

Índice de Contenido

PARTE I: Fundamentos del Trabajo

INTRODUCCIÓN	1
CAPÍTULO 1	3
Objetivos y Justificación del Proyecto	3
1.1. Antecedentes.....	3
1.2. Definición del Problema.....	4
1.2.1. Situación Problemática	4
1.2.2. Planteamiento del Problema	8
1.3. Objetivos	8
1.3.1. Objetivo General	8
1.3.2. Objetivos Específicos.....	8
1.4. Justificación.....	9
1.5. Alcance.....	11
1.5.1. Alcance del Contenido	11
1.5.2. Alcance Espacial	11
1.5.4. Alcance Temporal	11
CAPÍTULO 2	12
El Riesgo	12
2.1. El Riesgo.....	12
2.1.1. Características del Riesgo	14
2.1.2. Clases de Riesgo	16
2.2. Riesgo Informático	16
2.2.1. Elementos del Riesgo	17
2.2.2. Riesgo Inherente	18
2.2.3. Riesgo Residual	18
CAPÍTULO 3	19
Análisis de Riesgo.....	19
3.1. Concepto de Método	19
3.2. Definición de Análisis.....	20
3.3. Análisis de Riesgo	21
3.3.1. Definición Conceptual.....	21
3.3.2. Clasificación de Amenazas	22
3.3.3. Análisis de Riesgos Informáticos	23
3.3.4. Vulnerabilidades	23
3.3.5. Tipos de Análisis de Riesgos.....	24
CAPÍTULO 4	27
Data Center	27
4.1. Data Center.....	27
4.1.1. Elementos de un Data Center.....	28
4.1.2. Cualidades de un Data Center	31
4.1.3. Clasificación de la Infraestructura de Data Center	32
4.1.4. Disponibilidad de un Data Center	47
4.1.5. Consideraciones Ambientales	55
4.1.6. Diseño de Espacio de Piso y Zonas Seguras para Data Center	57
4.2. Green Data Center	62

CAPÍTULO 5	63
Norma Boliviana NB-ISO-IEC 17799.....	63
5.1. ¿Qué es la Seguridad de la Información?.....	63
5.2. Por qué es Necesaria la Seguridad de la Información.....	64
5.3. Cómo Establecer los Requerimientos de Seguridad.....	65
5.4. Evaluación de los Riesgos en Materia de Seguridad.....	66
5.5. Selección de Controles.....	67
5.6. Punto de Partida para la Seguridad de la Información.....	68
5.7. Factores Críticos del Éxito.....	69
5.8. Desarrollo de Lineamientos Propios.....	69
5.9. Seguridad Física y Ambiental.....	70
5.9.1 Áreas Seguras.....	70
5.9.2. Seguridad del Equipamiento.....	75
5.9.3 Controles Generales.....	80

CAPÍTULO 6	83
Metodologías.....	83
6.1. AS/NZS 4360:1999 Estándar Australiano.....	83
6.1.1. Requerimientos de Administración de Riesgos.....	83
6.1.2. Vista General de la Administración de Riesgos.....	86
6.1.3. Proceso de Administración de Riesgos.....	88
6.1.4. Identificación de Riesgos.....	92
6.1.5. Análisis de Riesgos.....	93
6.2. COBIT 4.0.....	98
6.2.1. Marco de Trabajo COBIT para el Control del Gobierno TI.....	98
6.2.2. Como Satisface COBIT la Necesidad.....	102
6.2.3. Modelos de Madurez.....	119
6.2.4. Medición del Desempeño.....	127
6.2.5. El Modelo del Marco de Trabajo COBIT.....	129
6.2.6. Nivel de Aceptabilidad General de COBIT.....	132
6.2.7. Planear y Organizar (PO).....	134
6.3. MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.....	140
6.3.1. Introducción a Magerit.....	140
6.3.2. Análisis de Riesgos.....	149
6.4. NIST – Introducción a Seguridad de Computación.....	168
6.4.1. Propósito.....	168
6.4.2. Guía de Administración de Riesgo para Sistemas IT.....	169
6.4.3. Importancia de la Administración de Riesgos.....	169
6.4.4. NIST - Análisis de Riesgos.....	169
6.5. PROTIVITI – IT Risk Assessment.....	187
6.5.1. Escalas de Puntuación de Riesgo.....	187
6.5.2. Escala de Efectividad de Controle y Metodología.....	189
6.5.3. Lista de Detalle de Riesgo.....	190

PARTE III: Análisis y Diseño del Método

CAPÍTULO 7	191
Requerimientos del Análisis de Riesgo.....	191
7.1. Administración de Riesgos.....	191
7.2. Planeamiento y Recursos.....	193
7.3. Revisión Gerencial.....	194
7.4. Concienciación y Formación.....	194

CAPÍTULO 8	196
Vista General del Análisis de Riesgo	196
8.1. Consideraciones Previas.....	196
8.2. Secuencias del Método.....	198
CAPÍTULO 9	200
Técnicas para el Análisis de Riesgo	200
9.1. Análisis Mediante Tablas	202
9.2. Análisis Algorítmico	202
9.2.1. Un Modelo Cualitativo.....	203
9.2.2. Un Modelo Cuantitativo	203
9.2.3. Un Modelo Escalonado.....	203
9.3. Árboles de Ataque.....	203
CAPÍTULO 10	205
Procesos del Análisis de Riesgo.....	205
10.1. Descripción de las Secuencias del Método y sus Técnicas.....	205
Proceso 1: Caracterización del Data Center	205
Proceso 2: Identificación del Riesgo.....	207
Proceso 3: Análisis de Impacto	221
Proceso 5: Determinación del Riesgo.....	225
Proceso 6: Análisis de Efectividad de los Controles	227
Proceso 7: Documentación de los Resultados.....	234
CAPÍTULO 11	238
Herramientas de Apoyo	238
11.1. Checklist de Requerimientos	238
11.2. Cuestionario de Seguridad.....	241
11.3. Ejemplo de Entrevista	241
PARTE IV: Pruebas y Resultados del Método	
CAPÍTULO 12	242
Pruebas y Resultados del Método.....	242
Empresa 1	242
12.1. 1. Pruebas	243
12.1.2. Resultados	244
Empresa 2	244
12.2.1. Pruebas	245
12.2.2. Resultados	246
Empresa 3	246
12.3.1. Pruebas	247
12.3.2. Resultados	248
Conclusiones.....	249
Recomendaciones.....	250
BIBLIOGRAFÍA	251
GLOSARIO	259
ANEXOS	269