

# CONTENIDO

AGRADECIMIENTOS	3
SOBRE EL AUTOR	5
PRÓLOGO	13
<b>CAPÍTULO 1</b>	
<b>SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN</b>	<b>17</b>
INTRODUCCIÓN	17
EVOLUCIÓN DE LA NORMA	19
FAMILIA ISO 27000	21
NATURALEZA DE UN SGSI	21
REFERENCIAS BIBLIOGRÁFICAS	24
<b>CAPÍTULO 2</b>	
<b>NATURALEZA DE LA NORMA ISO 27001:2005 Y LAS CLÁUSULAS GLOBALES</b>	<b>25</b>
INTRODUCCIÓN	25
ALCANCE DEL MODELO	26
APLICACIÓN	27
TÉRMINOS Y DEFINICIONES	27
SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	27
NATURALEZA DEL ESTÁNDAR	27
5.2 GESTIÓN DE LOS RECURSOS	32
6.0 AUDITORÍAS INTERNAS DEL SGSI	34
7.0 REVISIÓN GERENCIAL	35
8.0 MEJORAMIENTO DEL SGSI	36
8.2 ACCIÓN CORRECTIVA	36
B-5.2 NO-CONFORMIDAD	36
8.3 ACCIÓN PREVENTIVA	37
CONCLUSIONES	38
REFERENCIAS BIBLIOGRÁFICAS	38
<b>CAPÍTULO 3</b>	
<b>ESTABLECIMIENTO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN</b>	<b>39</b>
INTRODUCCIÓN	39
ALCANCE DE UN SGSI	39
ILUSTRACIÓN PARA DEFINIR UN ALCANCE	40

POLÍTICA DE UN SGSI	42
ENFOQUE PARA LA GESTIÓN DEL RIESGO	42
VALUACIÓN DEL RIESGO	43
PROCESO DE VALUACIÓN DEL RIESGO	43
ASPECTOS A CONTEMPLAR AL EFECTUAR EL ANÁLISIS DEL RIESGO	44
1. IDENTIFICACIÓN DE ACTIVOS	44
2. IDENTIFICACIÓN DE REQUERIMIENTOS LEGALES Y COMERCIALES RELEVANTES PARA LOS ACTIVOS IDENTIFICADOS	45
3. TASACIÓN DE ACTIVOS	46
4. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES	47
SEGURIDAD DE LOS RECURSOS HUMANOS	50
MANTENIMIENTO, DESARROLLO Y ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN	50
CONTROL DE ACCESO	50
GESTIÓN DE OPERACIONES Y COMUNICACIÓN	50
SEGURIDAD FÍSICA Y AMBIENTAL	50
VULNERABILIDADES	50
DESCRIPCIÓN DE LAS CATEGORÍAS DE VULNERABILIDADES	51
REVISIÓN DE LOS CONTROLES IMPLEMENTADOS	52
5. CÁLCULO DE LAS AMENAZAS Y VULNERABILIDADES	52
6. ANÁLISIS DEL RIESGO Y SU EVALUACIÓN	53
ASPECTOS A CONTEMPLAR AL EFECTUAR LA EVALUACIÓN DEL RIESGO	54
EVALUACIÓN DEL RIESGO	54
TRATAMIENTO DEL RIESGO Y EL PROCESO DE TOMA DE DECISIÓN GERENCIAL	55
PROCESO DE TOMA DE DECISIONES	55
ESTRATEGIAS POSIBLES PARA EL TRATAMIENTO DEL RIESGO	56
RIESGO RESIDUAL	59
SELECCIONAR OBJETIVOS DE CONTROL Y CONTROLES PARA EL TRATAMIENTO DE RIESGOS	59
PREPARACIÓN DE LA DECLARACIÓN DE APLICABILIDAD	60
PLAN DE TRATAMIENTO DEL RIESGO	60
MANTENIMIENTO Y MONITOREO DEL SGSI	61
REVISIÓN DE LOS RIESGOS Y LA REVALUACIÓN	63
CONCLUSIONES	64
REFERENCIAS BIBLIOGRÁFICAS	65

## CAPITULO 4

<b>GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO</b>	<b>67</b>
NATURALEZA DE UN PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO	67
EL PLAN DE CONTINUIDAD DEL NEGOCIO	68
EL PLAN DE CONTINUIDAD DEL NEGOCIO Y OTROS ENFOQUES	69
EL PROCESO DE PLAN DE CONTINUIDAD DEL NEGOCIO	70
FASE I <i>BUSINESS IMPACT ANALYSIS</i> (BIA)	70
FASE II GESTIÓN DEL RIESGO	71
FASE III DESARROLLO DE ESTRATEGIAS DE UN PCN	71
FASE IV DESARROLLO DEL PLAN DE REANUDACIÓN DE OPERACIONES	71
FASE V ENSAYO DEL PCN	71
FASE VI MANTENIMIENTO DEL PCN	72
FASE I <i>BUSINESS IMPACT ANALYSIS</i> (BIA)	72
MÉTODOS PARA LA RECOLECCIÓN DE INFORMACIÓN EN EL BIA	73
REQUERIMIENTOS DE TIEMPO DE RECUPERACIÓN	74
PROCESO METODOLÓGICO DEL BIA	74
PASO I - IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DE NEGOCIOS	75
PASO II - EVALUACIÓN DE LOS IMPACTOS FINANCIEROS Y OPERACIONALES	75
PASO III - IDENTIFICACIÓN DE PROCESOS CRÍTICOS	76
PASO IV - ESTABLECIMIENTO DE LOS TIEMPOS DE RECUPERACIÓN	77
PASO V - IDENTIFICACIÓN DE REQUERIMIENTOS DE RECURSOS	79
RECURSOS NO CRÍTICOS DE TECNOLOGÍA DE INFORMACIÓN	79

PASO VI - DETERMINACIÓN DEL <i>RECOVERY TIME OBJECTIVE</i>	80
PASO VII - DETERMINACIÓN DEL <i>RECOVERY POINT OBJECTIVE</i>	80
PASO VIII - IDENTIFICACIÓN DE PROCEDIMIENTOS ALTERNOS	80
PASO IX - GENERAR RESUMEN DE INFORME BIA	81
<b>FASE II GESTIÓN DEL RIESGO</b>	<b>81</b>
METODOLOGÍA DEL CÁLCULO DEL RIESGO	83
<b>FASE III DESARROLLO DE ESTRATEGIAS PARA LA CONTINUIDAD DEL NEGOCIO</b>	<b>89</b>
FASE IV - DESARROLLO DEL PLAN DE REANUDACIÓN DE OPERACIONES	90
<b>FASE V ENSAYO DEL PLAN DE CONTINUIDAD DEL NEGOCIO</b>	<b>92</b>
<b>FASE VI MANTENIMIENTO DEL PLAN DE CONTINUIDAD DEL NEGOCIO</b>	<b>93</b>
CONCLUSIONES	93
REFERENCIAS BIBLIOGRÁFICAS	94

## CAPITULO 5

### METODOLOGÍA PARA DOCUMENTAR UN SISTEMA

<b>DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN</b>	<b>95</b>
INTRODUCCIÓN	95
PIRÁMIDE DOCUMENTAL DEL ISO 27001:2005	96
NIVEL I - MANUAL DE SEGURIDAD	96
NIVEL II - PROCEDIMIENTOS	97
NIVEL III - INSTRUCCIONES DE TRABAJO	97
NIVEL IV - DOCUMENTOS	97
1. IDENTIFICAR PROCEDIMIENTOS A DOCUMENTAR	103
2. DEFINIR EL FORMATO DEL PROCEDIMIENTO	104
3. IDENTIFICAR ACTORES DEL PROCEDIMIENTO	105
4. CONVOCAR A LOS ACTORES A UNA REUNIÓN DE DOCUMENTACIÓN	105
5. LEVANTAR EL FLUJOGRAMA MATRICIAL NORMATIVO	106
6. VALIDAR EL FLUJOGRAMA	108
7. REDACCIÓN EN <i>PLAYSCRIPT</i>	108
8. VALIDAR LA NARRACIÓN EN <i>PLAYSCRIPT</i>	110
9. IDENTIFICAR SI SE REQUIEREN INSTRUCCIONES DE TRABAJO	110
10. REDACTAR INSTRUCCIONES DE TRABAJO	110
11. VALIDAR LAS INSTRUCCIONES DE TRABAJO	111
12. IDENTIFICAR LOS REGISTROS REQUERIDOS	112
13. IDENTIFICAR LOS DOCUMENTOS DE SEGURIDAD DE INFORMACIÓN	113
CONCLUSIONES	114
REFERENCIAS BIBLIOGRÁFICAS	115

## CAPÍTULO 6

### IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD

<b>DE INFORMACIÓN BAJO LA ÓPTICA ISO 27001:2005</b>	<b>117</b>
CICLO METODOLÓGICO PARA LA IMPLANTACIÓN DEL MODELO ISO 27001:2005	117
FASE I - TALLER ESTRATÉGICO CON LA GERENCIA PARA ANALIZAR REQUERIMIENTOS DEL MODELO ISO 27001:2005	120
FASE II - DETERMINACIÓN DEL ALCANCE DEL MODELO EN LA EMPRESA	120
FASE III - EFECTUAR UN ANÁLISIS Y EVALUACIÓN DEL RIESGO	122
FASE IV - ELABORACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO	123
FASE V - IMPLEMENTAR Y OPERAR EL SGSI	124
FASE VI - MONITOREAR Y REVISAR EL SGSI	124
FASE VII - MANTENER Y MEJORAR EL SGSI	125
FASE VIII - DESARROLLO DE COMPETENCIAS ORGANIZACIONALES	125
FASE IX - REDACCIÓN DEL MANUAL DE SEGURIDAD DE INFORMACIÓN	126
FASE X - EJECUCIÓN DE LAS AUDITORÍAS INTERNAS	127

FASE XI - OBTENCIÓN DE LA CERTIFICACIÓN INTERNACIONAL	127
CONCLUSIONES	128
REFERENCIAS BIBLIOGRÁFICAS	129

## APÉNDICE 1

<b>NORMA VENEZOLANA</b>	<b>131</b>
FONDONORMA	131
ISO/IEC 27001:2006	131
ISO/IEC 27001:2005	131
TECNOLOGIA DE LA INFORMACIÓN	131
TÉCNICAS DE SEGURIDAD	131
SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	131
REQUISITOS	131
PRÓLOGO	131
0 INTRODUCCIÓN	132
0.1 GENERALIDADES	132
0.2 ENFOQUE BASADO EN PROCESOS	132
0.3 COMPATIBILIDAD CON OTROS SISTEMAS DE GESTIÓN	134
1 OBJETO	134
1.1 GENERALIDADES	134
1.2 APLICACIÓN	134
2 REFERENCIAS NORMATIVAS	134
2.1 OTRAS NORMAS	135
3 TÉRMINOS Y DEFINICIONES	135
3.1 ACTIVO	135
3.2 DISPONIBILIDAD	135
3.3 CONFIDENCIALIDAD	135
3.4 SEGURIDAD DE LA INFORMACIÓN	135
3.5 EVENTO DE SEGURIDAD DE LA INFORMACIÓN	135
3.6 INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	135
3.7 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	135
3.8 INTEGRIDAD	136
3.9 RIESGO RESIDUAL	136
3.10 ACEPTACIÓN DEL RIESGO	136
3.11 ANÁLISIS DEL RIESGO	136
3.12 EVALUACIÓN DEL RIESGO	136
3.13 VALORACIÓN DEL RIESGO	136
3.14 GESTIÓN DEL RIESGO	136
3.15 TRATAMIENTO DEL RIESGO	136
3.16 DECLARACIÓN DE APLICABILIDAD	136
4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	137
4.1 REQUISITOS GENERALES	137
4.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI	137
4.3 REQUISITOS DE LA DOCUMENTACIÓN	140
5 RESPONSABILIDAD DE LA DIRECCIÓN	141
5.1 COMPROMISO DE LA DIRECCIÓN	141
5.2 GESTIÓN DE LOS RECURSOS	142
6 AUDITORÍAS INTERNAS DEL SGSI	142
7 REVISIÓN POR LA DIRECCIÓN DEL SGSI	143
7.1 GENERALIDADES	143
7.2 ELEMENTOS DE ENTRADA PARA LA REVISIÓN	143
7.3 RESULTADOS DE LA REVISIÓN	143
8 MEJORA DEL SGSI	144
8.1 MEJORA CONTINUA	144

8.2 ACCIÓN CORRECTIVA	144
8.3 ACCIÓN PREVENTIVA	144
<b>ANEXO A</b>	<b>145</b>
(NORMATIVO)	145
OBJETIVOS DE CONTROL Y CONTROLES	145
TABLA A.1: <i>OBJETIVOS DE CONTROL Y CONTROLES</i>	145
<b>ANEXO B</b>	<b>159</b>
(INFORMATIVO)	159
PRINCIPIOS OECD Y ESTA NORMA	159
TABLA B.1. <i>PRINCIPIOS OECD Y EL MODELO PHVA</i>	159
<b>ANEXO C</b>	<b>160</b>
(INFORMATIVO)	160
CORRESPONDENCIA ENTRE LA NORMA ISO 9001:2000, ISO 14001:2004 Y ESTA NORMA	160
TABLA C.1: CORRESPONDENCIA ENTRE LA NORMA ISO 9001:2000, LA ISO 14001:2004 Y ESTA NORMA	160
<b>BIBLIOGRAFÍA</b>	<b>162</b>
PUBLICACIONES DE NORMAS	162
OTRAS PUBLICACIONES	162
<b>APÉNDICE 2</b>	
<b>REGISTRO PARA LA REVISIÓN GERENCIAL ISO 27001:2005</b>	<b>163</b>
<b>APÉNDICE 3</b>	
<b>DOCUMENTOS EXIGIDOS POR EL ISO 27001:2005</b>	<b>165</b>
DOCUMENTOS EXIGIDOS POR EL ISO 27001:2005	165
<b>EPÍLOGO</b>	<b>169</b>
<b>ÍNDICE DE GRÁFICOS</b>	<b>172</b>
<b>ÍNDICE DE TABLAS</b>	<b>173</b>
<b>ÍNDICE DE TEMÁTICO</b>	<b>174</b>