

UNIVERSIDAD CIENTIFICA DEL SUR
FACULTAD DE INGENIERIA DESISTEMAS EMPRESARIALES

**PROYECTO DE IMPLEMENTACIÓN DE UNA EMPRESA
PRESTADORA DE SERVICIOS DEL CICLO COMPLETO DE
GESTION DE SEGURIDAD DE LA INFORMACIÓN PARA
PYMES.**

Trabajo Profesional para optar por el Título Profesional de
Ingeniero de Sistemas Empresariales

Eduardo Andrés Kodaka Yagi

Miraflores, 6 de Diciembre de 2011

Glosario de términos

TI: Tecnología de Información.

Decisión: elección de un curso de acción determinado entre varios posibles.

Plan: conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.

Política: definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

Meta: objetivo cuantificado a valores predeterminados.

Procedimiento: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

Norma: forma en que realiza un procedimiento o proceso.

Programa: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronostico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.

Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.

Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso.

Backbone: Segmento, generalmente de Fibra Óptica, que une la red de comunicaciones LAN entre diferentes localidades o edificios. También es la parte de la red que soporta el tráfico más pesado.

Cortafuegos/ Firewall: Una combinación de Hardware y Software que limita la exposición de un computador o un grupo de computadores a otras redes como internet para evitar ataques exteriores

Encriptación: La transformación de la data a un formato ilegible, sólo se puede acceder con una clave secreta.

Extranet: Red interna que usa la Compañía para comunicación de sus empleados con clientes y/o proveedores, incluye sitios Web. El acceso se puede hacer a través de Internet.

Internet: Es una red de uso público de computadores de todo tipo que se comunican con el protocolo estándar TCP IP, lo cual les permite compartir información al mismo tiempo.

Intranet: Red privada que usa software y estándares de Internet reservada para personas a las que se le ha dado autorización y claves necesarias para el acceso a la información de la Compañía

Networking: Trabajo en sistema de redes.

Ruteadores: Dispositivo que conecta 2 redes.

Site: Sitio o página Web.

Switches: Dispositivo que permite comunicación de computadoras.

VPN (Virtual Private Network): Red privada Virtual, permite encapsular la comunicación entre 2 puntos a través de una red generalmente pública.

INDICE

Dedicatoria	ii
Agradecimiento	iii
Resumen Ejecutivo	iv
Abstract	vi
Glosario	viii
Índice	x
Índice de Tablas	xiv
Índice de Figuras	xvi
Introducción	1
CAPITULO I : DESCRIPCION DEL CONTEXTO	3
1.1 Antecedentes	3
1.2 Formulación del Problema	20
1.3 Justificación	21
1.4 Objetivos	21
1.4.1 Objetivo General	22
1.4.2 Objetivos Específicos	22

CAPITULO II	NORMAS LEGALES Y TECNICAS	23
2.1	Internacionales	23
2.1.1	Normas ISO 27000:	23
2.2	Nacionales	24
2.2.1	NTP-ISO/IEC 17799	24
2.2.2	Ley de Delitos informáticos	27
2.2.3	Ley 29733 de protección de datos personales.	27
2.2.4	Normatividad Penal:	27
2.2.5	Normas Administrativas	27
2.2.6	Leyes que regulan a los Sistemas Administrativos	27
2.2.7	Otras normas:	28
CAPITULO III	METODO	29
3.1	Metodología general	29
3.1.1	ISO 27000.	29
3.1.2	ITIL	29
3.1.3	PMBOK	29
3.1.4	COBIT.	30
3.2.5	ISO 31000/2009	30
3.2.6	ISO/IEC 38500:2008	30
3.2	Metodología específica	32
3.2.1	Análisis del objetivo de la Seguridad Informática	32
3.2.1	Metodología para la Gestión de Riesgos de TI	41
3.2.1	Plan de Acción	54
3.2.2	Seguridad Organizativa	56
3.2.2	Seguridad Lógica	62

3.2.3 Seguridad Física	69
CAPITULO IV ETAPA DE PREPARACION Y EVALUACION DEL PROYECTO	81
4.1 Estudio del mercado	81
4.1.1 ANALISIS PESTE	81
4.1.2 ANALISIS FODA	91
4.1.3 FODA CRUZADO	92
4.1.4 ANALISIS DE LAS FUERZAS COMPETITIVAS	94
4.1.5 Matriz de evaluación de factor externo (EFE)	94
4.1.6 Matriz de evaluación de factor interno (EFI)	95
4.1.7 PLAN DE MARKETING	96
4.2 Constitución de la empresa y localización de la planta	97
4.2.1 Localización de planta	97
4.2.2 Constitución de la empresa	98
4.2.3 Misión de la Organización	102
4.2.4 Visión de la Organización	103
4.2.5 Valores de la Organización	103
4.3 Ingeniería del Proyecto	104
4.3.1 Consultoría.	104
4.3.3 Implementación.	106
4.3.4 Soporte técnico.	106
4.3.5 Auditoría.	107
4.3.6 Macro Procesos	107
4.4 Capital Humano	113
4.4.1 Estructura Organizacional	113
4.4.2 Descripción de puesto de trabajo	113

4.4.3 Competencias	114
4.5 Proyecciones financieras	120
4.5.1 Información económica.	120
4.5.2 Estado de Ganancias y Pérdidas	122
4.5.3 Estado de Flujo de Caja Proyectado	123
4.6 Evaluación financiera del proyecto	124
4.7 Estructura de Capital	124
4.8 Estimación de riesgos del Proyecto	125
4.8.1 Análisis de Impacto	125
4.8.2 Ponderación de Impacto	126
4.8.3 Análisis de Riesgo	126
4.8.4 Matriz de decisiones	127
CAPITULO V: CONCLUSIONES Y RECOMENDACIONES	130
5.1 Discusión	130
5.2 Conclusiones	130
5.3 Recomendaciones	131
5.4 Bibliografía	131

INDICE DE TABLAS

TABLA 1: El Proceso del Plan de Acción	43
TABLA 2: Proceso de Implantación	43
TABLA 3: Proceso de Control y Mantenimiento	44
TABLA 4: Matriz de Ponderación de los activos	48
TABLA 5: Matriz de amenazas a los activos de TI	50
TABLA 6: Controles de la seguridad de la información	52
TABLA 7: Dominios de la Seguridad de la Información	53
TABLA 8: Organización de la Seguridad de la Información	57
TABLA 9: Gestión de Activos de Información	58
TABLA 10: Seguridad de los Recursos Humanos	59
TABLA 11: Gestión de Continuidad del Negocio	60
TABLA 12: Control de Accesos	61
TABLA 13: PBI Per cápita 2010	89
TABLA 14: PBI Per cápita 2010 en US\$ corrientes	90
TABLA 15: Matriz FODA	93
TABLA 16: Matriz EFE	95
TABLA 17: Matriz EFI	96
TABLA 18: Participación de PYMES por Distrito	97
TABLA 19: Actividad de las Pymes	97
TABLA 20: Estimación de Precios para la consultoría	105

TABLA 21: Estimación de margen por ventas	106
TABLA 22: Productos ofrecidos	109
TABLA 23: Capacidad de Planificación y organización	114
TABLA 24: Comunicación	115
TABLA 25: Empowerment	116
TABLA 26: Enfoque al cliente	117
TABLA 27: Planificación y Visión Estratégica	118
TABLA 28: Liderazgo	119
TABLA 29: Gastos de Implementación de la Empresa (año 0)	120
TABLA 30: Gastos Administrativos	120
TABLA 31: Gastos esporádicos	121
TABLA 32: Estado de Ganancias y Pérdidas	122
TABLA 33: Estado de Flujo de Caja Proyectado	123
TABLA 34: Costo de capital, valor actual neto, Tasa interna de retorno, Pay Back Descontado	124
TABLA 35: Estructura de capital	124
TABLA 36: Análisis de impacto	125
TABLA 37: Análisis de Ponderación de impacto	126

INDICE DE FIGURAS

FIGURA 1: Amenazas para la seguridad	34
FIGURA 2: Tipos de intrusos.	37
FIGURA 3: Tipos de ataque según su fin	39
FIGURA 4: Relación Operatividad–Seguridad.	40
FIGURA 5: Procesos de la Gestión de Riesgos de TI	41
FIGURA 6: El proceso de Análisis de Riesgo	42
FIGURA 7: Riesgo de la Operación del Negocio	45
FIGURA 8: Riesgo de TI	46
FIGURA 9: Sub procesos del análisis de riesgo	46
FIGURA 10: Análisis del negocio	47
FIGURA 11: Tipos de activos de TI	47
FIGURA 12: Árbol de dependencias entre activos de TI	48
FIGURA 13: Activos Versus Dimensiones	50
FIGURA 14: El Impacto	51
FIGURA 15: El Riesgo	51
FIGURA 16: PDCA Ciclo de Vida de Deming	52
FIGURA 17: Dominios de la gestión de seguridad de la información	53
FIGURA 18: Implementación de la gestión de seguridad de la información	55

FIGURA 19: Seguridad Organizativa.	56
FIGURA 20: Organización de la Seguridad de la Información	57
FIGURA 21: Gestión de Activos de Información	58
FIGURA 22: Seguridad de los Recursos Humanos	59
FIGURA 23: Gestión de Continuidad del Negocio	60
FIGURA 24: La caída de la producción industrial -	82
FIGURA 25: Desplome Bursatil	83
FIGURA 26: La evolución del mercado de valores de EEUU	84
FIGURA 27: Contracción del Mercado internacional	85
FIGURA 28: Políticas anticrisis	86
FIGURA 29: Expansión de la oferta monetaria	87
FIGURA 30 : Creación de políticas y plan de implementación de tecnología	105
FIGURA 31: Los macro procesos	107
FIGURA 32: El Proceso de Consultoría	110
FIGURA 33: El proceso de valoración	111
FIGURA 34: El proceso de venta e implementación	112
FIGURA 35: Estructura Organizacional	113
FIGURA 36: Matriz de Riesgo	126