



ÍNDICE

AGRADECIMIENTOS	7
CAPÍTULO I: EL OBJETO A AUDITAR	9
I.1 Política de Seguridad de la Información	11
I.2 Política de alineación de TI con las necesidades del ente	16
I.3 Procedimiento de roles y responsabilidades del área de Sistemas - TI (Tecnología de la Información)	21
CAPÍTULO II: LA NECESIDAD DE EFECTUAR AUDITORÍAS DE LOS SISTEMAS DE INFORMACIÓN DE UNA ENTIDAD	57
II.1 El objetivo y la necesidad de las auditorías de los Sistemas de Información en una organización	57
II.1.1 Ejemplo sobre la necesidad de las auditorías de los Sistemas de Información de un ente	58
II.2 Herramientas teóricas para el desarrollo de las auditorías de Sistemas	59
CAPÍTULO III: DESARROLLO DEL MAPA DE RIESGOS DE AUDITORÍA DE SISTEMAS	61
III.1 Integrando el mapa de riesgos de Auditoría Interna	61
III.2 Visión de riesgos de TI dentro de Auditoría Interna	62
III.3 La estrategia de Auditoría Interna de Sistemas	62
III.3.1 Sistemas aplicativos instalados	63
III.3.2 Sistemas operativos instalados	64
III.3.3 Sistemas técnicos y de oficina	65
III.3.4 Instalación de redes y equipos de comunicación	65
III.3.5 Evaluación de riesgos de TI basada en la información contable	66
III.3.5.1 Evaluación del entorno tecnológico de la información	67
III.3.5.2 Riesgos propios de TI. Empleos	67

III.3.5.3 Relevamiento de las aplicaciones utilizadas para el tratamiento de la información. Ejemplos	67
III.3.5.4 Calificación del ambiente de control del ente	67
III.3.5.5 Planificación de la Auditoría en función de los riesgos detectados	67
CAPÍTULO IV: RELEVAMIENTO DEL ENTORNO TECNOLÓGICO POR CAPAS	71
IV.1 Un primer relevamiento de Auditoría Interna de Sistemas	71
IV.2 Definición de un mapa de riesgos preliminar de alto nivel	72
IV.2.1 Políticas, normas y procedimientos de TI	73
CAPÍTULO V: LA SEGURIDAD FÍSICA DE TI	75
V.1 Inventario de los recursos tecnológicos	75
V.1.1 Inexistencia o desactualización del inventario de los recursos tecnológicos	76
V.1.2 Recursos tecnológicos no identificados adecuadamente	77
V.2 Seguridad del área de Cómputos y de las instalaciones de comunicaciones	78
V.2.1 Seguridad del área de Cómputos	78
V.2.2 Instalaciones eléctricas y cableado de datos	78
V.3 Instalaciones contra incendios y planes de contingencia	79
V.4 Copias de respaldo de la información	80
V.4.1 Consideraciones sobre los respaldos de la información – <i>Backup</i>	81
V.4.2 Resguardos como protección contra virus y otros programas malignos	84
CAPÍTULO VI: LA SEGURIDAD LÓGICA DE SISTEMAS	85
VI.1 Accesos de usuarios a los sistemas aplicativos	85
VI.2 Accesos de usuarios especiales	86
VI.3 Seguridad de aplicaciones perimetrales	86
VI.4 La seguridad de aparatos móviles	87
CAPÍTULO VII: RELEVAMIENTO DE APLICACIONES DE TI	89
VII.1 Sistemas aplicativos centrales o ERP	90
VII.2 Otros sistemas existentes en el mercado local	90
VII.3 Desarrollos propios o “a medida”	91
VII.3.1 Desarrollo con personal propio	91
VII.3.2 Desarrollo por medio de terceros	91

VII.3.2.1	Términos del acuerdo	92
VII.3.2.2	Licencia de uso del software	92
CAPÍTULO VIII: SERVICIO DE SOPORTE Y SEGUIMIENTO DE CASOS		
VIII.1	Organización del área de Soporte a usuarios	93
VIII.2	Seguimiento de casos	93
VIII.2.1	Control de casos mediante número de incidentes	94
VIII.2.2	Encuestas sobre el servicio	94
CAPÍTULO IX: CONTINUIDAD DE LAS ACTIVIDADES		95
IX.1	Concepto de continuidad	95
IX.2	Concepto de contingencia	96
IX.3	Planificación de la continuidad en caso de emergencia	96
CAPÍTULO X: EL SISTEMA DE ADMINISTRACIÓN DE AUDITORÍA INTERNA		97
X.1	El objetivo y la necesidad de un Sistema de Administración de Auditoría Interna	97
X.2	El proceso de desarrollo e implementación del Sistema de Administración de Auditoría Interna	98
X.3	La necesaria información de salida del Sistema de Administración de Auditoría	99
X.3.1	Desarrollo de Auditorías y seguimiento	100
X.4	Valor económico generado por Auditoría	106
X.5	Cumplimiento de los objetivos anuales de Auditoría	107
X.6	Ranking de los logros obtenidos por empresa y por Auditor	109
X.7	Aplicación eficiente de los recursos de Auditoría	110
X.7.1	Análisis de gráficos sobre la gestión de la función	110
CAPÍTULO XI: PARTICIPACIÓN DEL AUDITOR DE SISTEMAS EN EL DESARROLLO DE SISTEMAS		111
XI.1	Introducción	112
XI.2	Algunos conceptos relacionados con un proyecto de implementación de Sistemas	113
XI.3	División de responsabilidades de las definiciones de Control Interno a ser implementadas en el nuevo sistema	114
CAPÍTULO XII: DESARROLLO DE TAAC		115
XII.1	Aspectos teóricos y prácticos para el desarrollo de TAAC	116

XII.2 Exposición de un caso práctico para el desarrollo de TAAC	118
-----------------------------------------------------------------	-----

CAPÍTULO XIII: CASOS PRÁCTICOS DE AUDITORÍA DE SISTEMAS 121

XIII.1 Auditoría de accesos de usuarios	121
-----------------------------------------	-----

XIII.2 Principios esenciales de la Seguridad de la Información aplicables en distintas organizaciones	123
-------------------------------------------------------------------------------------------------------	-----

XIII.3 Auditoría de entes medianos y pequeños en entornos tecnológicos	127
------------------------------------------------------------------------	-----

XIII.4 Relevamiento del circuito de Cuentas a Pagar mediante aprobaciones electrónicas	128
----------------------------------------------------------------------------------------	-----

XIII.5 Auditoría de resguardos	130
--------------------------------	-----

CAPÍTULO XIV: CONCLUSIÓN GENERAL 133

BIBLIOGRAFÍA 135