Capítulo X

Anexos

1.		Disposiciones reglamentarias sobre la Registración Contable por medios computacionales. Matriz de verificación para el Auditor Informático.	174
	1.1.	Resolución N° 412/04. Por la cual se adecuan a la legislación vigente las disposiciones reglamentarias de registración contable y de su empleo por medios computacionales.	174
	1.2.	Resolución N° 535/04. Por la cual se aclara disposiciones contenidas en la resolución n° 412 del 1 de octubre de 2004 “por la cual se adecuan a la legislación vigente las disposiciones reglamentarias de registración contable y de su empleo por medios computacionales”.	180
	1.3.	Resolución General N° 23/09. Por la cual se aclaran aspectos relativos a los Certificados de Cumplimiento Tributario, a la utilización de medios computacionales para la registración contable, a la comunicación de cesión de cuotas parte y de acciones a la recepción y gestión de las solicitudes de constancias de no retención de impuestos, se modifican los Artículos 8° y 13° de la Resolución N° 412/04 y los Artículos 2° y 18° de la Resolución General N° 15/07, se precisa la forma de llenado del Formulario N° 108 – Impuesto a la Renta y se derogan los Artículos 9° y 11° de la Resolución N° 412/04 y el Art. 5° de la Resolución N° 535/04.	182
	1.4.	Cuestionario para verificación del cumplimiento de la RG N° 412/04.	183