

CONTENIDO

Índice de Figuras	V
Índice de Tablas.....	VI
Tabla de Acrónimos.....	VII
INTRODUCCION.....	VIII
OBJETIVO GENERAL.....	IX
OBJETIVOS ESPECIFICOS.....	IX
JUSTIFICACION.....	IX
ALCANCE.....	X
METODOLOGIA.....	X
PARTE I: ANTECEDENTES DE LA EMPRESA	
1 CAPITULO 1: CLARA BELLA.....	13
1.1 DESCRIPCIÓN DE LA EMPRESA	14
1.2 ANTECEDENTES HISTÓRICOS	14
1.3 MISIÓN	16
1.4 VISIÓN	16
1.5 VALORES DE LA EMPRESA.....	14
1.6 ORGANIGRAMA.....	16
1.7 SISTEMAS	18
1.7.1 Misión	19
1.7.2 Visión.....	19
1.7.3 Objetivo.....	19
1.7.4 Descripción de Función Principal.....	19
1.7.5 Descripción de las Funciones Generales.....	19
2 CAPITULO 2: PROCESOS DE LA EMPRESA CLARA BELLA Y ÁREA TI	21
2.1 TECNOLOGÍA DE LA INFORMACIÓN.....	22
2.2 INFORMACIÓN DEL AMBIENTE DE SISTEMA	22
2.2.1 Procesos de la Empresa.....	22
2.2.2 Organigrama Funcional de Tecnología de Información.....	32
2.2.3 Recurso Tecnológico.....	36
2.2.4 Red	39
3 CAPITULO 3: DIAGNÓSTICO DE LA SEGURIDAD	41
3.1 PANORAMA ACTUAL	42
3.2 ELEMENTOS DE INFORMACIÓN	42

PARTE II: MARCO TEORICO

4	CAPITULO 4: SEGURIDAD DE LA INFORMACIÓN	46
4.1	CONCEPTO DE LA SEGURIDAD DE LA INFORMACIÓN	47
4.2	¿PORQUE ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN?	47
4.3	RETOS DE LA SEGURIDAD	48
4.4	¿CÓMO ESTABLECER LOS REQUISITOS DE SEGURIDAD?	49
4.5	EVALUACIÓN DE LOS RIESGOS EN MATERIA DE SEGURIDAD	49
4.6	SELECCIÓN DE CONTROLES	49
4.7	ELEMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN	50
4.8	ACTIVOS E INFORMACIÓN	52
4.9	VULNERABILIDADES, AMENAZAS, ATAQUES Y ATACANTES	52
5	CAPITULO 5: MEJORES PRÁCTICAS	54
5.1	ISO 27000	55
5.1.1	¿Por qué Utilizar ISO/IEC 27000?	55
5.1.2	ISO: 27XXX	56
5.2	NORMA ISO/IEC 27001	57
5.2.1	Objetivo	59
5.2.2	¿Por qué ISO 27001?	59
5.2.3	ISO 27001: Partes	59
5.3	NORMA ISO/IEC 27002:2005 ANTECEDENTES Y CARACTERÍSTICAS DE LA NORMA	60
5.3.1	ISO 27002: Partes	61
5.3.2	ISO/IEC 27002:2005: Descripción de guías y sus Contenidos	62
5.4	NORMA ISO/IEC 27005:2008 [ISO/IEC27005]	63
5.4.1	Objetivos y Campo de Aplicación ISO/27005:2008	64
5.4.2	Estructura de la Norma ISO/27005:2008	65
5.4.3	Visión General del Proceso de Gestión en la Seguridad de la Información	65
5.5	RELACIÓN ISO 27001 CON ISO 27005	65
5.6	ANÁLISIS DE RIESGOS SEGÚN LA NORMA ISO/IEC 27005:2008	66
5.6.1	Establecimiento del Contexto	66
5.6.2	Valoración del Riesgo en la Seguridad de la Información	67
5.6.3	Tratamiento del Riesgo en la Seguridad de la Información	70

PARTE III: PROPUESTA DE SEGURIDAD

6	CAPITULO 6: ESTABLECIMIENTO DEL CONTEXTO	74
6.1	ALCANCE Y LIMITES	75
6.2	CRITERIOS BÁSICOS	75
6.2.1	Criterios de Valoración de Activos	76
6.2.2	Criterios de Probabilidad de Ocurrencia de Amenazas	76
6.2.3	Criterios de Valoración de las Consecuencias	77
6.2.4	Criterios de evaluación del riesgo	78
6.2.5	Criterios para el Tratamiento del Riesgo	79
6.2.6	Criterios de Prioridad en la Aplicación de Controles	79
6.3	VALORACIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	80
7	CAPITULO 7: ANÁLISIS DE RIESGOS	81

7.1	IDENTIFICACIÓN DE RIESGOS.....	82
7.1.1	<i>Identificación de Activos</i>	82
7.1.2	<i>Valoración de Activos</i>	83
7.1.3	<i>Identificación de Amenazas</i>	85
7.1.4	<i>Identificación de Controles Existentes</i>	87
7.1.5	<i>Identificación de las Vulnerabilidades</i>	87
7.1.6	<i>Identificación de las Consecuencias</i>	87
7.2	ESTIMACIÓN DEL RIESGO	88
7.2.1	<i>Valoración de las Consecuencias</i>	88
7.2.2	<i>Valoración de los incidentes</i>	88
7.2.3	<i>Evaluación del Riesgo</i>	88
7.3	TRATAMIENTO DE RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN	93
7.4	RIESGO RESIDUAL.....	102
8	CAPITULO 8: CONTROLES SELECCIONADOS	111
8.1	ANÁLISIS SITUACIÓN ACTUAL.....	112
8.2	A.5 POLÍTICA DE SEGURIDAD.....	115
8.3	A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	119
8.3.1	<i>A.6.1 Organización Interna</i>	120
8.3.2	<i>A.6.2 Entidades Externas</i>	122
8.4	A.7 GESTIÓN DE ACTIVOS	124
8.4.1	<i>A.7.1.1 Inventario de Activos</i>	126
8.4.2	<i>A.7.1.2 Propiedad de los Activos</i>	126
8.4.3	<i>A.7.1.3 Uso Aceptable de los Activos</i>	127
8.4.4	<i>A.7.2 Clasificación de la Información</i>	133
8.5	A.8 SEGURIDAD DE LOS RECURSOS HUMANOS.....	135
8.5.1	<i>A.8.1. Antes del Empleo</i>	136
8.5.2	<i>A.8.2 Durante el Empleo</i>	137
8.5.3	<i>A.8.3 Terminación o Cambio de Empleo</i>	138
8.6	A.9 SEGURIDAD FÍSICA Y AMBIENTAL	140
8.6.1	<i>A.9.1. Áreas Seguras</i>	141
8.6.2	<i>A.9.2 Seguridad del Equipo</i>	145
8.7	A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	148
8.7.1	<i>A.10.1 Procedimientos y Responsabilidades Operacionales</i>	149
8.7.2	<i>A.10.3.Planeación y Aceptación del Sistema</i>	154
8.7.3	<i>A.10.4 Protección contra Software Malicioso y Código Móvil</i>	155
8.7.4	<i>A.10.5 Respaldo de Información o Backups (Copias de Seguridad)</i>	157
8.7.5	<i>A.10.6 Gestión de Seguridad de Redes</i>	158
8.7.6	<i>A.10.7 Gestión de Medios</i>	160
8.7.7	<i>A.10.10 Monitoreo</i>	162
8.8	A.11 CONTROL DE ACCESOS	165
8.8.1	<i>A.11.1 Requerimiento Comercial para el Control del Acceso</i>	167
8.8.2	<i>A.11.2 Gestión del Acceso del Usuario</i>	168
8.8.3	<i>A.11.3 Responsabilidades del Usuario</i>	171
8.8.4	<i>A.11.4 Control de Acceso a la Red</i>	172
8.8.5	<i>A.11.5 Control de Acceso al Sistema Operativo</i>	175
8.8.6	<i>A.11.6 Control de Acceso a la Aplicación y la Información</i>	179
8.8.7	<i>A.11.7 Computación y Tele-trabajo Móvil</i>	180
8.9	A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.....	182

8.9.1	A.12.1	<i>Análisis y Especificaciones de los Requerimientos de Seguridad</i>	184
8.9.2	A.12.2	<i>Seguridad en los Sistemas de Aplicación</i>	184
8.9.3	A.12.3	<i>Controles criptográficos</i>	186
8.9.4	A.12.4	<i>Seguridad de los Archivos de Sistema</i>	189
8.9.5	A.12.5	<i>Seguridad en los Procesos de Desarrollo y Soporte</i>	191
8.9.6	A.12.6	<i>Gestión de Vulnerabilidades Técnicas</i>	193
8.10	A.13	GESTIÓN DE UN INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN	194
8.10.1	A.13.1	<i>Reporte de los Eventos y Debilidades de la Seguridad de la Información</i>	195
8.10.2	A.13.2	<i>Gestión de los Incidentes y Mejoras en la Seguridad de la Información</i>	196
8.11	A.14	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	198
8.11.1	A.14.1	<i>Aspectos de la Seguridad de la Información de la Gestión de la Continuidad del Negocio 200</i>	
8.12	A.15	CUMPLIMIENTO	202
8.12.1	A.15.2	<i>Cumplimiento de las Políticas y Estándares de Seguridad y Cumplimiento técnico</i>	204
CONCLUSIONES			205
RECOMENDACIONES			207
BIBLIOGRAFÍA			208
ANEXOS			210

Anexo A Cartas Institucionales

Anexo B Plan de Continuidad del Negocio

Anexo C Flujogramas de Procesos

Anexo D Análisis de Riesgo