

## TABLA DE CONTENIDOS

	página
<b>Dedicatoria</b>	<b>I</b>
<b>Agradecimientos</b>	<b>II</b>
<b>Tabla de Contenidos</b>	<b>IV</b>
<b>Índice de Figuras</b>	<b>VIII</b>
<b>Índice de Tablas</b>	<b>XII</b>
<b>Resumen</b>	<b>XIII</b>
<b>Abstract</b>	<b>XIV</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Introducción . . . . .	1
1.1.1. Objetivos . . . . .	2
1.2. Contexto . . . . .	3
1.3. Problema . . . . .	3
1.4. Justificación . . . . .	4
1.5. Estructura de Trabajo . . . . .	6
<b>2. Marco Teórico</b>	<b>8</b>
2.1. Introducción . . . . .	8
2.2. Conceptos de Seguridad en Redes de datos . . . . .	8
2.2.1. Vulnerabilidades genéricas . . . . .	9
2.2.2. Estrategias de Seguridad de la Información. . . . .	9
2.2.3. Arquitectura de Seguridad OSI . . . . .	10
2.3. Metodologías y Normas para Auditorías de Seguridad. . . . .	11
2.3.1. SISAP. . . . .	11
2.3.2. Normas de la Seguridad de la Información. . . . .	12
2.3.3. Normas relacionadas. . . . .	12
2.3.4. La Norma ISO/IEC 27001:2005 . . . . .	14

2.3.5.	Ciclos adaptados para realizar auditorías de seguridad. . . . .	15
2.4.	Metodología para Análisis y Gestión del Riesgo. . . . .	18
2.4.1.	MAGERIT . . . . .	18
2.4.2.	CRAMM. (CCTA Risk Analysis and Management Methodology.)	21
2.4.3.	MSRSAT. . . . .	22
2.4.4.	Cuadro comparativo de las metodologías. . . . .	23
2.5.	Softwares de implementación de las metodologías anteriores. . . . .	24
<b>3.</b>	<b>Metodología.</b>	<b>27</b>
3.1.	Aplicación de metodología para análisis de riesgos. . . . .	27
3.1.1.	Etapa de planificación. . . . .	28
3.1.2.	Etapa de Análisis de Riesgos. . . . .	29
3.1.3.	Etapa de Gestión de Riesgos. . . . .	30
3.1.4.	Etapa de Selección de Salvaguardas. . . . .	31
3.2.	Auditoría de Seguridad General. . . . .	31
3.2.1.	Aplicación del modelo PDCA. . . . .	32
3.3.	Aplicación de estándares de Seguridad Física. . . . .	34
3.4.	Diseño del modelo de seguridad. . . . .	35
<b>4.</b>	<b>Desarrollo.</b>	<b>36</b>
4.1.	Aplicación de Metodología MAGERIT. . . . .	36
4.1.1.	Proceso de análisis de riesgos . . . . .	36
4.1.2.	Caracterización de los Activos. . . . .	37
4.1.3.	Vulnerabilidad de los dominios. . . . .	41
4.1.4.	Caracterización de las amenazas . . . . .	42
4.1.5.	Caracterización de las Salvaguardas. . . . .	46
4.1.6.	Estimación de estado del riesgo. . . . .	46
4.2.	Aplicación Norma ISO 27001 . . . . .	49
4.2.1.	Análisis de resultados de la aplicación de la Norma . . . . .	49
4.3.	Auditoría de Seguridad Física. . . . .	56
4.3.1.	Seguridad del edificio. . . . .	57
4.3.2.	Seguridad del equipamiento de Telecomunicaciones. . . . .	62
4.3.3.	Mantenimiento de los equipos. . . . .	64
4.3.4.	Análisis General e interpretación de resultados. . . . .	67

<b>5. Implementación del Modelo de Seguridad.</b>	<b>70</b>
5.1. Introducción . . . . .	70
5.2. Creación de un SGSI en base al modelo PDCA, para la Plataforma Corporativa de la Universidad de Talca . . . . .	71
5.2.1. Requerimientos del SGSI. . . . .	71
5.2.2. Documentación a considerar. . . . .	73
5.3. Hacia la Implementación de un modelo de seguridad basado en un código de buenas prácticas. . . . .	76
5.3.1. Resultado general aplicación metodología MAGERIT. . . . .	76
5.3.2. Resultado general aplicación ISO/IEC 27001:2005. . . . .	81
5.3.3. Creación de un modelo de seguridad Física. . . . .	85
<b>6. Conclusiones</b>	<b>93</b>
6.1. <b>Análisis de Riesgos.</b> . . . . .	93
6.2. <b>Auditoría de Seguridad General.</b> . . . . .	94
6.3. <b>Auditoría de Seguridad Física.</b> . . . . .	95
6.4. <b>Aportes de la memoria.</b> . . . . .	97
6.5. <b>Trabajos futuros.</b> . . . . .	98
<b>Glosario</b>	<b>99</b>
<b>Bibliografía</b>	<b>102</b>
<b>Anexos</b>	
<b>A: Submodelo de Procesos de MAGERIT.</b>	<b>106</b>
<b>B: Detección de amenazas por capas de activos.</b>	<b>107</b>
<b>C: Identificación de vulnerabilidades por dominios de activos.</b>	<b>109</b>
<b>D: Detección de funciones de Salvaguardas y mecanismos.</b>	<b>111</b>
<b>E: Tablas con cálculos de impacto sobre los activos.</b>	<b>114</b>
<b>F: Tablas con cálculos de riesgo sobre los activos</b>	<b>116</b>

<b>G:</b>	<b>Mapa de riesgos MAGERIT</b>	<b>118</b>
<b>H:</b>	<b>Controles ISO/IEC 27001:2005</b>	<b>121</b>
<b>I:</b>	<b>Controles Seguridad Física.</b>	<b>125</b>

## ÍNDICE DE FIGURAS

	página
1.1. Gráfico de incidentes de seguridad en las grandes organizaciones de Europa. Fuente IBM . . . . .	5
2.1. Ciclo de la Metodología PDCA. . . . .	16
2.2. Ciclo de la Metodología PDSA. . . . .	17
2.3. Estructura de Subprocesos de MAGERIT. . . . .	20
2.4. Cuadro comparativo de las características de las metodologías MAGERIT, CRAMM, MSRSAT y SISAP. . . . .	23
3.1. Etapas que componen la aplicación de la metodología MAGERIT. . .	28
3.2. Ciclo PDCA. . . . .	32
4.1. Capas de activos de Magerit. . . . .	37
4.2. Número de activos por capas o dominios. . . . .	38
4.3. Porcentaje de activos por capas o dominios de la Plataforma, por sobre el total de activos. . . . .	38
4.4. Valoración de activos y dimensiones de seguridad por dominios de activos. . . . .	40
4.5. Identificación y número de vulnerabilidades por capas de activos. . .	42
4.6. Identificación de amenazas existentes en la Plataforma. . . . .	43
4.7. Relación Activo - Amenaza. . . . .	44
4.8. Valoración de las amenazas detectadas en las capas de activos. . . . .	46
4.9. Identificación de amenazas y número de mecanismos por función. . .	47
4.10. Resultado General aplicación Norma ISO/IEC :27001:2005, Plataforma Corporativa Universidad de Talca. . . . .	55
4.11. Gráfico de análisis general acerca de aplicación ISO 27001, apéndice Seguridad Física. . . . .	68
5.1. Resumen resultados aplicación ISO/IEC 27001:2005 a Plataforma U. de Talca. . . . .	81
5.2. Comparación entre modelo actual y el modelo mejorado. . . . .	85
5.3. Resultados análisis seguridad física Plataforma U. de Talca.(Parte I) .	86

5.4. Seguridad Física. Comparación entre modelo actual y el modelo mejorado. . . . .	89
5.5. Resultados análisis seguridad física Plataforma U. de Talca.(Parte II)	90
5.6. Seguridad Física. Comparación de resultados, Modelo Actual y Modelo Mejorado. . . . .	92
6.1. Medición de eficiencia y comparación del modelo actual y la propuesta de modelo mejorado, usando la Norma ISO 27001. . . . .	95
6.2. Medición de eficiencia del modelo actual y propuesto, parte I.- Seguridad del Entorno. . . . .	96
6.3. Medición de eficiencia del modelo actual y propuesto, parte II.- Seguridad de los equipos de telecomunicaciones. . . . .	97
A.1. Etapas que componen el Submodelo de Procesos de MAGERIT. . . .	106
B.1. Número de amenazas por capas de activos, parte I. . . . .	107
B.2. Número de amenazas por capas de activos, parte II. . . . .	108
C.1. Identificación de vulnerabilidades por dominios, parte I. . . . .	109
C.2. Identificación de vulnerabilidades por dominios, parte II. . . . .	110
D.1. Funciones de salvaguardas por amenazas detectadas, parte I. . . . .	111
D.2. Funciones de salvaguardas por amenazas detectadas, parte II. . . . .	112
D.3. Valoración de funciones de salvaguardas y mecanismos por función. .	113
E.1. Tabla con impacto sobre los activos, parte I. . . . .	114
E.2. Tabla con impacto sobre los activos, parte II. . . . .	115
F.1. Tabla de riesgos sobre los activos, parte I. . . . .	116
F.2. Tabla de riesgos sobre los activos, parte II. . . . .	117
G.1. Mapa de Riesgos de MAGERIT, parte I. . . . .	118
G.2. Mapa de Riesgos de MAGERIT, parte II. . . . .	119
G.3. Mapa de Riesgos de MAGERIT, parte III. . . . .	120
G.4. Mapa de Riesgos de MAGERIT, parte IV. . . . .	120
H.1. Controles aplicación Norma ISO 27001, Apéndice A.5.- Políticas de seguridad. . . . .	121

H.2. Controles aplicación Norma ISO 27001, Apéndice A.6.- Organización de la Seguridad. . . . .	121
H.3. Controles aplicación Norma ISO 27001, Apéndice A.7.- Administración de activos. . . . .	122
H.4. Controles aplicación Norma ISO 27001, Apéndice A.8.- Seguridad de los RR.HH. . . . .	122
H.5. Controles aplicación Norma ISO 27001, Apéndice A.9.- Seguridad Física y del entorno. . . . .	122
H.6. Controles aplicación Norma ISO 27001, Apéndice A.10.- Gestión de Comunicaciones. . . . .	123
H.7. Controles aplicación Norma ISO 27001, Apéndice A.11.- Control de Accesos. . . . .	123
H.8. Controles aplicación Norma ISO 27001, Apéndice A.12.- Mantenimiento, actualización de los sistemas. . . . .	124
H.9. Controles aplicación Norma ISO 27001, Apéndice A.13.- Administración de Incidentes. . . . .	124
H.10. Controles aplicación Norma ISO 27001, Apéndice A.14.- Gestión de la Continuidad del Negocio. . . . .	124
H.11. Controles aplicación Norma ISO 27001, Apéndice A.15.- Cumplimiento.	124
I.1. Controles aplicación Seguridad Física.- Seguridad del Edificio. . . . .	125
I.2. Controles aplicación Seguridad Física.- Sistemas de detección de intrusos. . . . .	125
I.3. Controles aplicación Seguridad Física.- Controles físicos y lógicos de entrada. . . . .	126
I.4. Controles aplicación Seguridad Física.- Biometría. . . . .	126
I.5. Controles aplicación Seguridad Física.- Sistemas automáticos de control de acceso. . . . .	126
I.6. Controles aplicación Seguridad Física.- Protección frente a amenazas externas. . . . .	126
I.7. Controles aplicación Seguridad Física.- Protección frente a incendios.	127
I.8. Controles aplicación Seguridad Física.- Protección frente a inundaciones.	127
I.9. Controles aplicación Seguridad Física.- Reglamentación o Normativa e trabajo. . . . .	127

I.10. Controles aplicación Seguridad Física.- Ubicación y protección de equipos. . . . . 127

I.11. Controles aplicación Seguridad Física.- Seguridad del cableado. . . . . 128

I.12. Controles aplicación Seguridad Física.- Cambios (actualizaciones y mantenimiento). . . . . 128

I.13. Controles aplicación Seguridad Física.- Documentación de equipos de telecomunicaciones. . . . . 128

I.14. Controles aplicación Seguridad Física.- Suministro de energía al equipamiento de telecomunicaciones. . . . . 129

I.15. Controles aplicación Seguridad Física.- Climatización de equipos de telecomunicaciones. . . . . 129

I.16. Controles aplicación Seguridad Física.- Planificación del espacio para equipo de telecomunicaciones. . . . . 129

## ÍNDICE DE TABLAS

	página
4.1. Tabla para las dimensiones de seguridad. . . . .	39
4.2. Tabla para valoración de activos de MAGERIT. . . . .	39
4.3. Tabla con puntos que afectan a la dimensión de la seguridad de la Plataforma. . . . .	40
4.4. Identificación de escala estándar aplicada a la Plataforma U. de Talca.	41
4.5. Tabla para frecuencias de amenazas. . . . .	45
4.6. Tabla para degradación de las amenazas. . . . .	45
4.7. Tabla para estimación del impacto. . . . .	47
4.8. Tabla con rangos de degradación de los activos. . . . .	48
4.9. Tabla estimación del riesgo. . . . .	48
4.10. Tabla con rangos de frecuencia. . . . .	48